SOCIÉTÉ | NUMÉRIQUE

Société Numérique, CH-4000 Basel

Département fédéral de la défense,
de la protection de la population et des sports (DDPS)
3003 Berne

Par courrier: vincianne.grundschober@ndb.admin.ch

5. Septembre 2022

*(Disclaimer : Avis pour le lecteur ou la lectrice. Le texte suivant est uniquement une traduction de l'original envoyé en langue allemande)*

**Procédure de consultation : Révision de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)**

Madame la Conseillère fédérale,

Mesdames, Messieurs,

La Société Numérique souhaite participer à la procédure de consultation sur l'avant-projet de révision de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens) et vous prie de trouver ci-après sa prise de position sur ce projet.

## Table des matières


1. Remarques préliminaires....4
2. Affaiblissement des restrictions légales de traitement....5
2.1. Art. 5 al. 5 nLRens – « aucune donnée personnelle »....5
2.2. Art. 5 al. 5 nLRens – Exception pour les données administratives....8
2.3 Art. 5 al. 6 let. b et art. 5 al. 8 nLRens....9
2.4. Art. 5 al. 6 let. c nLRens – Protection d'une organisation ou d'une personne....9
2.5 Art. 45 al. 4 nLRens....9
2.6 Art. 46 nLRens – Examen de l'applicabilité de l'art. 5 al. 5 nLRens....10
3. Droit d'accès....11
3.1. Art. 63a al. 8 nLRens – Refus du droit d'accès....11
3.2. Art. 64 nLRens – Droit d'accès dans le cadre de la PES....12
4. Mesures de recherche soumises à autorisation (MRSA)....12
4.1. Art. 14 nLRens – Observation préventive secrète au moyen d'appareils de localisation....12
4.2 Conditions d'autorisation....14
4.2.1. Art. 27 al. 1 let. a ch. 1 nLRens– Élargissement à l'extrémisme violent....14
4.2.2. Art. 27 al. 1 let. a ch. 2 nLRens – Surveillance au profit d'États étrangers....15
4.3. Procédure d'autorisation....16
4.3.1. Art. 29 nLRens– Demande de MRSA....16
4.3.2. Art. 29a al. 5 nLRens – MRSA à l'étranger....17
4.4. Art. 29b et 30 nLRens – Durée de l'autorisation et prolongation de la MRSA....18
4.5. Art. 33 nLRens – Information à la personne surveillée....20
4.6. Art. 50 nLRens – Traitement des données recueillies lors d'une mesure de recherche soumise à autorisation....21
4.6.1. Tri et destruction des données....21
4.6.2. Art. 50 al. 2 nLRens – Données protégées par le secret professionnel....21
4.7. Art. 83 nLRens – Voies de droit....23
4.8 Art. 26 al. 1 let. f et g nLRens – surveillance des relations bancaires et des transactions financières....24
4.9 Art. 28 nLRens – Mesures de recherches soumises à autorisation contre des tiers....26
4.10. Art. 37 nLRens – Ordre urgent d'infiltrer des systèmes et réseaux informatiques à l'étranger. 28
4.11. Art. 38 LRens (exploration radio) et art. 39 ss LRens (exploration du réseau câblé)....29
4.12. Art. 39 nLRens – Exploration du réseau câblé contre des personnes physiques ou morales suisses se trouvant à l'étranger....29
4.13 Art. 41 al. 3 nLRens – Prolongation du délai....30
4.14. Art. 42 nLRens – Analyse des signaux et des données de mandats existants en matière d'exploration du réseau câblé....30
5. Assurance qualité : art. 58b nLRens – données personnelles relevant du renseignement..31
6. « Internet » au lieu de « cyberespace »....32
6.1 Art. 6 al. 1 let. b nLRens....32
6.2 Art. 19 al. 2 let. f nLRens....32

7. Art. 75 ss LRens – Révision totale de l'autorité de surveillance AS-Rens.....32
8. Dispositions pénales.....33
8.1. Art. 83a nLRens – Interdiction d'organisations.....33
8.2. Art. 83b en relation avec l'art. 73 al. 1 nLRens – Interdiction d'exercer une activité.....33
8.3. Art. 83c nLRens – Insoumission à une décision.....34
8.4. Art. 83d et 83e nLRens– Juridiction.....35
9. Élargissement de l'interdiction de se rendre dans un pays donné.....35
9.1. Art. 24h nLMSI.....35
9.2. Art. 24k nLMSI – Limite d'âge.....37
10. Traitement de données et assurance qualité : algorithmes et reconnaissance faciale……38

## 1. Remarques préliminaires

Il y a plus de 30 ans, une commission d'enquête parlementaire découvrait que les autorités fédérales et cantonales avaient établis des fiches et des dossiers sur plus de 900'00 personnes et organisations, sans aucune base légale pour ce faire[1]. Des bases légales lacunaires et une image dépassée des menaces avaient conduit à la collecte d'informations sur l'exercice légal des droits politiques par des organisations et des particuliers, pour la plupart de gauche et critiques. Le législateur a agi et a édicté une restriction de traitement dans la loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI) (aujourd'hui art. 5 al. 5 LRens ; à l'origine art. 3 al. 1 aLMSI)[2]. Ceci dans le but exprès de protéger l'exercice des droits politiques et la formation de l'opinion politique[3].

Néanmoins, en juin 2022, il a été rendu public que le Service de renseignement de la Confédération (SRC) – sous l'ancienne direction de Markus Seiler et de Jean-Philippe Gaudin – avait sciemment enfreint pendant des années la limite de traitement de l'art. 5 LRens et avait même ignoré des recommandations et des avis de droit de la Délégation des Commissions de gestion (DélCdG) et de l'Office fédéral de la justice (OFJ)[4]. Le SRC a alors annoncé à grand renfort de publicité qu'il avait adapté sa « directive de collecte » interne de manière à correspondre à la restriction légale de traitement et qu'il avait depuis effacé plus de 4 millions de données[5].

Malgré des années de violations systématiques de la restriction légale de traitement, la révision actuelle de la loi sur le renseignement prévoit d'élargir considérablement les compétences du SRC et de porter atteinte aux droits individuels des personnes concernées. C'est notamment pour cette raison que la Sociéte Numérique est de plus en plus préoccupée par la protection des droits fondamentaux et des droits humains en Suisse, notamment en relation avec les activités du SRC.

Cela commence déjà par la formulation vague des dispositions qui définissent le but et les tâches du SRC et auxquelles se rattachent les compétences légales de traitement des données. Si des dispositions légales autorisent des atteintes aux droits fondamentaux, elles doivent être suffisamment claires et concrètes pour qu'il soit possible de prévoir, à partir du texte de la loi, dans quelles conditions les justiciables peuvent être concernés et pour garantir ainsi une pratique conforme aux droits fondamentaux. Si les dispositions légales sont formulées de manière trop vague et ouverte, les autorités chargées de l'application du droit disposent d'une telle marge de manœuvre qu'il est difficile pour les justiciables d'estimer quelles seront les conséquences juridiques de l'exercice de leurs droits

1 Événements survenus au DFJP Rapport de la commission d'enquête parlementaire (CEP) du 22 novembre 1989 ; Événements survenus au DFJP Rapport complémentaire de la commission d'enquête parlementaire (CEP) du 29 mai 1990.
2 Art. 3 aLMSI.
3 Message concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire « S. o. S. – pour une Suisse sans police fouineuse », 7 mars 1994, FF 1994 II 1123, p. 1171.
4 Rapport annuel 2019 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, 28 janvier 2020, FF 2020 2865, p. 2941.
5 Émission de la SRF 10vor10 du 1er juin 2022. Cela s'explique probablement par le fait que la cheffe du DDPS a ordonné au directeur du SRC de mettre en œuvre toutes les mesures proposées par la Délégation des Commissions de gestion. (Rapport annuel 2020 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, 26 janvier 2021, FF 2021 570, p. 110).

fondamentaux. Cela peut les dissuader de les exercer (« chilling effect »), ce qui affecte fondamentalement les droits politiques. L'exercice de la liberté de réunion et d'association ainsi que de la liberté d'expression est particulièrement concerné. C'est pourquoi les dispositions légales qui portent atteinte à la libre communication doivent répondre à des exigences particulièrement strictes en matière de précision. Or, la LRens contient en partie des notions très larges et indéterminées, qui ne permettent pas de déterminer suffisamment clairement dans quelles circonstances un comportement peut donner lieu à la saisie de données par le SRC. Ces notions ne sont donc pas suffisantes pour justifier des atteintes aux droits fondamentaux[6].

Les dispositions légales existantes n'ont pas réussi jusqu'à présent à garantir une pratique du traitement des données par les services de renseignement conforme aux droits fondamentaux, notamment en raison du caractère vague des dispositions légales. La marge de manœuvre résultant de notions juridiques indéterminées ne doit pas avoir pour conséquence l'établissement d'une pratique qui viole régulièrement les droits fondamentaux. Le traitement des données par les services de renseignement doit être soumis à des limites légales claires. C'est la seule façon de garantir que toute activité politique protégée par les droits fondamentaux ne risque pas d'être enregistrée par les services de renseignement et de vider ainsi les droits fondamentaux de leur substance.

Au regard du présent projet de loi, ce sont notamment l'assouplissement supplémentaire de la restriction du traitement des données, les lacunes du droit d'accès, l'extension des mesures de recherche soumises à autorisation, l'introduction de dispositions pénales et l'extension de l'interdiction de quitter le territoire qui s'avèrent problématiques.

En outre, le projet de loi contient plusieurs dispositions qui se recoupent avec des réglementations figurant dans d'autres lois et qui seraient réglementées au mauvais endroit dans la législation sur le renseignement. Cela concerne notamment les dispositions pénales prévues ainsi que la surveillance des relations bancaires et des transactions financières.

## 2. Affaiblissement des restrictions légales de traitement

### 2.1. Art. 5 al. 5 nLRens – « aucune donnée personnelle »

Il faut renoncer à la modification proposée de l'art. 5 al. 5 nLRens. En lieu et place, il convient de préciser les limites de traitement prévues par la loi.

La limite de traitement ancrée à l'art. 5 al. 5 LRens (à l'origine art. 3 al. 1 aLMSI), selon laquelle le SRC ne collecte ni ne traite d'informations sur l'activité politique et sur l'exercice de la liberté d'opinion, de réunion ou d'association en Suisse, devait à l'origine garantir que les personnes et les organisations soient protégées contre le traitement d'informations par les services de renseignement dans l'exercice

6 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, p. 5 N 5 ss.

de leurs droits fondamentaux. Le message relatif à la LMSI considérait en outre que l'évaluation de l'exactitude et de la pertinence des informations était essentielle pour le traitement des informations par les services de renseignement. Le message soulignait que les données personnelles ne pouvaient être traitées que si et aussi longtemps que cela était nécessaire à l'accomplissement des tâches légales. Pour pouvoir satisfaire à ces exigences, le contrôle ne doit pas seulement avoir lieu à la réception des données, mais doit être répété régulièrement. C'est la seule façon de garantir qu'aucune information erronée, superflue ou devenue inutile ne soit conservée et traitée[7].

Ces exigences relatives au traitement des informations par les services de renseignement (ne pas enregistrer les personnes et les organisations dans l'exercice de leurs droits fondamentaux ; évaluer les données en fonction de leur exactitude et de leur pertinence ; ne traiter les données personnelles que si et aussi longtemps que cela est nécessaire à l'accomplissement des tâches légales ; vérifier les données dès leur réception ; vérifier périodiquement les données saisies ; s'assurer qu'aucune donnée fausse, superflue ou inutile ne soit conservée ou traitée) ont joué un rôle fondamental dans les efforts déployés à la suite du scandale des fiches pour donner une base légale claire à l'activité de renseignement et pour établir une pratique du renseignement qui garantisse le respect des droits fondamentaux.

Les droits fondamentaux et les limites de traitement qui ancrent les droits fondamentaux dans la loi doivent garantir que les personnes et les organisations puissent être sûres d'être libres de toute surveillance par les services de renseignement dans l'exercice de leurs droits politiques fondamentaux. Les justiciables doivent avoir la certitude qu'ils ne doivent s'attendre à une atteinte à leurs droits fondamentaux que si leur comportement en donne concrètement l'occasion. Sinon, ils doivent être protégés contre le fait d'être touchés par le traitement de données par les services de renseignement dans l'exercice de leurs droits fondamentaux, en particulier dans le cadre de leurs activités politiques.

Dans la pratique, cette protection des droits fondamentaux n'est toutefois pas garantie, comme le montrent différents rapports de la DélCdG et de nombreuses inscriptions dans les banques de données des services de renseignement rendues publiques par des personnes concernées. Dans son rapport du 21 juin 2010 sur le traitement des données dans l'ancien système de traitement des données relatives à la protection de l'Etat (ISIS), la DélCdG avait déjà constaté un fort accroissement des stocks de données et une série d'autres dysfonctionnements graves. La délégation est parvenue à la conclusion que l'état des données remettait fondamentalement en question l'utilité des services de protection de l'Etat. Dans ses rapports annuels 2019, 2020 et 2021, la DélCdG montre en outre que le SRC a collecté et traité des informations sur l'activité politique et sur l'exercice de la liberté d'opinion, de réunion ou d'expression en contradiction avec les dispositions légales. Les barrières légales qui devaient protéger les personnes et les organisations exerçant une activité politique contre une saisie de données par le service de renseignement n'ont donc pas été efficaces dans de nombreux cas.

7 Message concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire « S. o. S. – pour une Suisse sans police fouineuse », 7 mars 1994, FF 1994 II 1123, p. 1171.

La révision actuelle de la loi sur le renseignement doit garantir qu'à l'avenir, la protection de la limite du traitement des données sera également assurée dans la pratique. En réalité, elle manque totalement cet objectif :

Avec la révision, la formulation de la disposition légale qui interdit au SRC de collecter et de traiter certaines catégories de données change. Il ne sera plus indiqué « aucune *information* » mais « aucune *donnée personnelle* relative aux activités politiques ou à l'exercice de la liberté d'opinion, d'association ou de réunion en Suisse » (art. 5 al. 5 nLRens). Par le passé, le SRC a déjà argumenté à plusieurs reprises sur la notion de « données personnelles » pour refuser le droit d'accès et d'effacement des données. Ainsi, dans deux procédures de recours devant le Tribunal administratif fédéral – procédures n° A-3275/2021 et A-4873/2021 – le SRC a argumenté que les données dans lesquelles une personne ou une organisation est simplement mentionnée ne sont pas des données personnelles, car elles ne sont pas utilisées par le SRC en tant que données personnelles. Pour cette raison, il n'y aurait ni droit d'accès à ces données, ni motif d'effacement.[8]

A l'inverse, la DélCdG, le TAF et l'OFJ ont affirmé à plusieurs reprises que toutes les informations se rapportant à des personnes et à des organisations que le SRC peut trouver dans ses bases de données au moyen de la fonction de recherche sont considérées par la loi comme des « données personnelles ». Les données correspondantes constituent donc des données personnelles du point de vue de la protection des données et sont soumises à la restriction de traitement prévue à l'art. 5 al. 5 LRens.

Or, la nouvelle formulation de l'art. 5 al. 5 nLRens offrirait au SRC un champ supplémentaire pour collecter et traiter des données relatives à l'exercice de la liberté d'opinion, de réunion ou d'association, en arguant qu'il ne s'agirait pas de données personnelles et que, par conséquent, ces données ne seraient pas couvertes par la limitation du traitement des données. Ainsi, la protection que la limite de traitement devrait offrir en faveur de l'activité politique et de l'exercice de la liberté d'opinion, de réunion ou d'association est en grande partie inefficace. Enfin, la terminologie utilisée à l'art. 5 nLRens n'est pas homogène : à l'al. 1, le projet de loi continue d'utiliser le terme « informations ».

Les notions utilisées dans la loi et les limites du traitement doivent être précisées dans le cadre de la révision, dans le but de pouvoir garantir une pratique du traitement des données par les services de renseignement conforme aux droits fondamentaux. Pour ce faire, il convient de s'appuyer sur les recommandations émises par la DélCdG,[9] pour prévenir le traitement de données contraire au droit. Ces recommandations ne doivent pas être seulement prévues dans les directives internes du SRC mais ancrées dans la loi formelle.

8 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022.

9 Rapport annuel 2019 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, 28 janvier 2020, FF 2020 2865.

### 2.2. Art. 5 al. 5 nLRens – Exception pour les données administratives

L'exception de l'art. 5 al. 5 nLRens ne peut en aucun cas s'appliquer aux données personnelles relatives à l'activité politique et à l'exercice de la liberté d'opinion, de réunion ou d'association.

L'exception pour le traitement de données à des fins administratives ne devrait pas se trouver à l'art. 5 al. 5 nLRens, mais à l'art. 5 al. 6 nLRens.

L'art. 5 al. 5, nLRens introduit une nouvelle disposition selon laquelle les données personnelles relatives à l'activité politique et à l'exercice de la liberté d'opinion, de réunion ou d'association en Suisse peuvent être traitées par le SRC à titre exceptionnel si cela sert à l'accomplissement de ses tâches administratives.

Il n'y a en principe rien à objecter au traitement de données pour l'accomplissement de tâches administratives si, comme le mentionne le rapport explicatif, cette exception ne s'applique effectivement qu'aux objets parlementaires qui sont attribuées au SRC ou dans le cadre du droit d'accès aux données personnelles. Dans ce cas également, il convient toutefois de s'assurer que cette exception ne s'applique que dans la mesure où elle est réellement nécessaire à l'accomplissement de tâches administratives proprement dites. En outre, l'exception ne doit être appliquée que pour les informations qui ne sont pas pertinentes pour les services de renseignement.

Dans sa pratique actuelle, le SRC ne délimite pas de manière rigoureuse les informations relevant du renseignement et celles relevant de l'administration et n'a pas exploité ses banques de données conformément à leur but. De plus, il n'a pas respecté les directives de la Constitution fédérale, de la CEDH et de la LRens concernant la saisie et le traitement des données[10]. À l'avenir, la raison pour laquelle les données sont collectées et la finalité de leur traitement devront être claires et il devra être garanti que la limitation de la finalité est strictement respectée. Le SRC devra à l'avenir veiller à ce que les informations soient systématiquement attribuées aux bases de données concernées en fonction de leur finalité et que l'exception des tâches administratives ne soit pas utilisée comme échappatoire pour collecter et relier des données. Les données personnelles relatives à l'activité politique et à l'exercice de la liberté d'opinion, de réunion ou d'association, qui sont également pertinentes pour les services de renseignement, ne doivent en aucun cas être traitées pour l'accomplissement de tâches administratives.

Enfin, l'exception relative à l'accomplissement de tâches administratives ne doit pas être mentionnée à l'art. 5 al. 5 nLRens, mais à l'art. 5 al. 6 nLRens – parmi les autres exceptions. Il apparaît ainsi clairement que ces données personnelles sont en principe également couvertes par la limitation du traitement des données et qu'il ne s'agit que d'une exception au principe.

10 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, p. 34 N 137 s.

### 2.3 Art. 5 al. 6 let. b et art. 5 al. 8 nLRens

L'art. 5 al. 6 let. b et l'art. 5 al. 8 nLRens doivent garantir que seules les données des organisations et des personnes concernées peuvent être collectées et traitées.

Selon l'art. 5 al. 6 let. b nLRens, des données concernant une organisation ou une personne peuvent exceptionnellement être collectées et traitées s'il existe des indices concrets qu'une organisation ou une personne exerce ses droits afin de préparer ou d'exécuter des activités au sens de l'art. 6 al. 1 let. a nLRens. Dans ce contexte, il n'est pas clair quelles données et par rapport à qui ces données peuvent être collectées et traitées. Il convient de s'assurer que seules les données des organisations et des personnes concernées peuvent être collectées et traitées.

La même remarque vaut pour l'art. 5 al. 8 nLRens.

### 2.4. Art. 5 al. 6 let. c nLRens – Protection d'une organisation ou d'une personne

L'art. 5 al. 6 let. c nLRens doit être biffé.

Selon l'art. 5 al. 6 let. c nLRens, le SRC peut collecter et traiter des données sur une organisation ou une personne si cela est nécessaire pour la protéger contre une activité au sens de l'art. 6 al. 1 let. a LRens. Cette attitude paternaliste ne va pas avec un Etat de droit démocratique. Il convient d'ailleurs de souligner que le SRC a déjà justifié par le passé la saisie de données sur des organisations par cette approche, le SRC ayant saisi de nombreuses informations sur les organisations en question et ayant parfois commenté et classé leurs activités du point de vue des services de renseignement. Avec cette approche, les personnes actives au sein de l'organisation concernée perdent en grande partie la protection de pouvoir exercer leurs droits fondamentaux sans être observées par les services de renseignement[11].

### 2.5 Art. 45 al. 4 nLRens

L'art. 45 al. 4 nLRens doit être supprimé sans remplacement.

Selon l'art. 45 al. 4 nLRens, le SRC peut transmettre des données à l'étranger afin de vérifier s'il s'agit de données relevant du renseignement. Cette transmission de données ne se justifie pas, car la Suisse n'a plus aucun contrôle sur les données qui ont été mises à la disposition de services secrets étrangers. Il faut partir du principe que toutes les données, même si elles ont ensuite été effacées en Suisse, continuent d'être enregistrées à l'étranger. On sait depuis des années que la Suisse, en tant que partenaire Tier-B « focused cooperation », fait partie du cercle le plus étroit des services secrets entourant la NSA et les Five Eyes[12]. Depuis plus d'une décennie, de très grandes quantités de données

11 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, p. 31 N 124 et p. 33 s. N 133 ss.

12 https://www.elmundo.es/espana/2013/10/30/5270985d63fd3d7d778b4576.html.

sont enregistrées par ces services secrets[13]. On ne peut pas partir du principe qu'ils effaceront les données après les avoir reçues.

### 2.6 Art. 46 nLRens – Examen de l'applicabilité de l'art. 5 al. 5 nLRens

Même après l'anonymisation des données personnelles, il est possible de tirer des conclusions sur la personne ou l'organisation et donc de violer les droits fondamentaux.

L'art. 46 al. 1 phrase 2 nLRens doit être modifié comme suit : « Si tel est le cas et en l'absence d'exception au sens de l'art. 5 al. 6 ou 8, le SRC efface immédiatement les données personnelles ».

L'examen de l'admissibilité du traitement des données doit toujours être effectué dès leur saisie et non pas seulement lors de leur utilisation comme données de travail – sinon il y a une atteinte injustifiable aux droits fondamentaux. L'art. 46 al. 2 nLRens doit être modifié comme suit : « Pour les données personnelles provenant de sources accessibles au public et pour les données personnelles enregistrées séparément et provenant de mesures de recherche soumises à autorisation, cet examen a lieu immédiatement lors de la saisie ».

Selon l'art. 5 al. 6 let. a nLRens, le traitement des données qui tombent sous le coup de la restriction de traitement est exceptionnellement possible s'il est nécessaire selon l'art. 46 al. 1 nLRens. Selon l'art. 46 al. 1 nLRens, le SRC vérifie, en présence de données relevant du renseignement, si l'art. 5 al. 5 nLRens s'applique et, le cas échéant, anonymise les données personnelles. Le processus prévu par l'art. 5 al. 5 en relation avec l'art. 46 nLRens n'est globalement pas clair et constitue un renvoi circulaire.

Selon la loi sur la protection des données (LPD), les données sont personnelles lorsque les personnes auxquelles elles se rapportent sont identifiées ou identifiables (art. 3 let. a LPD). Une anonymisation par le SRC n'est donc suffisante que si les données relevant du renseignement ne permettent plus de déduire l'identité des personnes ou des organisations concrètes. Si, par exemple, une personne est mentionnée sans nom dans une donnée du service de renseignement mais que le contexte permet de trouver facilement de qui il s'agit en réalité, l'anonymisation est insuffisante.

En ce qui concerne les données personnelles provenant de sources accessibles au public et les données personnelles enregistrées séparément et provenant de mesures de recherche soumises à autorisation, l'art. 46 al. 2 nLRens prévoit en outre que l'examen ait lieu avant que le SRC n'utilise ces données comme données de travail. Il serait ainsi possible à l'avenir pour le service de renseignement de collecter et de stocker des informations sur des événements et des activités politiques, pour autant qu'il ne les attribue pas activement à une personne. Cela crée une base légale permettant de collecter n'importe quelle information et de ne vérifier que dans un deuxième temps si elle est réellement pertinente pour le SRC et si elle tombe sous le coup d'une exception. Avec ce principe, la limite de traitement de l'art. 5

13 https://www.heise.de/tp/features/XKeyscore-oder-die-totale-Informationshoheit-3399943.html ; https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

LRens est complètement vidée de sa substance. Il est en outre important de noter qu'aucun délai n'est prévu pour la vérification selon l'art. 46 al. 1 nLRens. Cette réglementation apparaît comme une validation *a posteriori* de la pratique actuelle du SRC, selon laquelle des données sont parfois conservées pendant des années et sans raison apparente dans les banques de données des services de renseignement. La DélCdG constate également que le SRC collecte de manière non systématique et aléatoire des données fausses, inutiles et sans intérêt pour la protection de l'Etat, qu'il les utilise de manière erronée et que l'effacement de ces données et de celles qui sont soumises à des restrictions de traitement ne fonctionne pas de manière fiable[14]. En 2010 déjà, la DélCdG demandait d'empêcher la collecte de ces informations[15]. Si des données tombent sous le coup de la limite de traitement des données, elles ne doivent pas être traitées du tout. Un éventuel effacement ultérieur n'y change rien.

## 3. Droit d'accès

### 3.1. Art. 63a al. 8 nLRens – Refus du droit d'accès

L'art. 63a al. 8 nLRens doit être supprimé. Le droit d'accès indirect par le PFPDT selon les art. 63a al. 3 ss nLRens ne remplace pas le recours effectif.

Conformément à l'art. 63a al. 8 nLRens, les renseignements visés aux al. 1 et 2 et les communications visées aux al. 3 et 4 ne peuvent pas faire l'objet d'un recours. Ce refus du droit d'accès et l'exclusion de tout recours contre celui-ci touchent aux droits fondamentaux et violent le droit à un recours effectif selon l'art. 13 CEDH. Aujourd'hui déjà, la pratique des services de renseignement en matière de renseignements n'est guère conforme à la CEDH[16]. Le Tribunal fédéral a constaté que le droit d'accès indirect selon les art. 64 s. LRens ne garantit pas en soi une possibilité de recours efficace selon l'art. 13 CEDH[17]. Il est inacceptable que ces droits déjà peu développés soient encore réduits par la révision. Même le rapport explicatif reconnaît que « 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 »[18].

Un droit d'accès qui fonctionne est d'autant plus important que le SRC a collecté des données de manière illicite ces dernières années. Dans son rapport annuel 2019[19], la DélCdG en arrive à la

14 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS). Rapport de la Délégation des commissions de gestion des Chambres fédérales, 21 juin 2010, FF 2010 7003 ; rapports annuels 2019, 2020 et 2021 de la DélCdG.
15 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS). Rapport de la Délégation des commissions de gestion des Chambres fédérales, 21 juin 2010, FF 2010 7003, p. 2 ss.
16 CourEDH, Klass et al. c. Allemagne, 5029/71, arrêt du 6 septembre 1978 ; CourEDH, Leander c. Suède, 9248/81, du 26 mars 1987.
17 ATF 147 I 280, consid. 9.2.4.
18 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 28.
19 Rapport annuel 2019 des Commissions de gestion et de la Délégation des Commissions de gestion des Chambres fédérales, 28 janvier 2020, FF 2020 2865, p. 2944.

conclusion que le SRC ne peut pas garantir que ses données sont traitées conformément aux prescriptions de la LRens. Ainsi, la conformité avec les limites fixées par l'art. 5 LRens n'a jamais été vérifiée pour une grande partie des données collectées. Et ce, bien que le traitement des données par les services de renseignement touche à des droits protégés par la CEDH et la Cst., comme l'autodétermination informationnelle en tant qu'élément du droit à la protection de la vie privée, la liberté d'expression et – dans la mesure où il s'agit de l'expression des opinions lors de manifestations – la liberté de réunion[20]. Si des données sont enregistrées de manière non-conforme au droit, il doit au minimum exister un droit d'accès qui fonctionne.

### 3.2. Art. 64 nLRens – Droit d'accès dans le cadre de la PES

La formulation de l'art. 64 nLRens doit également garantir que le droit d'accès vis-à-vis d'autres autorités fonctionne effectivement.

Selon l'art. 64 nLRens, l'obligation de fournir des renseignements sur les données personnelles contenues dans la présentation électronique de la situation (PES) incombe aux autorités fédérales et cantonales qui les ont enregistrées. Cela ne peut fonctionner que si ces autorités reçoivent effectivement les demandes de renseignements et s'acquittent de cette obligation. Ainsi, le rapport explicatif indique certes que le SRC transmet les demandes de renseignements aux autorités compétentes[21], mais un avis de droit montre que dans certains cas, il existe un grand nombre d'enregistrements PES provenant d'autres autorités, que les renseignements à ce sujet ont été refusés et qu'il n'était pas possible pour le SRC de déterminer de quelles autorités provenaient ces enregistrements[22]. L'art. 64 nLRens ne doit pas laisser de place à une telle argumentation, afin que le droit d'accès ne puisse pas être contourné.

## 4. Mesures de recherche soumises à autorisation (MRSA)

### 4.1. Art. 14 nLRens – Observation préventive secrète au moyen d'appareils de localisation

L'utilisation d'appareils de localisation sans l'accord d'un juge doit être supprimée. De manière générale, les observations – même lorsqu'elles sont réalisées sans appareil de localisation – doivent être requalifiées comme MRSA.

Conformément à l'art. 14 nLRens, le SRC pourrait, pendant la durée d'une observation, utiliser un appareil de localisation sur un véhicule ou un objet comme mesure de soutien, si cela est nécessaire pour assurer la continuité de la surveillance. La transmission des données devrait être interrompue

20 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, p. 49 N 188.
21 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 29.
22 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, p. 24 N 93.

lorsque l'observation est terminée ou que le contact visuel avec l'objet suivi est perdu de manière durable. Bien que l'observation soit effectuée en secret, elle ne fait pas partie des mesures de recherche soumises à autorisation. Le Conseil fédéral justifie cette renonciation à une procédure d'autorisation par le fait que l'observation représenterait une atteinte « relativement faible »[23] aux droits fondamentaux de la personne surveillée.

Ordonner une observation au moyen d'un appareil de localisation sans autorisation judiciaire est hautement problématique : dans un arrêt de principe, le Tribunal fédéral a constaté que la surveillance préventive par GPS sans autorisation judiciaire recèle un potentiel d'abus considérable. Même des abus isolés de cette possibilité de surveillance pourraient, dans certaines circonstances, conduire à un sentiment de méfiance généralisé et avoir ainsi des conséquences néfastes pour l'ordre libéral et démocratique[24]. L'opinion défendue par le Conseil fédéral, selon laquelle l'utilisation d'un appareil de localisation par le SRC se distinguerait de celle faite par la police, n'est pas convaincante.

Même – ou surtout – dans un lieu public, les personnes ont droit au respect de leur vie privée. Ainsi, selon la CourEDH, l'enregistrement de données par une administration étatique – même dans un lieu public – constitue une ingérence dans le droit à la vie privée[25]. Les personnes ne devraient en principe pas avoir à s'attendre à ce qu'un service secret enregistre leurs conversations et les conserve potentiellement pendant des décennies. Le fait que la loi actuelle et le projet de loi ne prévoient ni une procédure d'autorisation judiciaire ni une communication ultérieure à la personne surveillée signifie en outre que cette mesure n'est *de facto* soumise à aucun contrôle judiciaire. Une situation inacceptable dans un État de droit.

De plus, la gravité de l'ingérence dans les droits fondamentaux des personnes concernées ne résulte pas seulement de la recherche d'une information particulière mais également du recoupement de données provenant de plusieurs sources. L'observation peut entraîner des enregistrements visuels (photos, vidéos), et le SRC dispose d'un système de reconnaissance faciale, ce qui facilite l'identification des personnes et donc la mise en relation de ces données avec d'autres. Ainsi, même si les données sont recueillies dans l'espace public, leur conservation et leur mise en relation avec d'autres informations au sein d'une base de données gouvernementale aggrave dangereusement l'ingérence dans les droits fondamentaux.

Comme aucune information ultérieure n'est prévue, il n'est guère possible de vérifier si les limites déjà difficilement compréhensibles d'une telle surveillance ont été respectées et, le cas échéant, si les appareils de localisation ont effectivement été désactivés. La disposition n'est pas convaincante, notamment parce que les agents ne peuvent raisonnablement pas interrompre complètement une

23 Message concernant la loi sur le renseignement, 19 février 2014, FF 2014 2029, p. 2073.
24 ATF 147 I 103, consid. 17.5.2.
25 Parmi d'autres : CourEDH, Peck c. Royaume-Uni, 44647/98, arrêt du 28 janvier 2003, § 59 ; CourEDH, Perry c. Royaume-Uni, 63737/00, arrêt du 17 juillet 2003, § 38 ; Gonin Luc/Bigler Olivier, Convention européenne des droits de l'homme (CEDH) : commentaire des articles 1 à 18 CEDH, Berne, 2018, CEDH 8 N 54.

surveillance, même en cas de perte durable du contact visuel, car ils doivent pouvoir retrouver le véhicule pour démonter l'appareil de localisation.

Il faut encore relever que le SRC dispose aujourd'hui déjà de la possibilité de localiser une personne ou une chose (art. 26 al. 1 let. b LRens). Le nouvel art. 14 al. 3 nLRens et la réserve figurant à l'art. 26 al. 1 let. b nLRens *in fine* viennent donc exclusivement affaiblir la protection de la sphère privée des citoyens, alors même que la protection qu'apporte l'art. 14 LRens est déjà insuffisante à l'heure actuelle pour respecter les normes internationales auxquelles est soumise la Suisse.

### 4.2 Conditions d'autorisation

#### 4.2.1. Art. 27 al. 1 let. a ch. 1 nLRens– Élargissement à l'extrémisme violent

Les MRSA ne doivent pas être étendues à l'extrémisme violent.

L'extrémisme violent est une notion trop floue, dont il n'existe aucune définition légalement contraignante. Cela ne répond pas aux conditions de précision de la base légale qui doit justifier une ingérence dans les droits fondamentaux et contrevient donc aux exigences de l'art. 8 CEDH.

L'art. 27 al. 1 let. a ch. 1 nLRens prévoit que les MRSA puissent désormais être ordonnées pour toutes les menaces mentionnées à l'art. 19, al. 2 nLRens. Ainsi, les MRSA pourraient également être utilisées dans le domaine de l'extrémisme violent.

Toute surveillance secrète engendre une ingérence dans le droit à la vie privée protégé par l'art. 8 CEDH et doit donc être prévue par une loi prévisible et particulièrement précise[26]. La loi doit également énumérer les conditions[27] auxquelles les autorités peuvent surveiller une personne et définir les infractions et les catégories de personnes qui peuvent être surveillées[28].

Pourtant, le Conseil fédéral n'a jamais souhaité définir la notion d'« extrémisme violent », pour la prévention duquel des MRSA seraient désormais possibles. Déjà dans son message sur la LMSI, il indiquait que « le terme extrémisme ne peut pas non plus être cerné par une définition exhaustive » [29], de même que le terrorisme, et que pour cette raison « la loi évite sciemment de définir ces notions » [30].

---

26 GONIN Luc/BIGLER Olivier, Convention européenne des droits de l'homme (CEDH) : commentaire des articles 1 à 18 CEDH, Bern, 2018, CEDH 8 N 53 et 147 ; COUREDH, Guide sur l'article 8 de la Convention européenne des droits de l'homme, 31 août 2021, N 219.

27 COUREDH, Guide sur l'article 8 de la Convention européenne des droits de l'homme, 31 août 2021, N 16 ; COUREDH, Roman Zakharov c. Russie, 47143/06, arrêt du 4 décembre 2015, § 229 ; MEYER-LADEWIG Jens/ NETTESHEIM Martin, in MEYER-LADEWIG Jens/NETTESHEIM Martin/VON RAUMER Stefan (édit.), EMRK : Europäische Menschenrechtskonvention: Handkommentar, 4e éd., Baden-Baden, 2017, CEDH 8, N 34 et 37.

28 COUREDH, Roman Zakharov c. Russie, 47143/06, arrêt du 4 décembre 2015, § 231 ; COUREDH, Big Brother Watch et al. c. Royaume-Uni, 58170/13, 62322/14, 24960/15, arrêt du 13 septembre 2018, § 307 ; GONIN Luc/BIGLER Olivier, Convention européenne des droits de l'homme (CEDH) ; commentaire des articles 1 à 18 CEDH, Berne, 2018, CEDH 8, N 151.

29 Message concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire « S. o. S. – pour une Suisse sans police fouineuse », 7 mars 1994, FF 1994 II 1123, p. 1169.

30 Message concernant la loi fédérale sur des mesures visant au maintien de la sûreté intérieure ainsi que l'initiative populaire « S. o. S. – pour une Suisse sans police fouineuse », 7 mars 1994, FF 1994 II 1123, p. 1168.

L'art. 19 al. 2 LRens ne constitue donc « pas une définition légale »[31] des activités qui y sont listées mais une simple description des menaces.

Sur le fond, il faut donc retenir qu'il n'existe pas de définition légalement contraignante du terme « extrémisme violent ». La manière dont le SRC interprétera et appliquera cette notion à l'avenir est donc largement imprévisible et arbitraire. L'atteinte aux droits fondamentaux résultant des MRSA manque donc d'une base légale suffisamment précise[32]. Les simples descriptions de l'art. 19 al. 2 LRens sont trop floues pour constituer des définitions conformes aux exigences de la CEDH.

Comme l'ont montré les enquêtes sur la pratique des services de renseignement, la distinction entre les activités politiques légitimes et l'extrémisme violent relevant des services de renseignement n'a jamais fonctionné de manière fiable. Ainsi, les activités politiques protégées par les droits fondamentaux se sont toujours retrouvées dans le collimateur des services de renseignement. Jusqu'au scandale des fiches, cela concernait en particulier les « gauchistes », les « alternatifs », les « verts », les militants pour la paix, les activistes du tiers-monde, les mouvements féministes, les travailleurs étrangers, les mouvements antinucléaires et les groupements religieux, que les agents des services de protection de l'Etat considéraient comme potentiellement dangereux[33]. Plusieurs rapports de la DélCdG et des cas dans lesquels les personnes concernées ont pu consulter leurs données relevant du renseignement montrent clairement que, même après l'entrée en vigueur de la LMSI, par laquelle le législateur a voulu créer une base claire pour les activités de renseignement, le service de renseignement a continué à collecter des données sur des activités politiques protégées par les droits fondamentaux[34]. Un avis de droit, qui a examiné la pratique du SRC en matière de collecte d'informations, montre comment une ONG a été répertoriée par le service de renseignement dans 405 documents au total entre 1999 et 2019. L'ONG a été mentionnée à plusieurs reprises, à tort, dans le contexte de l'extrémisme de gauche et il lui a été reproché par endroits de ne pas s'être distanciée suffisamment clairement des actes de violence[35].

#### 4.2.2. Art. 27 al. 1 let. a ch. 2 nLRens – Surveillance au profit d'États étrangers

La possibilité d'ordonner des MRSA au profit d'États étrangers doit être supprimée. La Suisse risquerait ainsi de subir des pressions de la part d'autres États, ce qui mettrait en danger son indépendance et sa neutralité.

31 Message concernant la loi sur le renseignement, 19 février 2014, FF 2014 2029, p. 2082.
32 COUREDH, Guide sur l'article 8 de la Convention européenne des droits de l'homme, 31 août 2021, N 20.
33 Événements survenus au DFJP Rapport de la commission d'enquête parlementaire (CEP) du 22 novembre 1989 ; Événements survenus au DFJP Rapport complémentaire de la commission d'enquête parlementaire (CEP) du 29 mai 1990 ; https://www.bar.admin.ch/bar/fr/home/recherche/conseils-de-recherche/themes/nachrichtendienste--spione--landesverraeter-und-staatsschutz-in-/die-politische-polizei-und-der-staatsschutz-in-der-schweiz-.html.
34 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS). Rapport de la Délégation des commissions de gestion des Chambres fédérales, 21 juin 2010, FF 2010 7003 ; rapports annuels 2019, 2020 et 2021 de la DélCdG.
35 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, notamment p. 23 ss N 89 ss.

Selon le projet de loi, des mesures de recherche soumises à autorisation pourraient également être ordonnées à la demande d'États étrangers en cas de « menace concrète pour des intérêts internationaux importants en matière de sécurité ». Les États étrangers pourraient ainsi demander à la Suisse de mettre en œuvre des mesures de surveillance contre des organisations ou des individus qu'ils considèrent comme des terroristes ou des extrémistes selon leur propre définition.

Les recherches risquent aussi de concerner des personnes se situant sur le territoire d'un autre Etat mais utilisant un système de communication en Suisse (p. ex. une adresse courriel chez un prestataire suisse). Cela posera problème pour la communication ultérieure de la mesure à la personne concernée et cette difficulté particulière n'est pas réglée dans le projet.

La mise en place de MRSA à la demande d'États étrangers est en contradiction avec le principe de la préservation de l'indépendance de la Suisse et de sa neutralité (art. 54 Cst.). En particulier lorsque la sécurité de la Suisse n'est pas en jeu, mais qu'il pourrait simplement s'ensuivre – sans autre définition – une « réaction négative des États concernés » à l'égard de la Suisse ou qu'une « action internationale est indispensable » (art. 27 al 1 let. a nLRens), la Suisse court le risque de se rendre vulnérable au chantage. Ainsi, des États tiers pourraient menacer la Suisse de mesures de rétorsion si le SRC n'agissait pas dans l'intérêt de ces États. Du point de vue de la politique de souveraineté et de neutralité, une disposition aussi étendue ne semble pas défendable et la Suisse risque d'être impliquée de manière croissante et incontrôlable dans des conflits internationaux.

### 4.3. Procédure d'autorisation

#### 4.3.1. Art. 29 nLRens– Demande de MRSA

Le SRC doit toujours fournir au Tribunal administratif fédéral (TAF) son dossier *complet* et non seulement les « pièces *essentielles* ».

La personne surveillée doit avoir un représentant ayant un accès complet à la procédure et aux documents de l'autorisation et habilité à déposer des conclusions devant le TAF au nom de la personne concernée.

Des statistiques détaillées (pas uniquement le nombre de mesures autorisées au refusées) sur le processus d'autorisation doivent être publiées.

L'art. 29 al. 1 let. g nLRens prévoit que le SRC remet au TAF les « pièces essentielles au traitement de la demande [d'autorisation] ». Dans son message sur la LRens, le Conseil fédéral indiquait que le SRC devait présenter au TAF « toutes les indications permettant de vérifier si la mesure répond aux exigences légales, à savoir la description des indices effectifs de menace concrète pour la sûreté intérieure ou extérieure de la Suisse, la justification de la proportionnalité de la mesure [...] »[36].

36 Message concernant la loi sur le renseignement, 19 février 2014, FF 2014 2029, p. 2092.

Ceci n'est pas suffisant pour assurer au juge une vision éclairée de la situation car les indices choisis par le SRC et fournis seuls peuvent donner une vision biaisée de la situation, le risque étant que le TAF ne dispose en fait que des éléments favorables à la mesure. L'effet de la procédure d'autorisation judiciaire des MRSA est de toute façon limité par nature, puisque ces mesures visent à obtenir des renseignements, parfois sur la base de soupçons minces, du moins dans un premier temps. Le contrôle judiciaire ne pourra donc porter que sur la question de savoir si le SRC fait valoir l'existence des conditions de la mesure (éventuellement sur la base de suppositions), et non sur l'existence effective des faits invoqués par le SRC. Même si le juge peut demander des compléments au dossier, cela implique que son attention soit particulièrement attirée par un élément du dossier[37].

Il faut rappeler que le délai pour délivrer l'autorisation est court et que cela se prête donc mal à des allers-retours de dossiers entre le TAF et le SRC. Pour que le TAF puisse prendre dans les temps une décision pleinement informée, il est impératif que le SRC fournisse l'intégralité de son dossier au TAF.

Quoi qu'il en soit, il existe un déséquilibre flagrant entre les moyens dont disposent le SRC et la personne concernée puisque cette dernière est absente de la procédure. Pour assurer la défense de ses intérêts, il faut lui nommer un représentant chargé de faire contrepoids aux représentants du SRC.

Enfin, il faut rappeler que les décisions du TAF en la matière ne sont pas publiées (art. 5 al. 1 Règlement du 21 février 2008 du Tribunal administratif fédéral relatif à l'information[38]). Pour qu'un contrôle public et démocratique minimal puisse avoir lieu, il est donc impératif de fournir des données statistiques. Le SRC publie dans son rapport annuel uniquement le nombre de mesures réalisées. Le nombre annuel de mesures autorisées, autorisées partiellement, sous condition, avalisées, retirées, refusées, etc. doit également être publié de façon à apprécier l'effectivité du contrôle judiciaire. La justification des décisions devrait également être indiquée, notamment pour savoir s'il s'agit de terrorisme, d'extrémisme violent etc. Une fois l'opération terminée, les décisions devraient également être publiées comme tous les autres arrêts du TAF.

#### 4.3.2. Art. 29a al. 5 nLRens – MRSA à l'étranger

Le TAF doit se prononcer sur toutes les MRSA, qu'elles soient effectuées sur sol suisse ou à l'étranger

Même si l'exécution d'une surveillance par le SRC à l'étranger a lieu avec l'autorisation de l'Etat concerné, elle doit être soumise au contrôle du juge.

L'art. 29a al. 5 nLRens implique que, premièrement, des MRSA sont également effectuées à l'étranger et qu'un contrôle judiciaire par le TAF ne serait pas nécessaire dans ce cas. En ce qui concerne l'intrusion dans des systèmes informatiques, avec la référence à l'art. 37 nLRens qui s'applique à la place, il apparaît

37 SCHWERI Florian, Le respect de la vie privée des personnes concernées par une mesure de surveillance secrète: analyse du droit suisse au regard de la Convention européenne des droits de l'homme, Université de Genève, Master, 2021, [disponible sur : https://archive-ouverte.unige.ch/unige:159835], p. 14.

38 RS 173.320.4.

que le Conseil fédéral ou le chef du DDPS déciderait de l'exécution de telles mesures et, en cas d'urgence, la direction du SRC (art. 37 al. 3 nLRens).

L'exécution de MRSA à l'étranger est extrêmement problématique du point de vue du droit international public à la lumière des principes de territorialité et de souveraineté. A quelques exceptions près, de telles pratiques sont inadmissibles. Dans l'ATF 146 IV 36, le Tribunal fédéral a établi qu'en vertu du principe de territorialité, de telles mesures, même si elles ont été ordonnées valablement pour la Suisse, ne peuvent en principe être exécutées à l'étranger que si cela est compatible avec le droit international ou, à défaut, si l'Etat concerné a donné son accord préalable conformément aux règles de l'entraide judiciaire internationale.

En outre, on ne voit pas pourquoi le contrôle judiciaire devrait être supprimé lorsqu'une MRSA est effectuée ou poursuivie à l'étranger. Ainsi, il ne serait pas justifié que, par exemple, la prolongation d'une MRSA ne soit pas soumise au TAF parce que la personne se trouve à ce moment-là en vacances ou en voyage d'affaires à l'étranger. Il ne serait pas non plus admissible de ne pas informer ultérieurement la personne concernée ou de ne l'informer que de la partie de la surveillance qui a été effectuée en Suisse. Limiter l'autorisation judiciaire aux cas où le SRC agit sur le territoire suisse n'est pas défendable. Cela signifierait également que la Suisse protège mieux les droits fondamentaux de ses citoyens sur son propre territoire qu'à l'étranger. Ceci est particulièrement problématique pour les Suisses de l'étranger. Le projet de loi ne contient aucune disposition interdisant, par exemple, d'intercepter et d'ouvrir les enveloppes de vote des Suisses de l'étranger. Comme les personnes surveillées peuvent aussi être des citoyens d'un autre Etat, la Suisse court le risque d'être poursuivie devant la CourEDH par le biais d'une plainte interétatique selon l'art. 33 CEDH.

### 4.4. Art. 29b et 30 nLRens – Durée de l'autorisation et prolongation de la MRSA

Des délais maximaux doivent être fixées par la loi entre la demande et l'examen judiciaire, respectivement l'autorisation judiciaire, de la MRSA et sa mise en œuvre concrète.

Il doit être prévu expressément que, même si le SRC renonce finalement à mettre en œuvre la mesure, cette dernière doit néanmoins être communiquée à la personne concernée

Il faut prévoir que la prolongation d'une MRSA doit être approuvée avant l'expiration de la mesure en cours. La poursuite d'une MRSA au-delà de la durée autorisée est, dans tous les cas, interdite.

Il faut renoncer à l'allégement de la procédure d'aval en cas de prolongation. De même, la notion d'« extension limitée » doit être supprimée. Chaque prolongation ou extension de la MRSA doit suivre un processus complet en bonne et due forme.

Le projet de loi prévoit que l'approbation des MRSA prend effet à une date fixée par le TAF. En ce qui concerne l'efficacité des MRSA, il est toutefois nécessaire de fixer certains délais légaux. Par exemple,

entre l'autorisation du juge et l'exécution effective de la mesure, les circonstances peuvent changer de manière déterminante. En outre, plus l'évaluation d'une menace concrète est faite longtemps à l'avance, plus elle devient une spéculation et donc une simple probabilité qui ne peut pas justifier une telle atteinte aux droits fondamentaux.

Si les circonstances changent effectivement depuis l'autorisation, le SRC doit en outre avoir la responsabilité d'informer le tribunal de cette circonstance afin que l'autorisation puisse être révoquée. Dans ce contexte, il est particulièrement important que la personne concernée soit informée de la mesure même si celle-ci a été levée avant son exécution.

Si une prolongation de la MRSA est nécessaire, il suffirait, selon l'art. 29b nLRens, que le SRC dépose sa demande de prolongation auprès du TAF avant l'expiration de la mesure en cours. La possibilité de poursuivre les MRSA jusqu'à ce qu'une décision du TAF concernant la prolongation soit rendue ouvre un potentiel d'abus non négligeable. L'objectif de l'autorisation judiciaire est justement de limiter la durée des MRSA à la lumière du principe de proportionnalité. Afin de prévenir les abus, la loi doit prévoir explicitement la solution inverse, à savoir que, dans le cadre de la décision d'approbation, la poursuite d'une MRSA au-delà de la durée autorisée n'est pas permise. La poursuite d'une mesure doit dans tous les cas être soumise à l'approbation du TAF.

Enfin, l'obligation de détruire les données en cas de refus de l'autorisation ou de la prolongation, prévue à l'art. 29b al. 3 nLRens, n'est pas non plus suffisante, en particulier si le SRC a entre-temps transmis des données à d'autres services. Si la possibilité susmentionnée de poursuivre la MRSA avant l'obtention de l'autorisation du juge devait être maintenue, la loi devrait garantir que tant que l'autorisation et l'aval de la prolongation n'ont pas été accordées, le SRC ne peut pas transmettre les données à d'autres instances.

Il n'est pas non plus justifié que les chefs du DFJP et du DFAE ne doivent plus être consultés lors de la prolongation des MRSA. Cette simplification semble avoir lieu en premier lieu parce que la consultation représente une charge pour les chefs du DFAE et du DFJP. On oublie cependant que chaque adresse (art. 30 al. 4 let. a nLRens) ou objet supplémentaire « en possession de la personne déjà sous surveillance » (art. 30 al. 4 let. b-d nLRens) peut également être la propriété ou destinée à l'usage d'une autre personne et peut donc potentiellement inclure de nouvelles personnes concernées. En outre, une surveillance prolongée ou étendue signifie une atteinte encore plus grave aux droits de la personne surveillée et en aucun cas, comme on le suggère, une gravité identique à la première mesure. Le gain de temps minimal est sans commune mesure avec la gravité de l'atteinte aux droits fondamentaux que représente une MRSA pour les personnes concernées. Comme la question de la proportionnalité est de plus en plus importante avec la durée d'une mesure, les conditions et les mécanismes de contrôle devraient également être renforcés et non pas affaiblis. Enfin, selon l'art. 30 al. 3 nLRens, le chef du DDPS ne devrait plus consulter les chefs du DFJP et du DFAE, en cas d'« extensions limitées ». Mais de fait, ces extensions constituent également une surveillance supplémentaire qui ne peut être autorisée

que si toutes les garanties de procédure sont respectées. Le rapport explicatif tente de rassurer en soulignant que la consultation préalable pourrait toujours se faire sur une base volontaire. Mais dans les faits, ces services ne sont informés qu'*a posteriori* et cette indication n'est donc rien de plus que de la poudre aux yeux.

### 4.5. Art. 33 nLRens – Information à la personne surveillée

La possibilité de *renoncer* définitivement à l'information doit être supprimée. Conformément à la CEDH, à la Cst. et à la jurisprudence du Tribunal fédéral, seul un report limité dans le temps (et éventuellement renouvelable) est acceptable.

Il convient de ne conserver que la possibilité de *différer* l'information pendant trois mois. Ce report doit être soumis à la procédure d'approbation et de validation.

La communication à la personne concernée après la fin de la surveillance est un élément essentiel dans un Etat de droit. Sans être informée *a posteriori* de la surveillance, la personne concernée n'a pas de possibilité effective de recours au sens de l'article 13 CEDH et elle ne peut ni constater ni faire réparer d'éventuelles violations de son droit à la vie privée. La notification n'est certes pas toujours possible immédiatement, mais elle doit avoir lieu « dès que la notification peut être donnée sans compromettre le but de la restriction »[39].

La LRens prévoit la possibilité de « déroger » de manière définitive à l'information. Or, selon la jurisprudence du Tribunal fédéral, une telle renonciation durable à l'information n'est pas admissible[40]. Seul un report bref et limité dans le temps de la communication est possible.

Selon l'art. 33 al. 2bis nLRens, le délai de report des communications serait étendu de trois à six mois. Compte tenu de la gravité de l'atteinte aux droits de la personne concernée, cela est inapproprié. Le report de l'information « jusqu'à la survenue d'un événement particulier » est en outre problématique si l'événement n'est pas décrit clairement, s'il ne se produit pas ou si l'autorité qui en est responsable oublie d'en informer le SRC. Un contrôle régulier à intervalles rapprochés est le seul moyen de s'assurer que l'information ne sera pas oubliée et que les droits de la personne concernée sont respectés.

Le Conseil fédéral exerce une surveillance sur le SRC et est politiquement responsable de ses actions. Il est donc justifié que toute restriction de l'obligation de communiquer soit soumise à la procédure d'aval et pas seulement à l'autorisation du TAF. L'idée d'un « report nécessaire en raison des relations que la Suisse entretient avec l'étranger » (al. 4) pourrait en outre poser des problèmes d'interprétation.

39 CourEDH, Klass et al. c. Allemagne, 5029/71, arrêt du 6 septembre 1978, § 58 ; CourEDH, Roman Zakharov c. Russie, 47143/06, arrêt du 4 décembre 2015, § 286 à 290.

40 ATF 109 Ia 273, consid. 12b *in fine* « [Es ist nicht unverhältnismässig] von der nachträglichen Benachrichtigung der Betroffenen abzusehen, soweit und solange eine solche den Zweck der durchgeführten Überwachungsmassnahmen gefährden würde » (nous soulignons) ; Kreyden Aileen, Das Nachrichtendienstgesetz im Spannungsverhältnis zwischen Geheimhaltungsinteresse und Recht auf Rechtsschutz: wie kann bei geheimen Überwachungsmassnahmen Rechtsschutz gewährt werden ?, Zurich, 2017, N 59.

### 4.6. Art. 50 nLRens – Traitement des données recueillies lors d'une mesure de recherche soumise à autorisation

#### 4.6.1. Tri et destruction des données

Une instance indépendante doit trier les données et détruire celles qui ne sont pas nécessaires – avant de les transmettre au SRC.

Le tri des données non pertinentes du point de vue du renseignement doit avoir lieu avant la transmission des données au SRC, car les communications surveillées peuvent par exemple contenir des données sensibles ou protégées par le secret professionnel.

L'art. 50 al. 1 nLRens prévoit que les données collectées dans le cadre d'une MRSA doivent être examinées et, le cas échéant, détruites au plus tard à la fin d'une opération (qui peut donner lieu à plusieurs MRSA). Selon le texte de loi actuel, elles doivent être détruites dans les 30 jours suivant la fin de la mesure individuelle. Plus les données sont conservées longtemps, plus le risque pour les personnes concernées d'être lésées dans leurs droits fondamentaux est grand. Dans ce contexte, il convient de rappeler qu'une surveillance entraîne souvent la collecte d'informations sur des personnes qui ne sont pas visées par la surveillance (p. ex. les interlocuteurs de la personne surveillée) et donc des atteintes à leur sphère privée.

Selon la jurisprudence de la CourEDH, des règles doivent exister sur le traitement des informations recueillies lors d'une surveillance secrète[41]. Les données sans lien avec l'infraction, respectivement la menace, qui a donné lieu à la surveillance devraient être détruites aussitôt[42]. Les informations doivent déjà être protégées au stade de leur collecte et des obligations de sécurité à appliquer par les tiers éventuellement impliqués (par ex. Service SCPT, banques, etc.) doivent être prévues afin de protéger les données. En ce qui concerne le Service SCPT, les données qui, selon le SRC, devraient être effacées doivent l'être non seulement dans les banques de données du SRC, mais aussi dans le système de traitement du Service SCPT. Afin de protéger pleinement les droits des personnes concernées, le tri et l'effacement de toutes les données devraient être réalisés par une instance indépendante, avant leur transmission au SRC.

#### 4.6.2. Art. 50 al. 2 nLRens – Données protégées par le secret professionnel

Le juge qui effectue le tri doit se récuser dans toutes les autres affaires pour lesquelles il a pris connaissance de données couvertes par le secret professionnel au cours de la procédure de tri.

41 CourEDH, Roman Zakharov c. Russie, 47143/06, arrêt du 4 décembre 2015, § 253 à 256 ; CourEDH, Kennedy c. Royaume-Uni, 26839/05, arrêt du 18 mai 2010, § 164.

42 CourEDH, Roman Zakharov c. Russie, 47143/06, arrêt du 4 décembre 2015, § 258.

Les données couvertes par le secret professionnel doivent être immédiatement détruites, qu'elles aient été recueillies en surveillant directement la personne soumise au secret professionnel ou toute autre personne qui était en communication avec une personne soumise au secret. Le statut de la personne surveillée (personne surveillée parce que le SRC recherche des informations sur elle ou personne surveillée en tant que tiers [art. 28 LRens]) est également indifférent sur l'obligation de détruire les données.

Conformément à l'art. 50 al. 2 nLRens, lors de MRSA visant des personnes soumises au secret professionnel, le tri et la destruction des données non nécessaires sont effectués sous la direction du TAF.

Dans un premier temps, il est essentiel que ce tri soit effectué avant que le SRC n'ait accès aux données. C'est la seule façon de garantir que le SRC ne puisse consulter que les données qui lui sont nécessaires *et* qui ne sont pas protégées par le secret professionnel. En revanche, le juge du TAF qui procède au tri prend nécessairement connaissance d'informations confidentielles. En particulier lors de la surveillance des avocats, il existe donc un risque que les juges obtiennent des informations sur d'autres procédures dans lesquelles les avocats surveillés représentent des clients devant le TAF. Les juges ne doivent en aucun cas pouvoir profiter de telles informations pour le traitement d'autres affaires et doivent se récuser dans ces cas.

En outre, dans le cas des MRSA, le tri et la destruction se limitent explicitement, vis-à-vis des personnes soumises au secret professionnel, aux « données qui ne sont pas nécessaires ». Et ce, bien qu'il soit tout à fait concevable que des données « nécessaires » du point de vue des services de renseignement soient en même temps couvertes par le secret professionnel. Si ces données sont néanmoins traitées par le SRC, cela viderait le secret professionnel de sa substance. Selon la deuxième phrase de l'art. 50 al. 2 nLRens, les données recueillies lors de la surveillance d'une autre personne et pour lesquelles une personne soumise au secret professionnel a le droit de refuser de témoigner doivent en outre être effacées, indépendamment de leur caractère nécessaire. La protection est donc plus large dans ce cas. En ce sens, il est inacceptable que les données des personnes soumises au secret professionnel soient mieux protégées lorsqu'elles proviennent de la surveillance d'une autre personne.

La loi doit donc garantir que toutes les données soumises au secret professionnel sont détruites, quelle que soit la personne visée par la surveillance. En outre, en cas de surveillance directe de personnes soumises au secret professionnel, toutes les autres données non « nécessaires » doivent également être effacées. En outre, la loi doit explicitement préciser que le tri et la destruction doivent être effectués avant que le SRC n'ait accès aux données : celui-ci ne doit avoir accès qu'aux données qui remplissent la double condition de ne pas être soumises au secret professionnel *et* d'être « nécessaires ». Enfin, il faut préciser qui est responsable du tri et de la destruction lorsque la personne surveillée n'est pas soumise au secret professionnel.

Il convient de souligner qu'un tri ultérieur ne suffit pas à préserver les droits découlant du secret professionnel et de la protection des sources, mais qu'il faut s'assurer que – sauf cas exceptionnels justifiés – les données soumises au secret professionnel ou à la protection des sources ne peuvent pas être saisies par le SRC.

### 4.7. Art. 83 nLRens – Voies de droit

Les données transmises doivent être détruites si la décision, immédiatement exécutoire, ordonnant leur transmission est finalement invalidée.

Il faut préciser les informations que le SRC doit fournir à la personne concernée après une MRSA.

La répartition des compétences judiciaires en matière d'autorisation et de recours doit être revue.

Si des données sont transmises mais que la décision se révèle invalide, les données doivent être détruites immédiatement.

Pour être effectif, le recours doit pouvoir se baser sur des informations précises et il faut donc détailler quelles données doivent être fournies après coup à la personne surveillée. Le TAF ne doit pas autoriser les surveillances et traiter lui-même les recours contre ses propres décisions.

L'art. 83 al. 2 nLRens prévoit que les recours contre certaines décisions n'ont pas d'effet suspensif. Cela concerne notamment les cas où le SRC ordonne à une personne ou à une autorité de lui fournir des renseignements. Cette disposition doit être complétée en ce sens que les données mises à disposition doivent dans tous les cas être détruites si la décision du SRC est déclarée invalide ultérieurement suite à un recours.

Selon l'art. 83 al. 3 LRens, un recours contre une MRSA est possible dans les 30 jours suivant la notification de la mesure à la personne concernée. Cette disposition n'est toutefois pas satisfaisante, car elle ne prévoit qu'une possibilité vaguement formulée de recours contre « l'ordre d'effectuer une mesure de recherche soumise à autorisation ». Il serait au contraire nécessaire que l'ordre interne du SRC ainsi que l'autorisation du TAF et la décision d'aval du Conseil fédéral puissent être explicitement contestés. Comme une opération pourrait potentiellement avoir duré plusieurs années, le délai de recours de 30 jours est en outre beaucoup trop court. Il n'accorde pas suffisamment de temps à la personne concernée pour prendre connaissance de tous les éléments de la surveillance et les vérifier – surtout s'ils ne sont pas mis à sa disposition dès le début.

Selon l'art. 33 nLRens, la communication d'une mesure à la personne concernée ne contient en outre que le type, le motif et la durée de la surveillance. Cette simple description de la mesure effectuée ne suffit cependant pas pour juger de sa légalité. Il faudrait plutôt mentionner la procédure d'autorisation (ordinaire ou urgente), la date de la demande et de l'autorisation, le nombre de prolongations ainsi que

les motifs de celles-ci[43]. En rédigeant la lettre d'information, le SRC risque d'omettre des éléments qui lui semblent sans importance mais qui sont essentiels du point de vue de la personne concernée pour faire valoir ses droits. Pour ces raisons, il est impératif que le SRC communique également à la personne concernée l'ordre de surveillance, les décisions du TAF et du Conseil fédéral ainsi que, le cas échéant, toute information complémentaire utile.

Le fait que le TAF soit compétent pour autoriser la mesure puis pour connaître du recours contre sa propre décision pose un problème de conflit d'intérêt. Ceci est encore plus problématique lorsque la personne surveillée est soumise au secret professionnel. Dans ce cas, le TAF a autorisé la mesure, effectué le tri des informations et traite le recours. Pour peu que la personne ait fait valoir son droit d'accès indirect aux données personnelles par le passé, c'est également le TAF qui aura statué sur sa requête. Le TAF avait lui-même soulevé ce problème de conflit d'intérêt dans la procédure de consultation sur la première version de la LRens en suggérant de confier ces recours à un autre tribunal. Cette critique reste d'actualité.

### 4.8 Art. 26 al. 1 let. f et g nLRens – surveillance des relations bancaires et des transactions financières

La surveillance secrète des relations bancaires et des transactions financières doit être supprimée dans sa forme indéterminée.

L'art. 26 al. 1 let. f et g nLRens prévoit comme MRSA l'obtention de renseignements concernant les relations entre une personne physique ou morale et des intermédiaires financiers ou des négociants (art. 26 al. 1 let. f nLRens) ainsi que la surveillance de ces relations (art. 26 al. 1 let. g nLRens). Les effets de ces deux mesures ne doivent guère être sous-estimés et soulèvent diverses questions de doctrine juridique.

Il est frappant de constater que cette mesure - contrairement aux autres MRSA de plus grande portée (en particulier l'exploration radio et du réseau câblé, l'intrusion dans des systèmes informatiques, etc.) ne trouve aucune réglementation matérielle dans la loi. Au contraire, elle n'est mentionnée qu'en passant, dans l'énumération de l'obligation d'autorisation, ce qui rend le texte extrêmement vague. Contrairement aux art. 284 et 285 CPP (surveillance des relations bancaires), il manque une délimitation minimale de la mesure selon la nLRens concernant ses conditions et sa portée. De plus, la mesure n'est pas limitée à la personne visée, mais peut également s'étendre à des tiers. Ainsi, le compte bancaire d'un avocat représentant des personnes accusées de terrorisme ou d'extrémisme violent pourrait faire l'objet d'une surveillance secrète dans le but de surveiller les expéditeurs des paiements d'honoraires et d'explorer le réseau de la personne cible concernée.

43 SCHWERI Florian, Le respect de la vie privée des personnes concernées par une mesure de surveillance secrète: analyse du droit suisse au regard de la Convention européenne des droits de l'homme, Université de Genève, Master, 2021, [disponible sur : https://archive-ouverte.unige.ch/unige:159835], p. 15 s.

Avec cette mesure, les banques sont considérablement mises au service du SRC (et, le cas échéant, des services de renseignement étrangers), ce qui sape le secret bancaire et le secret des affaires. De même, il manque une réglementation concernant le droit de ne pas s'auto-incriminer des intermédiaires financiers et des négociants concernés, telle qu'elle existe par analogie dans le CPP (art. 285 al. 2 CPP).

Selon le Conseil fédéral, cette mesure doit viser par exemple « aux entreprises, aux organisations idéologiques ou aux institutions religieuses ». La mesure vise expressément à pouvoir ordonner une surveillance dans les cas où il n'existe *pas* de soupçons fondés (par exemple de financement du terrorisme). Ainsi, une éventuelle menace doit pouvoir être identifiée et mieux évaluée[44]. En outre, la mesure vise explicitement à contourner le principe de spécialité interétatique : les informations échangées au niveau international dans un but précis pourraient alors être utilisées dans le cadre de la nLRens – et même, le cas échéant, dans d'éventuelles procédures pénales ultérieures – même si elles vont à l'encontre de ces buts et conditions.

Dans l'ensemble, la mesure s'avère dans ce contexte sans limite, ce qui n'est pas acceptable du point de vue de l'Etat de droit compte tenu des droits fondamentaux concernés, à savoir la liberté économique, la liberté personnelle, la sphère privée et l'autodétermination informationnelle ainsi que le secret bancaire et le secret des affaires.

C'est précisément parce qu'il est prévu d'étendre la MRSA au domaine de l'« extrémisme violent » que cette mesure semble particulièrement problématique au regard de la liberté d'opinion, de réunion et d'association. Ceci d'autant plus que l'instrument doit être utilisé de manière très large, par exemple pour l'« exploration du réseau » concernant les grandes manifestations ou pour la clarification du soutien financier de personnes et d'organisations[45]. Un « comportement violent » – du moins selon la définition du « concordat sur le hooliganisme », sur laquelle les autorités cantonales d'exécution se basent le cas échéant – peut déjà consister en une *contrainte*, ce qui permettrait d'y inclure la forme d'action « tapis humain ». Comme la contrainte est classée parmi les « crimes ou délits contre la liberté », une « menace concrète » au sens de l'art. 27 al. 1 nLRens (en relation avec l'art. 19 al. 2 nLRens) risquerait d'être admise plutôt facilement. Ainsi, une organisation qui utilise ce type d'actions pourrait être la cible d'une surveillance secrète des transactions financières. De même, la novelle semble taillée sur mesure pour mettre en place une surveillance des transactions financières des réseaux de soutien qui, à la suite d'une action ou d'une manifestation, soutiennent des personnes concernées par des mesures policières ou des poursuites pénales. Une seule surveillance de ce type – par exemple d'un *crowdfunding* – peut placer des centaines, voire des milliers de personnes et de donateurs dans le collimateur du SRC.

La surveillance secrète des relations bancaires et des transactions financières s'avère également particulièrement problématique à la lumière de l'art. 27 nLRens, qui permettra à l'avenir d'ordonner des MRSA même en cas de menace diffuse contre des « intérêts internationaux importants en matière de

44 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 9.
45 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 10.

sécurité » ou de menace de « réactions négatives » de la part d'États tiers à l'égard de la Suisse. Cela ouvre un risque considérable pour la neutralité et l'indépendance de la Suisse, par exemple dans la mesure où des États tiers pourraient exiger de la Suisse qu'elle surveille les transactions de certaines cibles étrangères et la menacer de conséquences négatives en cas de refus. Ainsi, une grande puissance mondiale pourrait, dans le cadre d'un conflit armé, exiger de la Suisse qu'elle surveille les transactions financières des représentants d'une partie belligérante, considérée par cet Etat comme terroriste.

Enfin, il convient de souligner que l'objet de la réglementation proposée ici se recoupe avec celui d'autres lois (en particulier le CP, le CPP, la LBA, la MPT, la LB). Il n'y a pas lieu d'ajouter aux dispositions légales existantes une nouvelle disposition dans la LRens qui pose problème du point de vue de l'Etat de droit.

### 4.9 Art. 28 nLRens – Mesures de recherches soumises à autorisation contre des tiers

Il faut renoncer à la suppression de l'art. 28 al. 2 LRens. Les MRSA ne doivent pas être réalisées à l'égard de tiers soumis au secret professionnel, à la protection des sources ou à d'autres obligations de garder le secret.

L'art. 28 nLRens prévoit que des tiers non impliqués puissent désormais être explicitement visés par les MRSA, même si des données sont transmises « vers cet emplacement » – c'est-à-dire vers eux en tant que simples destinataires – ou reçues ou conservées par eux. Cela a de graves conséquences : à l'avenir, les canaux de communication de toutes les personnes se trouvant dans l'environnement d'une personne cible (famille, amis, etc.) pourraient devenir les cibles potentielles de MRSA. L'accent devrait être mis sur les tiers auxquels sont confiées des données particulièrement confidentielles. La condition des « indices fondés » ne permet pas de limiter suffisamment la mesure.

Il est particulièrement grave que les mesures prévues par le projet – en raison de la suppression prévue de l'art. 28 al. 2 LRens – s'appliquent également à des tiers soumis au secret professionnel, à la protection des sources s'agissant des journalistes ou à d'autres obligations de garder le secret (art. 171-173 CPP). Cela représente une grave érosion des dispositions de l'État de droit en matière de protection du secret, avec des conséquences différentes selon les cas. Les trois domaines présentant les conséquences plus graves sont brièvement abordés à titre d'exemple :

1 le secret professionnel de l'avocat : l'exercice d'un mandat d'avocat suppose une proximité et une relation de confiance particulières ; sans la garantie de cette confidentialité, l'exercice des obligations professionnelles de l'avocat serait rendu impossible. C'est précisément lorsque des personnes se trouvent à l'étranger que des entretiens personnels ne sont pas possibles, raison pour laquelle la communication se fait régulièrement par des canaux susceptibles d'être surveillés par une MRSA. La possibilité légale de surveiller ces canaux suscitera – en particulier s'agissant des avocats – un intérêt marqué du SRC mettre en œuvre concrètement de telles

mesures. En conséquence, tout avocat exerçant dans un domaine intéressant pour le SRC (terrorisme, mais aussi extrémisme violent) devrait s'attendre à ce que tous les canaux de communication (en particulier téléphone, e-mail, etc.) soient surveillés au moyen d'une MRSA. Ainsi, par cette surveillance étatique, non seulement les clients représentés deviennent « hors-la-loi », mais aussi les défenseurs et avocats correspondants. La perspective d'un « triage sous la surveillance du Tribunal administratif fédéral »[46] ne peut en aucun cas dissiper les graves doutes qui y sont liés.

2 Secret médical : l'érosion du secret professionnel dans le domaine médical est tout aussi problématique. Le conseil et le traitement des patients supposent que le corps médical prenne connaissance d'informations sensibles concernant la sphère privée et intime. Les personnes concernées ne fournissent toutefois de telles informations que si la confidentialité est garantie. L'obligation absolue de confidentialité est donc une condition nécessaire à la réussite du diagnostic et du traitement[47].

3 Protection des sources des journalistes : La protection des sources journalistiques est une pierre angulaire de la liberté de la presse et garantit ainsi la liberté d'information[48]. Si les journalistes doivent s'attendre, lors de la simple correspondance avec des personnes qui pourraient être des cibles d'une surveillance selon la nLRens, à ce que toute leur correspondance soit soumise à une surveillance ou à une MRSA, cela a un grave effet de dissuasion et d'intimidation (« chilling effect »). Les professionnels des médias ne peuvent remplir leur rôle de diffuseurs d'informations et de gardiens de la démocratie que s'ils obtiennent les informations nécessaires de tiers, notamment des indications sur des événements d'intérêt social qui resteraient sinon cachés. Cela présuppose à son tour que les sources d'information puissent avoir confiance dans le fait que leur nom ne sera pas divulgué. Une obligation de divulguer les informations confiées pourrait dissuader les informateurs. L'identité de la source est donc particulièrement protégée[49]. Avec la base légale existante, la protection de la confidentialité en matière de journalisme ne fonctionne déjà pas de manière fiable, notamment en ce qui concerne la protection de l'identité de la source. La LRens devrait être améliorée sur ce point. Avec la révision proposée de l'art. 28 nLRens, la menace serait au contraire plus grande, ce qui est inacceptable dans un paysage médiatique libre, critique et indépendant dans un Etat de droit.

---

46 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 11.

47 Prise de position de l'association professionnelle des médecins FMH in Tagesanzeiger online, 24 juin 2022, Werden Ärzte, Anwälte und Journalisten bald ausgespäht ?, [disponible sur : https://www.tagesanzeiger.ch/nachrichtendienst-soll-anwaelte-aerzte-und-journalisten-ausspaehen-duerfen-121795356050].

48 COUREDH, Jecker c. Suisse, 35449/14, arrêt du 6 janvier 2021.

49 MÜLLER Jörg Paul/SCHEFER Markus [avec ZELLER Franz], Grundrechte in der Schweiz, 4e éd., Berne 2008, p. 472 ; FROWEIN/PEUKERT, EMRK-Kommentar, 3e éd., Kehl am Rhein 2009, Art. 10 N 17 ; Handkommentar EMRK-MEYER-LADEWIG/NETTESHEIM, CEDH 10 N 39; Basler-Komm/ZELLER, Art. 172 StPO, N 2, N 7 s. ; DONATSCH, in: Kommentar zur Schweizerischen Strafprozessordnung, DONATSCH/HANSJAKOB/LIEBER (édit.), 2e éd., Zurich/Bâle/Genève 2014, Art. 172 N 2 et 4 ; Basler-Komm/BOMMER/GOLDSCHMID, Art. 264 StPO, N 15 ; GYÖRFFY Viktor, Quellenschutz im Strafprozess, in: medialex 6/16 et medialex Jahrbuch 2016, p. 79 ss., N. 2 s. ; COUREDH, Goodwin c. Royaume-Uni (GC), 17488/90, arrêt du 27 mars 1996 ; COUREDH, Voskuil c. Pays-Bas, 64752/01, arrêt du 22 novembre 2007 ; ATF 132 I 184 ; ATF 140 IV 108.

Le respect du secret professionnel et de la protection des sources ne fonctionne déjà pas de manière fiable dans la LRens en vigueur, d'autant plus que la saisie de données relevant du renseignement peut parfois inclure des données de tiers en plus de celles de certaines personnes ou organisations cibles. Parfois – par exemple dans le cas de l'exploration radio et du réseau câblé - des données sont également saisies, pour lesquelles le SRC ne sait pas du tout, du moins initialement, à quelle personne ou organisation elles se rapportent. Il est donc nécessaire de prévoir dans la loi une disposition claire selon laquelle les données soumises au secret professionnel ou à la protection des sources ne peuvent pas être saisies par le SRC. Les exceptions à ce principe nécessiteraient une base légale explicite, tout en garantissant qu'elles ne peuvent être appliquées que dans les cas où cela semble justifié.

Il convient de souligner que l'effacement ultérieur de données soumises au secret professionnel ou à la protection des sources ne saurait remplacer le principe selon lequel ces données ne doivent pas être saisies. L'effacement ultérieur ne change rien au fait que le secret professionnel et la protection des sources ont été violés et que les personnes concernées ont ainsi perdu la protection que leur confèrent leurs droits fondamentaux. La prise de connaissance des faits soumis au secret en soi ne pourra pas non plus être annulée.

La suppression de l'art. 28 al. 2 LRens doit donc être fermement rejetée. Dans son arrêt de principe ATF 147 I 280, le Tribunal fédéral a également déclaré : « Les communications confidentielles entre les journalistes et leurs sources ou entre les avocats et leurs clients bénéficient d'une protection particulière : des mesures ciblées visant à les surveiller sont en principe exclues [...] ; s'il existe néanmoins un risque de saisie de telles communications, des mesures particulières sont nécessaires pour les protéger »[50].

C'est pourquoi – précisément contrairement à ce qui est prévu – les dispositions relatives à la protection du secret professionnel et à la protection des sources doivent être développées de manière à ce que le respect des droits fondamentaux des personnes concernées dans ce domaine soit garanti en permanence. Si les instruments des services de renseignement ne peuvent pas être utilisés de manière à garantir le respect de ces droits fondamentaux, ils doivent être supprimés. Cela concerne notamment l'exploration radio et du réseau câblé, qui porte sur des flux de communication entiers (par ex. toutes les données qui passent par une ligne de fibre optique donnée), et qui inclut donc également toutes les données couvertes par le secret professionnel et la protection des sources qui se trouvent dans le flux de communication saisi.

### 4.10. Art. 37 nLRens – Ordre urgent d'infiltrer des systèmes et réseaux informatiques à l'étranger

Il convient de renoncer à la procédure d'urgence en matière d'infiltration dans des systèmes et des réseaux informatiques à l'étranger.

50 ATF 147 I 280, consid. 6.2.3.

La mesure consistant à s'introduire dans des systèmes et des réseaux informatiques situés à l'étranger est extrêmement délicate du point de vue du droit international public et de la politique de souveraineté. Les mesures urgentes visant à préserver la sécurité extérieure et intérieure sont en principe régies par les articles 184 et 185 Cst. et relèvent de la compétence du Conseil fédéral.

Du point de vue de la souveraineté, il semble problématique de déléguer de manière générale et abstraite dans la loi une telle compétence étendue à des fonctionnaires. Il semble plus judicieux de laisser cette compétence au Conseil fédéral – dans la mesure où elle serait admissible – et de doter éventuellement la loi d'une compétence de délégation en cas d'urgence. Cela permet au Conseil fédéral de prévoir des limites claires au niveau de l'ordonnance ou des directives.

### 4.11. Art. 38 LRens (exploration radio) et art. 39 ss LRens (exploration du réseau câblé)

Les dispositions relatives à l'exploration radio (art. 38 LRens) et à l'exploration du réseau câblé (art. 39 - 43 LRens) doivent être supprimées.

En ce qui concerne l'exploration du réseau câblé, le projet mis en consultation propose des modifications ponctuelles. Il est juste que la révision de la LRens soit l'occasion de se pencher sur la problématique fondamentale de l'exploration du réseau câblé : cette exploration est une surveillance de masse sans motif qui permet au SRC de rechercher des mots-clés dans toutes les télécommunications non cryptées qui passent par des câbles à fibres optiques transfrontaliers. Comme une grande partie des communications basées sur Internet des personnes résidant en Suisse passent par des serveurs et des réseaux étrangers, toutes les personnes se trouvant en Suisse et se déplaçant sur Internet peuvent être concernées par cette surveillance.

L'ingérence importante dans les droits fondamentaux de toutes les personnes qui utilisent des canaux numériques pour s'informer et communiquer avec d'autres personnes et qui doivent s'attendre à être touchées par l'exploration du réseau câblé ne peut pas être justifiée. Il en va de même pour l'exploration radio, qui vise à détecter les émissions électromagnétiques de systèmes de télécommunication situés à l'étranger. Pour cette raison, les dispositions relatives à l'exploration radio (art. 38 LRens) et à l'exploration du réseau câblé (art. 39 - 43 LRens) doivent être supprimées.

### 4.12. Art. 39 nLRens – Exploration du réseau câblé contre des personnes physiques ou morales suisses se trouvant à l'étranger

Il faut renoncer à l'exploration du réseau câblé contre des personnes physiques ou morales suisses se trouvant à l'étranger.

Avec la suppression de la limitation actuelle de l'exploration du réseau câblé aux personnes physiques ou morales non-suisses, l'exploration serait désormais autorisée à l'égard de tous les Suisses, pour

autant qu'ils se trouvent à l'étranger. Cela représente une extension considérable par rapport à la réglementation promise à l'origine.

### 4.13 Art. 41 al. 3 nLRens – Prolongation du délai

Il est plus que probable que chaque exploration du réseau câblé constitue une intrusion dans l'essence de la sphère privée. C'est pourquoi il faut la rejeter en soi, mais en tout cas ne pas l'autoriser plus généreusement. Le délai de l'art. 41 al. 3 nLRens ne doit pas être étendu à 12 mois.

Jusqu'à présent, l'exploration du réseau câblé était limitée à 6 mois, avec une option de prolongation de trois mois. Ces délais seraient étendus à 12, et respectivement à 6 mois.

Toute exploration du réseau câblé implique très probablement une atteinte à l'essence de la sphère privée, qui doit être rejetée. Les arguments avancés dans le rapport explicatif ne sont en tout cas pas convaincants pour une prolongation, c'est-à-dire une extension de l'atteinte : la prolongation est notamment justifiée par le fait que « les besoins en termes de renseignement ne changent pas tous les trois mois », que la Suisse évolue encore en terrain inconnu en matière d'exploration du réseau câblé et que l'acquisition de connaissances prend du temps. Mais c'est justement lorsqu'on se trouve encore en terrain inconnu qu'il est d'autant plus judicieux d'examiner attentivement chaque étape. Un délai de contrôle plus court est également souhaitable pour le développement des connaissances, car les ressources mal attribuées peuvent être réaffectées plus rapidement. La rapidité du changement semble au mieux spéculative, étant donné qu'il s'agit justement, comme l'écrit le rapport lui-même, d'un terrain vierge. Une prolongation des délais n'a donc au contraire aucun sens.

### 4.14. Art. 42 nLRens – Analyse des signaux et des données de mandats existants en matière d'exploration du réseau câblé

Il convient de renoncer à l'analyse des signaux et des données issus des mandats d'exploration du réseau câblé existants.

Dans le cadre d'une procédure de recours menée par la *Digitale Gesellschaft* en collaboration avec sept personnes privées, dont des journalistes et un avocat, le Tribunal fédéral a décidé que le Tribunal administratif fédéral devait examiner de manière approfondie la pratique d'exploration radio et du réseau câblé et vérifier si celle-ci viole les droits fondamentaux. Dans ses prises de position vis-à-vis du Tribunal administratif fédéral dans le cadre de cette procédure, le SRC n'a jusqu'à présent pas montré de volonté d'exposer de manière précise et compréhensible la pratique de l'exploration radio et du réseau câblé. En même temps, le SRC s'est efforcé de présenter une image dans laquelle l'exploration du réseau câblé apparaît comme une mesure très ciblée, en particulier en ce qui concerne la prétendue possibilité d'identifier et d'extraire de manière ciblée les signaux de certaines lignes transfrontalières qui

contiennent des données ayant leur origine ou leur destination dans des pays plus éloignés, comme par exemple la Syrie ou la Russie. Le SRC a rejeté les indications des recourants selon lesquelles les explications du SRC ne concordaient pas avec les données techniques et a insisté sur le fait qu'il était en mesure de trouver et d'extraire le trafic recherché dans un nombre restreint de lignes transfrontalières, malgré les obstacles et difficultés techniques existants.

La justification des compétences que le SRC veut se voir accorder par l'art. 43 al. 3bis nLRens contraste fortement avec les déclarations faites par le SRC dans la procédure de recours mentionnée. Dans le rapport explicatif, le SRC admet qu'il n'est pas possible de déterminer facilement par quelles lignes les données sont transmises depuis et vers des pays plus éloignés. En même temps, il faut constater que les explications du rapport explicatif – tout comme celles de la procédure de recours – semblent difficilement compréhensibles et peu convaincantes. Ainsi, on ne voit pas pourquoi le SRC serait mieux à même de déterminer l'origine ou le point final des données en provenance ou à destination de pays plus éloignés que les exploitants suisses de réseaux filaires et les fournisseurs de prestations de télécommunication, d'autant plus que le SRC explique dans la foulée que les exploitants et les fournisseurs optimisent en permanence leurs flux de données (ce qui concerne justement aussi les flux de données vers des pays plus éloignés).

Certes, le SRC affirme que l'analyse souhaitée est de nature purement technique. Mais cela ne doit pas faire oublier qu'une telle analyse porte nécessairement sur la communication de nombreuses personnes manifestement irréprochables. Sans l'évaluation des métadonnées et, du moins en partie, des données de contenu, une telle analyse ne sera pas possible. Une telle analyse serait donc nécessairement liée à la saisie et à l'évaluation de données personnelles et donc à des atteintes aux droits fondamentaux. Cela ne se justifie pas non plus si le SRC a pour but ultime d'optimiser les missions d'exploration du réseau câblé. Il convient donc de renoncer à la disposition prévue.

## 5. Assurance qualité : art. 58b nLRens – données personnelles relevant du renseignement

Dans le cadre de la révision, les dispositions relatives au contrôle périodique doivent être précisées. Il convient notamment de fixer des délais qui indiquent au SRC de manière complète, claire et sans équivoque quelles données doivent impérativement être vérifiées et, le cas échéant, effacées, et dans quel délai.

La LRens en vigueur prévoit déjà que le SRC vérifie périodiquement les données qu'il traite. Dans le cadre de la réorganisation de la saisie et du classement des données, une nouvelle réglementation est proposée à ce sujet.

Il convient de souligner que l'examen périodique n'a jamais réussi jusqu'ici à garantir que les données qui ne doivent pas (ou plus) être enregistrées ou qui ne sont pas (ou plus) nécessaires soient effacées. L'activité de surveillance de la DélCdG a toujours mis au jour des quantités considérables de données qui n'auraient déjà pas dû être saisies ou qui auraient au moins dû être effacées dans le cadre de l'examen périodique. Ainsi, la DélCdG a trouvé en 2019 des données pour lesquelles elle avait déjà constaté en 2010 qu'elles devaient être effacées[51]. D'autres exemples rendus publics montrent également que des données qui auraient dû être effacées dans le cadre de l'examen périodique sont restées enregistrées pendant des années[52].

## 6. « Internet » au lieu de « cyberespace »

Le terme de "cyberespace" est une notion très vague. De fait, le but est de surveiller l'Internet, c'est pourquoi cela doit être mentionné littéralement.

### 6.1 Art. 6 al. 1 let. b nLRens

A l'art. 6 al. 1 let. b nLRens, le mot « cyberespace » doit être remplacé par « internet » :

« détecter, observer et évaluer des événements importants en matière de politique de sécurité se produisant à l'étranger et sur internet ; »

### 6.2 Art. 19 al. 2 let. f nLRens

A l'art. 19 al. 2 let. f nLRens, le mot « cyberespace » doit être remplacé par « internet » :

« les activités importantes en matière de politique de sécurité sur internet »

## 7. Art. 75 ss LRens – Révision totale de l'autorité de surveillance AS-Rens

Dans le cadre de la révision de la LRens, il faut élaborer une base légale dans laquelle l'AS-Rens n'a aucune dépendance vis-à-vis du DDPS et la plus grande indépendance possible par rapport aux autres institutions étatiques.

Aux art. 75 ss LRens, la loi actuelle prévoit les bases légales pour l'autorité de surveillance « indépendante » des activités de renseignement (AS-Rens). Il est évident qu'une autorité qui, à l'instar du SRC, est rattachée au DDPS (art. 77 LRens) et dont la direction est proposée par le DDPS (art. 76 al.

51 Traitement des données dans le système d'information relatif à la protection de l'Etat (ISIS). Rapport de la Délégation des commissions de gestion des Chambres fédérales, 21 juin 2010, FF 2010 7003 ; rapports annuels 2019, 2020 et 2021 de la DélCdG.

52 GYÖRFFY Viktor, Rechtsgutachten zur Praxis der Informationsbeschaffung durch den Nachrichtendienst des Bundes (NDB), 25 mai 2022, notamment p. 42 ss N 167 ss.

2 LRens), ne dispose pas de l'indépendance nécessaire et ne peut donc pas non plus assumer sa tâche de contrôle du SRC de manière satisfaisante.

## 8. Dispositions pénales

### 8.1. Art. 83a nLRens – Interdiction d'organisations

Il faut renoncer à une interdiction d'organisation. Si tant est qu'une telle interdiction soit décidée, elle ne doit pas l'être par le Conseil fédéral, mais par le Parlement.

L'interdiction d'une organisation est désormais réglée par l'art. 74 LRens alors que les interdictions étaient jusqu'à présent fondées sur une loi spéciale (loi fédérale du 12 décembre 2014 interdisant les groupes « Al-Qaïda » et « Etat islamique » et les organisations apparentées[53]). Désormais, la compétence de prononcer l'interdiction revient au Conseil fédéral, ce qui est moins démocratique qu'une loi votée par le parlement et soumise à un débat ouvert et au référendum. L'interdiction d'une organisation est un acte particulièrement grave dans l'atteinte qu'il porte aux valeurs constitutionnelles et notamment au respect des libertés d'expression, d'association ou de réunion.

La procédure menée durant l'été 2022 pour la mise en consultation de la décision interdisant Al-Qaïda et l'Etat islamique a montré son caractère biaisé. En effet, à teneur de la publication dans la Feuille fédérale[54], le projet de décision motivée ne pouvait être consulté que dans les bureaux du secrétariat général du DDPS et à condition de démontrer au préalable être personnellement concerné par l'interdiction à prononcer. Autrement dit, il était indispensable d'apporter la preuve de son appartenance à une organisation terroriste et donc d'avoir violé la loi existante et ses dispositions pénales pour avoir le droit de s'exprimer sur la décision visant à faire perdurer cette interdiction. Une telle procédure contrevient notamment au droit de ne pas s'auto-incriminer (art. 113 al. 1 CPP). En demandant aux personnes de se dénoncer, elle est une procédure alibi car il semble clair que personne ne va avouer être un terroriste pour pouvoir participer à une procédure administrative.

Une décision du Conseil fédéral prise suite à un tel processus et dont le non-respect serait sanctionné par des dispositions pénales manque donc de légitimité. Dans la mesure où le Conseil fédéral peut modifier sa décision pour inclure d'autres groupes dans la liste des organisations interdites, cela revient de fait à donner au Conseil fédéral la compétence de définir les éléments constitutifs de l'infraction, ce qui est et doit rester une prérogative du parlement par le biais de lois en bonne et due forme.

### 8.2. Art. 83b en relation avec l'art. 73 al. 1 nLRens – Interdiction d'exercer une activité

La disposition pénale « violation de l'interdiction d'exercer une activité » doit être biffée.

53 RS 122.
54 Décision de portée générale concernant l'interdiction des groupes « Al-Qaïda » et « État islamique » et des organisations apparentée, FF 2022 1802.

Si l'exercice de l'activité engendre de vrais risques, cela tombe déjà sous le coup des dispositions pénales actuelles. Il n'y a donc aucun intérêt à créer une infraction et une disposition pénale supplémentaires.

L'interdiction d'exercer une activité est un acte particulièrement grave dans l'atteinte qu'il porte aux valeurs constitutionnelles et notamment au respect des libertés personnelle, économique, d'expression, d'association ou de réunion.

La personne qui menace concrètement la sécurité de la Suisse peut aujourd'hui déjà tomber dans le champ d'application des dispositions pénales comme la participation ou le soutien à une organisation criminelle ou terroriste (art. 260ter CP), le financement du terrorisme (art. 260quinquies CP) le recrutement, la formation et le voyage en vue d'un acte terroriste (art. 260sexies CP) ou les actes préparatoires délictueux (art. 260bis CP) si elle prépare concrètement un attentat. Le droit pénal est soumis à un principe de légalité plus strict que d'autres domaines du droit en raison des conséquences qu'il implique pour les personnes concernées. Il ne se justifie pas de prévoir des sanctions pénales en cas de violation de l'interdiction d'exercer une activité puisque cette dernière intervient encore plus en amont et de manière préventive.

Dans la mesure où le Conseil fédéral peut modifier sa décision pour inclure d'autres groupes dans la liste des organisations interdites, cela revient de fait à donner au Conseil fédéral la compétence de définir les éléments constitutifs de l'infraction, ce qui est et doit rester une prérogative du parlement par le biais de lois en bonne et due forme.

### 8.3. Art. 83c nLRens – Insoumission à une décision

La disposition pénale « insoumission à une décision et violation de l'obligation de garder le secret » doit être biffée.

Selon le texte de l'art. 83c al. 1 let. a nLRens, la disposition semble s'appliquer à toutes les décisions signifiées par le SRC. Le rapport[55] ne mentionne toutefois que les décisions en matière d'acquisition de renseignements. Le champ d'application réel de la disposition ne semble donc pas clair.

La disposition prévoit une peine-menace de CHF 100'00,00 d'amende. En matière d'acquisition de renseignement, le recours contre une décision du SRC n'a pas d'effet suspensif (art. 83 al. 2 LRens). Le SRC, vu qu'il se base sur des renseignements confidentiels, ne peut pas forcément motiver de manière détaillée les décisions qu'il rend. Ainsi, il se pourrait qu'une personne ayant reçu une décision motivée de manière lacunaire et ayant fait recours se retrouve poursuivie pour ne pas avoir exécuté la décision dans le délai que le SRC lui-même a fixé.

55 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 32.

L'amende de CHF 100'000,00 est dix fois plus élevées que l'amende qui peut être infligée par un tribunal en cas de non-respect d'un jugement. On ne voit pas en quoi les décisions du SRC seraient dix fois plus importantes et dignes de respect que celles d'un tribunal.

Le SRC dispose aujourd'hui déjà de la possibilité de rendre des décisions sous commination de la peine prévue à l'art. 292 CP. Le droit actuel apparaît donc suffisant.

### 8.4. Art. 83d et 83e nLRens– Juridiction

La compétence de droit pénal administratif du SRC et du service chargé de l'exploration du réseau câblé doit être supprimée. Le SRC ne peut pas rendre des décisions et poursuivre lui-même les gens qui ne les respecteraient pas.

Si les dispositions pénales en matière d'interdiction d'organisations et d'interdiction d'exercer une activité étaient maintenues malgré tout, l'art 83e nLRens devrait préciser que l'obligation de communiquer ne concerne que les décisions relatives à ces deux infractions.

Selon l'art. 83d nLRens, le SRC pourrait poursuivre lui-même les personnes n'ayant pas exécuté une de ses décisions. Cette nouvelle disposition rend encore plus floue la distinction entre les activités préventives qui sont du ressort du SRC et les activités répressives qui reviennent aux autorités pénales.

Le SRC serait, dans cette configuration, juge et partie et ne pourrait donc pas garantir le droit à un procès équitable pour les personnes accusées. Ce d'autant plus que le SRC peut garder secrets certains éléments du dossier. La personne se retrouverait donc face à une autorité qui lui a notifié une décision motivée de manière lacunaire, qui potentiellement pourrait lui refuser l'accès à certains éléments du dossier mais qui en disposerait malgré tout. Une poursuite par le SRC conformément à la DPA n'est pas acceptable. Ces réflexions valent également pour le service chargé de l'exploration du réseau câblé.

La communication des décisions d'autres autorités au SRC semble d'appliquer à toutes les décisions rendues en vertu des dispositions pénales de la LRens, alors que – selon le message – ce n'est le cas que pour les décisions en matière d'interdiction d'organisations et d'exercer une activité. Si ces infractions sont conservées dans la nLRens, le champ d'application de l'obligation de communiquer de l'art. 83e nLRens doit être précisé dans le texte de loi.

## 9. Élargissement de l'interdiction de se rendre dans un pays donné

### 9.1. Art. 24h nLMSI

Il faut s'abstenir de modifier la LMSI dans le cadre de la révision de la LRens.

Mais il faut au moins supprimer l'exception de la preuve policière à l'art. 24h al. 1 let. a nLMSI, de sorte que l'interdiction de se rendre dans un pays donné ne puisse être ordonnée qu'en cas de jugement entré

en force. L'art. 24h al. 1 let. a nLMSI doit donc être modifié comme suit : « elle a été condamnée pour cela par un jugement définitif et ».

L'art. 24h al. 2 nLMSI doit être supprimé, car les preuves policières ne suffisent pas pour ordonner une interdiction de quitter le territoire.

Dans la nouvelle section « mesures contre les actes de violence lors de défilés et de manifestations », fedpol pourrait, conformément à l'art. 24h nLMSI, interdire à des personnes de quitter la Suisse pour se rendre dans un pays donné pendant une durée déterminée s'il faut s'attendre à ce que des actes de violence y soient commis. Jusqu'à présent, la LMSI ne connaissait cette interdiction de se rendre dans un pays donné que pour les personnes présentant un danger terroriste selon l'art. 23n LMSI et pour les manifestations sportives selon l'art. 24c LMSI. L'interdiction de se rendre dans un pays donné est ainsi massivement étendue.

Selon l'art. 24h al. 1 let. a nLMSI, le déplacement d'une personne pourrait lui être interdit si elle a été condamnée pour avoir participé à des actes de violence contre des personnes ou des biens lors d'une manifestation ou d'un rassemblement en Suisse ou à l'étranger, ou exceptionnellement si « des preuves policières indiquent qu'elle a pris part à de tels actes ».

Selon l'art. 24h al. 2 nLMSI, sont notamment considérées comme des preuves policières les plaintes pénales reposant sur des constatations policières (let. a) et les décisions policières d'interdiction d'accès et de renvoi (let. b). Cette énumération n'est pas exhaustive en raison de l'utilisation du terme « notamment ». Le rapport explicatif renvoie ensuite explicitement à l'art. 5 OMAH, selon lequel des déclarations crédibles de la police ou de particuliers ou des communications d'autorités étrangères doivent également suffire comme présomption de dangerosité.

Or, ni les plaintes pénales déposées par la police, ni les décisions d'éloignement ou de renvoi, et encore moins les déclarations crédibles, ne prouvent l'existence d'une infraction. Le rapport explicatif explique cela par le fait que plusieurs années peuvent s'écouler jusqu'à ce qu'une personne soit définitivement condamnée, lorsqu'un recours est déposé contre un jugement ou une ordonnance pénale et qu'attendre des années avant d'imposer une interdiction de sortie du territoire irait à l'encontre des objectifs préventifs de la mesure. Cela peut être vrai, mais est néanmoins normal dans un État de droit où seul un jugement définitif permet de prouver l'existence d'une infraction. L'article 24h nLMSI est donc contraire au principe de la présomption d'innocence. Il n'est pas justifié d'ordonner une interdiction de sortie du territoire à titre préventif et sans preuve qu'une infraction ait effectivement été commise.

En plus des conditions de l'al. 1 let. a, il doit exister (art. 24h al. 1 let. b nLMSI) des soupçons concrets que la personne cherche à se rendre à l'étranger pour prendre part dans ce pays à des actes de violences dirigés contre des personnes ou des biens dans le cadre d'un défilé ou d'une manifestation à caractère international. Le degré de gravité qui doit être atteint pour les actes de violence contre des biens n'est pas précisé. Il doit au contraire être précisé expressément que toute atteinte aux biens ne suffit pas à

ordonner une interdiction de quitter le territoire mais que ces actes doivent atteindre un certain degré de gravité.

Le rapport explicatif reconnaît justement que l'interdiction de se rendre à l'étranger touche à la liberté d'expression. Ceci est expliqué par le fait que la réglementation prévue ne s'appliquerait qu'à des personnes qui participeraient avec une haute vraisemblance à des actes de violence, ce qui n'est pas protégé par la liberté d'expression. De cette manière, le droit fondamental à la liberté d'expression ne serait pas touché. Une simple probabilité, même élevée, que la personne pourrait participer à l'avenir à des actes de violence ne suffit toutefois pas pour ne pas toucher au droit à la liberté d'expression. Ceci en particulier car à ce stade il n'existe aucune condamnation entrée en force qui prouve la commission des prétendus actes de violence. Cette réglementation entraîne donc une atteinte aux droits fondamentaux en matière de liberté d'expression et de liberté personnelle, qui ne peut pas être justifiée par une simple probabilité que des actes violents soient commis à l'avenir.

De plus, on peut se demander comment il serait possible de prédire d'éventuels comportements violents futurs qui pourraient survenir dans le cadre d'une manifestation. Le comportement potentiel d'une personne ne peut pas être simplement déduit des comportements passés, surtout avec une notion aussi floue de la « violence ». Déjà dans le domaine du droit pénal, les pronostics négatifs en matière de récidive sont l'exception et les difficultés d'établir un pronostic ont été largement discutées en droit.

Dans le rapport explicatif lui-même, il est dit que l'interdiction de se rendre à l'étranger fait partie des « mesures policières préventives »[56]. Il en ressort que cette interdiction ne relève pas du domaine du renseignement et n'a donc rien à faire dans le projet de loi proposé. Cela relève d'une confusion typique entre les activités policières et les activités de renseignement, qui doivent pourtant être clairement distinguées.

### 9.2. Art. 24k nLMSI – Limite d'âge

L'application de cette mesure dès 15 ans (art. 24k nLMSI) doit être biffée.

Selon l'art. 24k nLMSI, l'interdiction de se rendre à l'étranger pourrait être ordonnée contre toute personne de plus de 15 ans. Les mesures contre les enfants et les adolescents doivent, comme le droit pénal des mineurs, déployer un effet éducatif. La mesure prévue contre les mineurs dès 15 ans est donc hautement problématique sur ce point et entre en contradiction avec la convention de l'ONU sur les droits de l'enfant, ratifiée par la Suisse.

56 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 33.

## 10. Traitement de données et assurance qualité : algorithmes et reconnaissance faciale

Il convient de renoncer au traitement automatisé de données personnelles et au traitement de données biométriques. En tout cas, il ne doit pas être effectué sans base légale explicite. Une telle base devrait tenir suffisamment compte des intérêts en matière de droits fondamentaux et prévoir des limites strictes ainsi que des mesures de protection adéquates. L'utilisation de données biométriques et le traitement automatisé de données personnelles par les services de renseignement ne se justifieront toutefois pas au vu de la grave atteinte aux droits fondamentaux qu'ils impliqueraient et des problèmes fondamentaux que posent de telles technologies dans leur ensemble.

L'AS-Rens a publié son rapport d'activité en mars 2022. Dans ce rapport, elle a annoncé que le SRC utilisait depuis 2020 un système de reconnaissance faciale permettant d'identifier des personnes sur des photos. L'autorité de surveillance indépendante constate que le SRC procède ainsi, bien qu'aucun des systèmes d'information ne prévoie un tel traitement de données biométriques.

Il est frappant de constater que le présent projet de révision estime certes « indispensable » l'utilisation de programmes capables d'apprendre pour la recherche et la catégorisation d'informations, mais qu'il renonce en même temps à une réglementation légale des conditions et des limites à leur appliquer. Au lieu de cela, il s'en tient à une déclaration du bout des lèvres et incompréhensible selon laquelle l'utilisation de l'intelligence artificielle, avec le risque d'atteintes graves aux droits fondamentaux, n'est « pas prévue »[57].

La législation révisée en matière de protection des données prévoit des mesures de protection particulières concernant les données biométriques, notamment en les considérant comme sensibles[58]. De même, le traitement automatisé de données personnelles qui présente un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée est qualifié de « profilage à risque élevé » (art. 5 let. g nLPD), ce qui implique diverses mesures de protection.

Dans ce contexte législatif, il n'appartient pas au Conseil fédéral ou au SRC de déterminer quand des données biométriques ou un traitement automatisé de données personnelles constituent une atteinte grave aux droits fondamentaux. Il appartient plutôt au Parlement d'élaborer, le cas échéant, une base légale qui tienne suffisamment compte des intérêts en matière de droits fondamentaux. L'utilisation de données biométriques et le traitement automatisé de données personnelles par les services de renseignement entraîneraient toutefois de graves atteintes aux droits fondamentaux, notamment parce qu'ils permettraient d'analyser de grandes quantités de données. En outre, ces systèmes posent toute une série de problèmes fondamentaux (notamment : grand nombre de personnes concernées par une utilisation ou manque de ciblage des systèmes ; manque de transparence et de traçabilité ; effet discriminatoire, en particulier des systèmes de reconnaissance faciale). On peut donc se demander dans

57 Rapport explicatif concernant la révision de la loi fédérale du 25 septembre 2015 sur le renseignement, mai 2022, p. 21.
58 Art. 5 let. c ch. 4 nLPD dans la version adoptée, FF 2020 7397.

quelle mesure l'utilisation de données biométriques ou le traitement automatisé de données personnelles dans le domaine du renseignement peuvent se justifier.

Nous vous remercions d’avance de prendre en compte nos remarques dans la suite de vos travaux et vous adressons, Madame la Conseillère fédérale, Mesdames, Messieurs, nos meilleures salutations.