Bern, 21. April 2026

Révision de la LRens : critiques et revendications concernant le paquet de base

Fin janvier 2026, le Conseil fédéral a adopté le message relatif au paquet de base de la révision de la LRens et l'a transmis au Parlement. Le projet va dans le même sens que l'avant-projet. Malgré quelques adaptations ponctuelles, la critique de fond à l'égard du projet demeure. Restent notamment problématiques l'extension des mesures de recherche soumises à autorisation, le maintien de l'exploration du réseau câblé, ainsi que de nouvelles compétences étendues en matière de traitement des données et le recours au profilage au moyen de systèmes d'IA.

Le groupe de travail LRens, un groupe de travail de la Plateforme des ONG suisses pour les droits humains, suit d'un œil critique la révision de la LRens et intervient dans le processus parlementaire afin d'obtenir les corrections nécessaires dans l'intérêt des droits fondamentaux et des droits humains. L'analyse actualisée ci-dessous s'inscrit dans le prolongement de l'analyse précédente relative à l'avant-projet mis en consultation. Elle situe le message du Conseil fédéral et met en évidence les points centraux sur lesquels des corrections sont nécessaires, du point de vue des droits fondamentaux et des droits humains, dans le cadre des débats parlementaires.

Revendications centrales du groupe de travail LRens

- Pas de surveillance de l'exercice des droits politiques fondamentaux
- Pas d'extension des mesures de recherche soumises à autorisation et pas d'affaiblissement des contrôles
- Pas d'extension générale des compétences du SRC au « cyberespace »
- Abolition de la surveillance indépendante de tout motif et de tout soupçon (exploration du réseau câblé, conservation des données)
- Des limites légales claires au traitement des données et des obligations de suppression effectives
- Renoncer au profilage au moyen de systèmes d'IA
- Renforcement du droits d'accès des personnes concernées à leurs propres données personnelles

Ci-dessous, l'analyse actualisée du groupe de travail LRens relative au message du Conseil fédéral sur le paquet de base de la révision de la LRens :

Contenu

1 Pas de surveillance de l'exercice des droits politiques fondamentaux

Le Service de renseignement de la Confédération est soumis à des limites dans la collecte de données : il ne peut recueillir ni traiter des « informations sur l'activité politique et sur l'exercice en Suisse de la liberté d'expression, de réunion ou d'association » (art. 5, al. 5 LRens), à moins qu'il n'existe des « indices concrets » que ces droits soient exercés « pour préparer ou exécuter des activités terroristes, d'espionnage interdites ou relevant de l'extrémisme violent » (art. 5, al. 6 LRens).

Le respect de cette limite au traitement des données n'a jusqu'ici pas été effectivement garanti dans la pratique. Le projet de loi n'y remédie pas de manière suffisante et crée, avec le nouveau concept de traitement des données, de nouvelles lacunes en matière de protection.

Le projet de loi prévoit qu'exceptionnellement, des données visées à l'art. 5, al. 5 LRens concernant une organisation ou une personne puissent être recueillies et traitées lorsque cela est nécessaire pour protéger une organisation ou une personne contre une activité au sens de l'art. 6, al. 1, let. a LRens (art. 5, al. 6, let. c), ainsi que lorsque cela est nécessaire à l'accomplissement des tâches administratives du SRC (art. 5, al. 6, let. f). La limite au traitement des données prévue à l'art. 5, al. 5 serait ainsi supprimée sans qu'une raison matérielle ne justifie une telle exception. Il ne peut appartenir au SRC de traiter des données relatives à des activités politiques afin de protéger la personne ou l'organisation concernée contre des menaces. Le cas échéant, une telle protection doit être assurée dans le cadre des mesures de police de sécurité existantes. Dans la mesure où un traitement de données est effectivement nécessaire à l'accomplissement des tâches administratives du SRC, celui-ci peut déjà y procéder sur la base de la LOGA. Une base légale spécifique qui déroge à cette limite au traitement des données apparaît dès lors inutile.

Nous demandons:

- Aucune collecte ni aucun traitement d'informations sur l'activité politique ainsi que sur l'exercice en Suisse de la liberté d'expression, de réunion et d'association.
- Une garantie et un contrôle effectifs, dans la pratique, de cette limite au traitement des données.
- Aucune nouvelle faille de protection pour les droits politiques fondamentaux du fait du concept de traitement des données.

2 Pas d'extension des mesures de recherche soumises à autorisation et pas d'affaiblissement des contrôles

La révision de la LRens prévoit une extension problématique des mesures de recherche soumises à autorisation et, simultanément, un affaiblissement des contrôles existants. Parmi les mesures de recherche soumises à autorisation figurent notamment l'écoute téléphonique, la pose de micros dans des locaux, la perquisition de locaux, de véhicules et de contenants, l'intrusion dans des systèmes et réseaux informatiques, ainsi que la surveillance des courriels et des communications sur Internet. Ces méthodes de surveillance, qui portent gravement atteinte au droit à la vie privée, ne pouvaient jusqu'ici être utilisées que pour prévenir le terrorisme, l'espionnage, une attaque contre une infrastructure critique et la prolifération d'armes nucléaires, biologiques ou chimiques.

Critique 1 : extension de la surveillance à la lutte contre l'extrémisme violent
Désormais, cette surveillance intrusive devrait aussi être possible pour lutter contre l'« extrémisme violent » (art. 27, al. 1, let. a, ch. 1, P-LRens). Comme l'extrémisme violent n'est pas défini juridiquement, on ignore ce que recouvre exactement cette notion. Une chose est toutefois certaine : le cercle des personnes susceptibles d'être surveillées s'en trouverait considérablement élargi. En étendant de graves atteintes au droit fondamental à la vie privée au-delà de menaces majeures telles que le terrorisme, on risque rapidement de rendre la surveillance disproportionnée, et donc inadmissible. C'est précisément pour cette raison que le Conseil fédéral avait, lors de l'introduction de la LRens en 2017, renoncé à étendre la surveillance soumise à autorisation à l'« extrémisme violent ». Quelques années plus tard, il compte pourtant le faire.

Critique 2: suppression des possibilités de recours contre une surveillance disproportionnée
Le caractère proportionné d'une mesure de surveillance ordonnée sera encore plus difficile à contrôler après la révision qu'il ne l'est déjà aujourd'hui. En effet, la révision prévoit aussi un affaiblissement des contrôles existants dans le domaine des mesures de recherche soumises à autorisation. Actuellement, les personnes surveillées doivent être informées une fois la surveillance terminée et elles ont la possibilité de recourir. Désormais, l'information ultérieure des personnes surveillées pourra être reportée plus facilement et plus longtemps (art. 33 P-LRens). En outre, il resterait possible de renoncer complètement à informer ultérieurement les personnes surveillées. Celles-ci seraient ainsi privées de toute possibilité de recours.

Critique 3 : affaiblissement du contrôle dans la procédure d'autorisation des mesures de recherche
Un autre affaiblissement du contrôle concerne la procédure d'autorisation. Aujourd'hui, les mesures de recherche soumises à autorisation doivent être approuvées par le Tribunal administratif fédéral et par la Délégation pour la sécurité du Conseil fédéral. Désormais, l'accord de l'ensemble de la Délégation pour la sécurité ne serait plus impératif pour la prolongation ou l'extension des mesures de recherche soumises à autorisation (art. 30, al. 3 et 4). Le Tribunal administratif fédéral lui-même se montre critique à cet égard (ch. 10 de sa prise de position dans la procédure de consultation).

Il serait également possible que l'autorisation du Tribunal administratif fédéral n'intervienne qu'a posteriori (art. 29b, al. 2, P-LRens). Entre l'expiration d'une autorisation en cours et la nouvelle décision du Tribunal administratif fédéral, le SRC pourrait donc continuer à surveiller des personnes sans autorisation judiciaire (art. 29b, al. 2, P-LRens). En outre, seules les mesures exécutées en Suisse seraient encore être soumises à l'autorisation du Tribunal administratif fédéral.

Critique 4 : usage de chevaux de Troie étatiques
Grâce à des enquêtes journalistiques internationales, nous savons depuis un certain temps que le Service de renseignement de la Confédération utilise des logiciels espions étatiques, en particulier le spyware « Pegasus ». L'intrusion dans des systèmes informatiques fait partie des mesures de recherche soumises à autorisation (art. 26b LRens), mais l'ampleur et l'intensité de la surveillance déjà pratiquée aujourd'hui ne sont pas claires. L'usage de chevaux de Troie étatiques viole la sphère intime numérique et mine la sécurité informatique de l'ensemble de la population, puisque les failles de sécurité ne sont pas corrigées mais exploitées à des fins de surveillance.

Critique 5 : usage de traceurs GPS sans autorisation judiciaire
Bien que le Conseil fédéral reconnaisse que l'usage de traceurs GPS constitue une grave atteinte aux droits fondamentaux, il souhaite désormais rendre un tel usage possible sans autorisation judiciaire dans le cadre d'observations (art. 14, al. 3, P-LRens). Or, la qualification de l'observation comme mesure *non* soumise à autorisation constitue déjà aujourd'hui une atteinte significative aux droits fondamentaux. L'observation devrait être qualifiée de mesure de recherche soumise à autorisation et ne doit en aucun cas conduire à un affaiblissement supplémentaire des droits fondamentaux par l'usage incontrôlé de traceurs GPS.

Critique 6 : traitement des données issues des mesures de recherche soumises à autorisation
Le régime prévu pour le traitement des données n'est pas suffisant pour protéger le secret professionnel. Lorsqu'une personne soumise au secret professionnel (avocat, journaliste, médecin, etc.) fait l'objet d'une surveillance, les données « qui ne présentent aucun lien avec la menace spécifique » sont détruites. Or il peut aussi exister des données qui présentent un lien avec la menace tout en étant protégées par le secret professionnel. À l'inverse, lorsque la personne surveillée n'est pas soumise au secret professionnel, doivent être détruites les données « à propos desquelles une personne peut refuser de témoigner selon les art. 171 à 173 CPP », indépendamment de leur lien avec la menace. Il en résulte que le secret professionnel est mieux protégé lorsque la personne surveillée n'y est pas elle-même soumise.

Surveillance d'une personne soumise au secret professionnel		
Données récoltées…	…soumises au secret	…non soumises au secret
…en lien avec la menace	Conservées	Conservées

… sans lien avec la menace	Supprimées	Supprimées

Surveillance d'une personne non soumise au secret professionnel		
Données récoltées…	…soumises au secret	…non soumises au secret
…en lien avec la menace	Supprimées	Conservées
… sans lien avec la menace	Supprimées	Conservées

La loi doit donc garantir que toutes les données soumises au secret professionnel sont détruites, quelle que soit la personne visée par la surveillance. De même, conserver des données sans lien avec la menace viole le principe de finalité et de légalité. Quelle que soit la catégorie de la personne surveillée, seules les données en lien avec la menace et non soumises au secret devraient être conservées :

Indépendamment de la catégorie de la personne surveillée		
Données récoltées…	…soumises au secret	…non soumises au secret
…en lien avec la menace	Supprimées	Conservées
… sans lien avec la menace	Supprimées	Supprimées

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 en lien avec la menace. Enfin, il faut préciser qui est responsable du tri et de la destruction lorsque la personne surveillée n'est pas soumise au secret professionnel mais que de telles données sont interceptées. Il serait en effet inacceptable que le SRC puisse prendre connaissance de données protégées parce qu'il effectue lui-même le tri. Ceci viderait de son sens la protection du secret professionnel. Un tri ultérieur ne suffit pas à préserver les droits découlant du secret professionnel. Ces données ne doivent donc pas pouvoir être saisies par le SRC.

La solution la plus simple et la plus protectrice des droits fondamentaux consiste donc à mettre en place un tri des données par une instance indépendante pour toutes les MRSA indépendamment de la catégorie de personne visée. Cette instance trierait les données avant de ne transmettre au SRC que celles qui sont à la fois nécessaires et non-protégées par le secret professionnel.

Nous demandons :

- Les méthodes de surveillance invasives ne doivent pas être étendues au domaine de l'« extrémisme violent ».
- Les contrôles dans la procédure d'autorisation ne doivent pas être affaiblis.
- Les personnes surveillées doivent, dans tous les cas, être informées après la fin des mesures afin qu'elles puissent faire valoir leur droit d'être entendues par un tribunal. Les failles de sécurité doivent impérativement être signalées aux fabricants.
- Il faut renoncer à la possibilité d'utiliser des traceurs GPS sans autorisation judiciaire.
- Le tri et la destruction des données issues des mesures de recherche soumises à autorisation doivent être adaptés afin que seules les données en lien avec une menace et non couvertes par le secret professionnel soient communiquées au SRC.

3 Pas d'extension des compétences de surveillance au « cyberespace »

Jusqu'ici, la marge d'action du service de renseignement sur Internet n'existait que lorsque l'espace concerné relevait d'un autre but énuméré à l'art. 6, al. 1 (par exemple des attaques contre des infrastructures critiques). Désormais, les compétences du SRC devraient s'étendre de manière générale au « cyberespace ». Il s'agit d'une extension massive. Seraient désormais visés tous les « événements importants du point de vue de la politique de sécurité » dans le cyberespace, sans lien avec des menaces particulières (voir p. ex. art. 6, al. 1, let. a, ch. 1 à 4). Cette extension ouvre la porte à ce que le SRC puisse définir pratiquement tout ce qui se passe dans le « cyberespace » comme relevant de ses tâches.

Le cyberespace va bien au-delà d'Internet, comme la Confédération le relève elle-même : « Le cyberespace désigne l'ensemble des infrastructures d'information et de communication (matérielles et logicielles) qui échangent, collectent, stockent et traitent des données ou les transforment en actions (physiques), ainsi que les interactions qu'elles permettent entre personnes, organisations et États. Cela va au-delà d'Internet. » (Message, p. 28) À la différence d'« Internet », le cyberespace englobe aussi les intranets, les systèmes de commande tels que SCADA, les bus de communication comme le CAN-Bus, les transmissions radio et satellites, ainsi que les objets connectés sans connexion Internet ou des systèmes cloisonnés de toute sorte.

Cette extension est disproportionnée. On ne voit pas pourquoi le service de renseignement devrait potentiellement avoir accès à des systèmes de commande (tels que SCADA ou CAN-Bus), qui sont principalement utilisés dans des contextes industriels ou dans des entreprises. Il n'existe pas davantage de nécessité que des systèmes IoT sans connexion à Internet – du four aux capteurs – constituent un champ d'investigation pour le SRC.

Nous demandons :

- **À l'art. 6, al. 1, let. b (tâches du SRC), le mot «cyberespace» doit être remplacé par «internet»:** *«pour constater, observer et évaluer des événements importants du point de vue de la politique de sécurité à l'étranger et sur internet;* »
- **À l'art 19, al. 2, let. b (obligation de renseigner), le mot « cyberespace » doit être remplacé par «internet»:** «*pour constater, observer et évaluer des événements importants du point de vue de la politique de sécurité à l'étranger et sur internet;» ; «activités importantes du point de vue de la politique de sécurité sur internet»*

4 Abolition de la surveillance indépendante de tout motif et de tout soupçon (exploration du réseau câblé, conservation des données)

L'exploration du réseau câblé constitue une atteinte particulièrement grave aux droits fondamentaux des personnes en Suisse. Ce qui peut sembler inoffensif signifie en réalité une surveillance de masse, sans motif concret, des communications transfrontières. Dans le message, la Confédération parle elle-même d'un « capteur ». Or toute exploration du réseau câblé constitue une atteinte au noyau dur de la sphère privée, raison pour laquelle nous nous y opposons fondamentalement. Dans son arrêt de principe du 19 novembre 2025, le Tribunal administratif fédéral a tout récemment constaté que l'exploration du réseau câblé violait les droits fondamentaux. Le régime actuel de l'exploration du réseau câblé viole la Constitution fédérale et la Convention européenne des droits de l'homme (CEDH).

Avec sa proposition de révision de la LRens, le Conseil fédéral ignore manifestement cet arrêt. Au contraire, il souhaite encore faciliter pour le service de renseignement le recours à l'exploration du réseau câblé. Seule la suppression de ce type d'exploration permettrait pourtant de rétablir une situation conforme au droit. Au lieu de cela, il étend à l'art. 39, al. 1 le champ d'application de l'exploration du réseau câblé au « cyberespace » (jusqu'ici : seulement les « événements survenant à l'étranger »).

En outre, l'exploration du réseau câblé reste limitée à six mois, mais la possibilité de prolongation passerait désormais de trois à six mois (art. 41, al. 3). Nous rejetons cette extension. Le nouvel instrument d'analyse prévu à l'art. 42, al. 3bis constitue également une extension de l'exploration du réseau câblé, que nous rejetons aussi. On ne voit pas pourquoi le SRC serait mieux à même que les exploitantes suisses de réseaux filaires et les fournisseurs de services de télécommunication de déterminer l'origine ou le point final de données provenant de ou allant vers des pays plus éloignés. Le SRC affirme certes que l'évaluation souhaitée est de nature purement technique. Cela ne doit toutefois pas masquer le fait qu'une telle analyse toucherait nécessairement les communications de nombreuses personnes manifestement irréprochables. Sans analyse des métadonnées et, au moins en partie, des données de contenu, une telle analyse ne peut être réalisée. Elle

serait donc nécessairement liée à la collecte et à l'évaluation de données personnelles et, partant, à des atteintes aux droits fondamentaux. Cela ne saurait se justifier, même si le SRC entend finalement optimiser ainsi les mandats d'exploration du réseau câblé. Il faut donc renoncer à la disposition prévue.

Le service de renseignement s'appuie également, pour ses mesures de recherche, sur la conservation des données (art. 26, al. 1, let. a). La conservation des données constitue une violation flagrante du droit fondamental à la vie privée, garanti par la Constitution fédérale et consacré aussi par la Convention européenne des droits de l'homme. Elle impose aux fournisseurs de services postaux, téléphoniques et Internet en Suisse d'enregistrer pendant six mois le comportement de communication de leurs client·e·s, c'est-à-dire de conserver préventivement les données des utilisateurs et utilisatrices indépendamment de tout soupçon. En Allemagne, la Cour constitutionnelle fédérale avait déjà déclaré la conservation des données inadmissible en 2010. La Cour de justice de l'Union européenne (CJUE) a déjà rejeté à trois reprises la surveillance de masse sans motif et sans soupçon. En 2014, des recourant·e·s ont aussi contesté en Suisse la conservation des données ; le recours a été porté devant la Cour européenne des droits de l'homme (CourEDH), où il est pendant. Il faut s'attendre à ce que la CourEDH confirme sa jurisprudence et juge également contraire aux droits fondamentaux la conservation des données en Suisse. Le service de renseignement ne doit pas pouvoir s'appuyer sur un tel instrument.

Nous demandons:

- Suppression complète de l'exploration du réseau câblé : section 7 entière, art. 39 à 43.
- Suppression de la collecte d'informations fondée sur la conservation des données : art. 26, al. 1, let. a.

Variantes, si l'exploration du réseau câblé n'est pas entièrement supprimée :
Suppression des extensions de l'exploration du réseau câblé :

- Suppression du terme « cyberespace » à l'art. 39, al. 1.
- Annulation de l'extension de la possibilité de prolongation (désormais 6 mois au lieu de 3) à l'art. 41, al. 3.
- Suppression du nouvel instrument d'analyse prévu à l'art. 42, al. 3bis.

5 Clarification des catégories de données et des obligations de suppression qui en découlent pour le Service de renseignement de la Confédération

Jusqu'ici, les données et informations collectées par le service de renseignement étaient enregistrées, selon leur utilisation, dans neuf systèmes d'information différents : l'un pour les informations sur l'extrémisme violent, un autre pour les informations relatives exclusivement à des mesures de police de sécurité, un autre encore pour les données provenant

de sources accessibles au public. Ces multiples réservoirs de données doivent disparaître avec la révision de la LRens.

Selon la nouvelle procédure prévue, le service de renseignement collecterait d'abord autant de données que possible. Ce n'est que dans un second temps que les données qui sont ou pourraient être pertinentes pour ses activités seraient distinguées des données dites administratives (par exemple interventions parlementaires, prises de position, lettres de citoyen·ne·s, demandes d'accès, etc.). Lorsque, dans une étape ultérieure, les données potentiellement importantes pour les activités de renseignement (les « données brutes ») sont traitées plus avant, elles deviendraient des données de travail, conservées plus ou moins longtemps selon leur pertinence.

Pour les données provenant de sources accessibles au public et de mesures de recherche soumises à autorisation, le respect de la limite au traitement des données prévue à l'art. 5, al. 5 LRens ne serait vérifié qu'avant l'utilisation comme données de travail. Cela doit être rejeté. Le respect de l'interdiction de collecter et de traiter des informations sur l'activité politique et sur l'exercice en Suisse de la liberté d'expression, de réunion ou d'association doit aussi être garanti pour les données provenant de sources accessibles au public. Il convient de rappeler les constatations de la Délégation des Commissions de gestion dans son rapport annuel 2019 : lors de son examen, elle avait trouvé un très grand nombre d'articles de journaux, de dépêches d'agences de presse et de textes de sites Internet, et elle avait conclu que la majorité de ces documents n'auraient dû être ni collectés ni traités par le SRC.

Le nouveau système de collecte a pour effet de rendre flou le but pour lequel les différentes données sont recueillies. Cela paraît particulièrement délicat en matière d'extrémisme violent : lors de l'adoption de la LRens en 2017, le législateur avait reconnu que les données en lien avec l'extrémisme violent devaient être traitées dans un système d'information distinct et soumises à des exigences particulièrement strictes en matière de traitement des données. Il entendait ainsi tenir compte de l'expérience selon laquelle le traitement de données dans ce domaine s'était révélé particulièrement sensible sur les plans politique et de la protection des données. Cette séparation opérée pour de bonnes raisons disparaîtrait, selon les projets actuels du Conseil fédéral, avec la nouvelle LRens.

À l'avenir, les données de travail devraient certes être examinées périodiquement quant à leur pertinence. Les données brutes, elles, ne seraient contrôlées que par sondage. Or le projet de loi ne prévoit aucun délai explicite à cet effet. Il renvoie plutôt à des délais de conservation ou de suppression fixés au niveau de l'ordonnance, que le Conseil fédéral peut modifier en tout temps. Il en résulte un risque de stockage démesuré des données, portant atteinte aux droits fondamentaux des personnes concernées par la surveillance. Il est insuffisant de ne soumettre les données brutes qu'à un contrôle par sondage. Il existe ainsi un risque d'accumulation continue de données inutilisées et sans pertinence. Il faut prévoir que ces données elles aussi soient contrôlées périodiquement quant à leur pertinence.

Dans l'état actuel de la révision, il reste également flou à partir de quand les personnes ou organisations concernées peuvent faire valoir un droit d'accès : dès l'entrée dans le système de collecte, après le tri en données brutes, ou seulement lorsque les informations deviennent des données de travail du renseignement ? Il en va de même du contrôle parlementaire : il n'est pas clair s'il a, dès le départ, accès ou connaissance de toutes les données collectées, indépendamment de leur utilisation ultérieure. Or seul un tel accès permet de contrôler de manière fiable si le SRC respecte ses limites légales (pas de surveillance d'activités politiques licites).

Nous demandons:

- Le traitement des données doit dès le départ être clairement lié à une finalité déterminée ; la loi doit garantir que les données ne soient collectées et traitées qu'à des fins de renseignement clairement définies. Les données sans finalité de renseignement suffisante ne doivent pas être collectées.
- Les données en lien avec l'extrémisme violent doivent continuer à être traitées séparément et dans le cadre d'exigences particulièrement strictes en matière de traitement des données.
- Il faut garantir qu'aucun vaste ensemble de données ne se constituent alors pour des motifs flous.
- Pour toutes les données, des délais courts de contrôle et de suppression doivent être prévus au niveau de la loi ; toutes les données, y compris les données brutes, doivent être examinées périodiquement quant à leur pertinence, et non seulement par sondage.
- La limite au traitement des données prévue à l'art. 5, al. 5 LRens doit être respectée dès le départ aussi pour les données provenant de sources accessibles au public et pour celles issues de mesures de recherche soumises à autorisation.
- La loi doit garantir que le droit d'accès s'applique déjà aux données brutes et que le contrôle parlementaire ait lui aussi, dès le départ, accès ou connaissance de toutes les données collectées.

6 IA et profilage dans l'analyse des données

À l'avenir, le service de renseignement devrait disposer d'une base légale pour recourir au profilage au moyen de systèmes automatisés (art. 53). Le service de renseignement entre ainsi dans l'ère de l'IA. La nécessité d'une approche particulièrement prudente et soigneuse ressort clairement de ce qui se passe aux États-Unis, où de tels outils sont utilisés de manière excessive par des autorités de sécurité étatiques, avec des effets dévastateurs et contraires aux droits humains. En Suisse, le Tribunal fédéral a déjà fixé des limites étroites à l'usage d'algorithmes et de big data. Dans son arrêt de 2024 sur la loi lucernoise sur la police,il a relevé que l'usage de systèmes algorithmiques constitue une grave atteinte aux droits fondamentaux et conduit à des décisions difficilement compréhensibles ainsi qu'à de possibles discriminations. Les données en cause ont été obtenues au prix d'atteintes particulièrement graves aux droits fondamentaux, et leur réutilisation

est soumise à des exigences qualifiées. C'est pourquoi il a posé des limites étroites au recours à des instruments automatisés de traitement des données.

Dans le domaine du renseignement, l'usage de l'IA est extrêmement sensible du point de vue des droits fondamentaux. Le recours à de tels instruments nécessite donc des limites claires ancrées dans la loi. Or les explications du Conseil fédéral relatives à cet article ne révèlent aucune conscience des risques liés au profilage ni des mesures de précaution nécessaires.

Un simple article autorisant le recours à l'IA dépourvu de limites et de mesures d'accompagnement serait extrêmement dangereux. Nous recommandons donc les mesures suivantes :

- élaborer un système de réglementation des atteintes aux droits fondamentaux résultant d'instruments automatisés de traitement des données, afin de pouvoir distinguer dans la pratique entre des usages plus ou moins graves de ces méthodes;

- sur cette base, prévoir des restrictions substantielles pour les différents scénarios afin de mieux garantir la proportionnalité des atteintes aux droits fondamentaux;

- renforcer le contrôle indépendant des méthodes utilisées, par exemple en accordant à l'Autorité de surveillance indépendante des activités de renseignement et à la Délégation des Commissions de gestion des compétences approfondies de surveillance, de recommandation et d'instruction.

Nous demandons:

- Supprimer l'art. 53 P-LRens
- A défaut, n'introduire l'art. 53 sur le profilage que si des mesures d'accompagnement (voir ci-dessus) sont simultanément inscrites dans la loi.
- Le cas échéant, demander au sein de la commission des clarifications et rapports approfondis sur cette disposition. Réévaluer ensuite la question.

7 Renforcement des droits d'accès à ses propres données personnelles

La pratique actuelle du SRC en matière d'accès est opaque, insuffisante et plutôt arbitraire. Souvent, il n'accorde l'accès que sous la forme d'une liste qu'il a lui-même établie des entrées enregistrées, sans divulguer intégralement les données traitées ni les pièces correspondantes, ce qui rend impossible de vérifier si l'on a réellement obtenu un accès complet. La loi exige qu'une réponse soit donnée dans les 30 jours ; or le service de renseignement met parfois jusqu'à un an pour le faire – et n'accorde alors l'accès qu'aux

entrées existantes à la date de réception de la demande, donc à des données déjà vieilles de plus d'un an.

Le projet de loi prévoit à l'art. 63a, al. 5 une nouvelle restriction du droit d'accès. Lorsque la communication des renseignements entraîne une charge disproportionnée, le SRC pourrait, pour les données que la requérante ou le requérant a publiées ou remises au SRC, fournir un renseignement sommaire sous la forme d'un index. Cela n'est pas compatible avec le droit au respect de la vie privée et à l'autodétermination informationnelle (art. 13, al. 2 Cst., art. 8 CEDH), sur lesquels repose le droit d'accès aux données. Une autorité qui traite des données ne peut pas opposer aux personnes concernées que la communication de renseignements sur ces données représenterait un effort excessif. On ne voit d'ailleurs pas même en quoi la disposition proposée réduirait réellement la charge de travail : il est plus simple de divulguer les données telles qu'elles sont enregistrées que d'établir un index de ces données.

Nous demandons:

- Un accès complet à ses propres données personnelles traitées par le SRC, ainsi qu'aux pièces correspondantes.
- Aucune limitation de l'accès à des listes établies par le SRC, à de simples aperçus ou à un index.
- Le respect du délai légal de 30 jours et la communication de l'ensemble actuel des données conservées.
- Renoncer à la restriction du droit d'accès prévue à l'art. 63a, al. 5, P-LRens ; une charge prétendument disproportionnée ne doit pas justifier une limitation de l'accès.