Loi sur le renseignement : menace pour les droits fondamentaux?

« Renoncer à sa liberté c'est renoncer à sa qualité d'homme, aux droits de l'humanité, même à ses devoirs. »

Jean-Jacques Rousseau, *Du contrat social*

Florian Schweri

Collège Voltaire

Travail de maturité

octobre 2016

Table des matières

Introduction **3**

1. Dans quel contexte se trouve l'Occident ? **4**

1.1. Sous quelles formes le terrorisme se manifeste-il ? **4**

1.2. Comment contrer les groupes terroristes ? **4**

1.3. Comment réagit l'Occident: les Etats-Unis, l'Europe et la Suisse ? **5**

2. Qu'est-ce que la LRens ? **8**

2.1. Quel but et quelles nouvelles compétences pour le SRC ? **8**

2.2. Pourquoi un référendum ? **9**

3. Une loi à l'encontre des principes démocratiques **10**

3.1. Démocratie et collusion **10**

3.2. Le secret, une part de l'identité suisse **13**

3.3. Jusqu'où les atteintes aux droits fondamentaux sont-elles proportionnées aux impératifs de sécurité ? **14**

3.3.1. Protection des données : de vraies garanties ? 15

3.3.2. Soupçon généralisé : une menace pour la présomption d'innocence ? 16

3.3.3. Manque de précisions et abus potentiels 19

4. Votation populaire : pourquoi un tel résultat ? **20**

Conclusion **21**

Bilan personnel **23**

Lexique **24**

Bibliographie **25**

Annexes **27**

Annexe I: Articles de loi **27**

Annexe II: Revue de presse **28**

Annexe III: Questions des interviews **31**

Introduction

Avec les attentats contre les tours jumelles de New-York le 11 septembre 2001, il y a 15 ans, le monde occidental s'est découvert la cible d'attentats meurtriers, remettant en question les fondements des démocraties qui le composent, autant par l'action directe des terroristes que par les réponses des gouvernements. Les législations se sont adaptées à cette nouvelle menace devenue depuis omniprésente et ont remis en question – de l'intérieur – les libertés des citoyen-ne-s en autorisant parfois une surveillance préventive, voire de masse.

Ainsi, les gouvernements ont d'eux-mêmes opposé sécurité et liberté, amenant à hiérarchiser ce qui se trouve pourtant être deux droits fondamentaux interdépendants.

Les images d'attentats reviennent aujourd'hui de plus en plus régulièrement sur nos écrans, dans nos journaux et dans notre quotidien, avec leur lot de morts, de souffrance et de tristesse, d'incompréhension aussi face à la barbarie humaine. Notre monde change et nous nous habituons malheureusement à devoir vivre avec ces actes qui dépassent notre entendement et notre capacité à comprendre comment certains peuvent en venir à commettre de telles atrocités.

Face à la progression de ce type d'actions, le désarroi et le rejet ne peuvent toutefois constituer des réponses satisfaisantes ; nous nous devons au contraire de réagir dans le respect de nos valeurs, de nos convictions démocratiques et de notre Etat de droit.

En Suisse, une loi – *Loi fédérale sur le renseignement*, LRens* – a été votée au Parlement pour renforcer les pouvoirs du *Service de renseignement de la Confédération* (SRC*). Cette loi fait peser un risque sur les droits fondamentaux des citoyen-ne-s en utilisant la peur comme argument. La question principale qui se pose est alors de savoir si ce texte est proportionné aux buts qu'il vise et jusqu'à quel point nous sommes prêt-e-s à livrer des informations sur nous dans le but de nous « défendre ». Malgré les dérives dont a été victime le SRC, pouvons-nous faire confiance à ce service pour assurer la protection de notre pays mais aussi celle des données qu'il enregistrera sur chacun de nous ?

Répondre à ces questions est essentiel pour savoir si nous devons accepter le risque d'un Etat policier dont l'affaire des fiches nous a démontré le manque de transparence et de discernement entre le respect de la démocratie et la peur irraisonnée d'une éventuelle menace.

L'analyse de ces points doit passer tout d'abord par une présentation du contexte sécuritaire dans le monde, et plus particulièrement en Occident, avant d'aborder le contenu et l'analyse juridique de la loi par rapport à nos droits fondamentaux.

Pour ce faire, les publications officielles et notamment la Feuille fédérale, dans laquelle ont été publiés la loi et le message du Conseil fédéral y relatif, ainsi que de nombreux articles de presse sont nécessaires pour comparer à la fois les données brutes – comme le texte de loi – et les interprétations qui pourraient en être faites, dont le message et les articles fournissent certains exemples. S'agissant d'un sujet très actuel en Europe suite aux attentats de ces derniers mois et en Suisse en raison de la votation populaire sur la LRens, les articles de presse constituent un réservoir important d'idées et de visions diverses, et parfois critiques, sur la question.

---

* Les mots suivis d'un astérisque sont explicités dans le lexique

1. Dans quel contexte se trouve l'Occident ?

1.1. Sous quelles formes le terrorisme se manifeste-il ?

Le terrorisme est une pratique revendicatrice utilisant la violence, visant à obtenir un changement au niveau politique et qui existe depuis plusieurs siècles. Les premières formes de terrorisme sont les régicides dont le but était d'assassiner le roi et ainsi faire tomber le pouvoir en place. Il s'agissait alors d'attentats préparés dans un but précis et ciblés sur une personne en particulier. [1]

Depuis, le monde a évolué et nous sommes passés de ces attentats à caractère politique à du terrorisme de masse. Les actes commis ces dernière années, que ce soit à New-York, Londres, Paris ou encore Nice, le montrent : certaines organisations sont devenues des usines de la terreur.

Nous devons aujourd'hui apprendre à nous protéger et à faire face à ces nouvelles menaces, sans pour autant suivre certains gouvernements dans le piège de la suspicion systématique. Au terrorisme de masse ne doit pas répondre la surveillance de masse, qui est tout aussi dangereuse, sur un autre plan : celui de la liberté.

Bien que les terroristes ne soient pas tous de confession musulmane, c'est aujourd'hui le terrorisme qualifié d'*islamiste* qui est le plus connu et redouté. Il est vrai que les exemples d'attentats commis par leurs auteurs au nom de l'Islam sont nombreux, et ce surtout depuis le 11 septembre 2001. Les récents attentats commis à Paris en janvier et novembre 2015, à Nice, ou encore à Ansbach en 2016 en sont les derniers exemples, en Occident du moins.

Les organisations terroristes se livrent une guerre d'influence pour le contrôle tant des régions sous leur domination que des fidèles qu'elles appellent à les rejoindre dans un exil qu'elles nomment *djihad*. Elles rivalisent de moyens de promotion de leur cause, notamment au niveau visuel, avec la production de films de propagande destinés en priorité aux jeunes qu'elles espèrent convaincre d'entrer dans leurs rangs.

Les principales organisations de ce type sont actives dans des pays politiquement instables où il est relativement aisé de se fournir en armes et en combattants, suite notamment aux diverses révolutions qui ont secoué ces régions. Les pays actuellement en guerre tels que la Syrie sont donc, pour elles, un terrain de prédilection.

1.2. Comment contrer les groupes terroristes ?

Cette situation et le nombre de jeunes qui décident de quitter leur pays pour aller combattre dans les rangs de *l'Etat islamique*, aussi appelé *Daech*, qui est la principale organisation terroriste contre laquelle les Etats occidentaux se battent à l'heure actuelle[2], pousse les gouvernements à réagir et à « déclarer la guerre au terrorisme ». Pour cela, ils durcissent les lois, en créent de nouvelles et prennent, dans l'urgence, des mesures visant à intercepter les combattants lors de leur retour ainsi qu'à prévenir leur départ.

---

[1] Cette vision et cette histoire du terrorisme ont été développées par Robert Badinter, ancien ministre français de la justice, lors d'une conférence tenue le 11 novembre 2015 dans le cadre de la 48e session des Rencontres internationales de Genève.

[2] Il en existe bien d'autres mais c'est au nom de ce groupe qu'ont été commis les derniers attentats sur sol occidental.

Par ailleurs, certains gouvernements ont également décidé de participer au combat armé, directement dans les pays où ces organisations sont actives, et notamment en Syrie et en Irak. Sur le plan militaire, la coopération internationale fait toutefois défaut et plusieurs visions s'affrontent. Certains Etats demandent de combattre à la fois les groupements terroristes et le gouvernement de Bachar Al-Assad, alors que d'autres préfèrent s'associer à ce dernier pour ramener la région à une relative paix.

La controverse porte donc, en partie, sur la définition et sur la liste des groupes à combattre. Si certains estiment que seuls les djihadistes doivent être combattus, d'autres intègrent également l'armée rebelle syrienne dans les cibles à détruire. Ces différents points de vue crispent les pays et provoquent des tensions sur la scène internationale.

L'intervention de la Russie dès le 30 septembre 2015 contre *l'Etat islamique* et les rebelles syriens a ajouté aux tensions déjà existantes avec les pays européens et les Etats-Unis au sujet de l'annexion de la Crimée en 2014. La coopération militaire a pris beaucoup de temps pour se mettre en place, en provoquant parfois des incidents sur le terrain avec, par exemple, un avion russe abattu par l'armée turque.[3]

1.3. Comment réagit l'Occident: les Etats-Unis, l'Europe et la Suisse ?

Suite aux attentats contre le World Trade Center le 11 septembre 2001, les Etats-Unis ont déclaré une véritable guerre au terrorisme. Cette dernière a permis le développement de pratiques non conformes au cadre légal. L'administration Bush a créé notamment le *USA Patriot Act** qui permet aux services de sécurité américains d'accéder sans mandat et secrètement à des données informatiques détenues par des entreprises.

Cette loi, bien que jugée liberticide par de nombreux juristes et défenseurs des libertés individuelles, a permis aux services de sécurité des Etats-Unis de surveiller un grand nombre de personnes au motif de la lutte antiterroriste. D'énormes quantités de données personnelles ont ainsi pu être recueillies et stockées.

De plus, l'association des services de renseignement de plusieurs pays au sein de programmes d'espionnage communs a permis la mise en réseau de ces informations mais également la mise en réseau de certaines sources et a donc amené une augmentation spectaculaire du nombre d'informations récoltées.

Par ailleurs, la *National Security Agency* (NSA*) a profité de ce contexte pour élargir ses capacités en matière de surveillance. C'est ce qu'Edward Snowden a révélé en 2013 après être parvenu à quitter les Etats-Unis en emportant des documents confidentiels relatifs à divers programmes de surveillance.

Même si ces collaborations interservices existaient déjà auparavant avec des programmes d'interception des communications tels que le réseau *Echelon*, de nouveaux partenariats se sont développés avec l'apparition de *Tempora*[4] par exemple,

---

[3] Voir notamment : Radio Télévision Suisse, **RTS *[En ligne]***, http://www.rts.ch/info/monde/7279618-la-turquie-se-met-la-russie-a-dos-apres-avoir-abattu-un-de-ses-avions.html (site consulté le 11 septembre 2016)

[4] Le projet Tempora vise à intercepter et stocker l'ensemble des données transitant par les câbles sous-marins entre l'Europe et les Etats-Unis, voir : Groupe Altice Média, **L'express *[En ligne],*** http://lexpansion.lexpress.fr/high-tech/operation-tempora-comment-les-britanniques-depassent-les-americains-pour-espionner-internet_1434134.html (site consulté le 11 septembre 2016)

qui, bien qu'étant un projet du *Government Communications Headquarters* (GCHQ*) britannique, partage beaucoup de données avec la NSA américaine.

Au niveau européen, une évolution similaire a eu lieu à partir des attentats commis contre *Charlie Hebdo* en janvier 2015. La France a promulgué une loi étendant les pouvoirs de ses services de renseignement. On peut constater que toutes les lois de ce type reprennent des formulations et des mesures communes telles que la « lutte contre le terrorisme » et l'accès plus large à un plus grand nombre de données, ainsi qu'une conservation plus longue de celles-ci.

On retrouve également des idées plus politiques que justifiées par les circonstances. Un exemple flagrant est l'interdiction du burkini et/ou de la burqa en tant que signe d'allégeance à une vision extrémiste de la religion (sans ouvrir ici le débat sur ces vêtements par rapport à la condition de la femme). Ces interdictions découlent d'un amalgame dangereux entre religion et violence alors qu'objectivement le fait de se dissimuler le visage ou le corps pour des raisons religieuses ne met pas plus en danger l'ordre public que de porter une cagoule à cause du froid en hiver. Seules l'animosité voire la haine de certaines personnes spectatrices de cela provoquent des troubles, ce sont donc ces personnes qui doivent faire l'objet de mesures et non celles dont le seul « délit » est de ne pas avoir respecté les critères subjectifs de leurs spectateurs. En France, la déchéance de nationalité pour les personnes ayant commis des actes terroristes et possédant une double-nationalité a failli être acceptée, et, dans nombre d'autres pays, des restrictions de l'immigration au nom de la sécurité l'ont été également ; partout on retrouve la stigmatisation d'une catégorie de la population, le plus souvent les étrangers, alors que le terrorisme n'a pas de nationalité.

En effet, on retrouve au sein de Daech des combattants de nombreux pays (27'000 personnes de 86 pays[5]). Les djihadistes viennent de partout, et le principal constat que l'on peut faire, vu la situation, est bien le suivant : nous sommes aujourd'hui incapables de stopper ces départs vers les zones de guerre car le terrorisme n'est plus l'apanage de groupes radicaux qui embrigadent les jeunes de leur région. Internet et le développement des nouvelles technologies ont mis l'idéologie djihadiste, comme toutes les autres d'ailleurs, à la portée de n'importe quelle personne sur la planète.

La grande difficulté de la lutte antiterroriste réside dans le fait que la répression ne fonctionne pas et pour cause, punir un terroriste nécessite de l'intercepter alors que son but est de mourir en martyr. On ne peut donc que dans de très rares cas punir pénalement un auteur d'attentat et le menacer de sanctions n'a dès lors pas réellement d'intérêt dissuasif.

De cette impossibilité de réagir de manière satisfaisante découle un besoin de plus en plus fort de prévention. Cependant, alors que le terrorisme islamiste, puisque c'est celui dont il est question ici, est connu depuis plusieurs années, nous commençons seulement à mettre en place des structures telles que des centres de déradicalisation et à chercher à prévenir le départ des sympathisants aux groupes terroristes. Mais dans le même temps nous continuons à emprisonner les personnes de retour de régions en guerre, alors que nous savons depuis des siècles que la prison est l'école du crime, l'endroit où peuvent se former les futurs meneurs de ces mouvements radicaux.

---

[5] Le Huffington Post SAS, **Le Huffington Post *[En ligne]***, http://www.huffingtonpost.fr/2015/12/08/jihadistes-syrie-combattants-etrangers-nombre-origine-etat-islamique-daech_n_8747236.html (site consulté le 1er septembre 2016)

C'est bien la raison pour laquelle nous devons envisager d'autres options et moyens, car s'il nous est impossible de punir le terrorisme, nous pouvons et devons nous donner les moyens de le prévenir en parvenant à proposer une politique globale, construite, ciblée et réfléchie face à une situation, il est vrai, sans précédent.

En Suisse, certains ont dénoncé le retard de la législation. En effet, il est apparu suite aux attentats de janvier 2015 à Paris que notre pays ne disposait d'aucune législation spécifiquement antiterroriste. En effet, « tout acte terroriste matériel – homicide, prise d'otages, destruction d'infrastructures, etc. – est déjà couvert par une disposition existante du Code pénal »[6], rendant inutile la création d'une disposition légale spécialement adaptée.

On constate cependant qu'une loi spéciale[7] est entrée en vigueur le 1er janvier 2015 pour interdire certaines organisations, et notamment Al-Qaïda et Daech.

Par ailleurs, une loi sur le renseignement (LRens) a été votée par le Parlement fédéral le 25 septembre 2015[8] afin d'octroyer plus de pouvoirs au Service de renseignement de la Confédération (SRC), dans le but de lutter de manière plus efficace contre le terrorisme.

---

[6] Frédéric Bernard *cité par :* **MISSON Joëlle,** « La Suisse dans le viseur des terroristes », *in GHI*, 21-22 janvier 2015, p. 3

[7] Dénommée : *Loi fédérale interdisant les groupes «Al-Qaïda» et «Etat islamique» et les organisations apparentées* (RS 122) du 12 décembre 2014

[8] Curia Vista objet 14.022, accepté par 145 voix contre 41 et 8 abstentions au Conseil national ; 35 voix contre 5 et 3 abstentions au Conseil des Etats

2. Qu'est-ce que la LRens ?

2.1. Quel but et quelles nouvelles compétences pour le SRC ?

La nouvelle LRens vise à donner au SRC un nouveau cadre de travail aujourd'hui défini par la *Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure* (LMSI*) et la *Loi fédérale sur le renseignement civil* (LFRC*). Le but de cette loi est de renforcer la sécurité de la Suisse en donnant aux agents du renseignement des capacités nouvelles et étendues, notamment en matière de surveillance.

La LRens accorde plus de pouvoir aux agents du SRC notamment au niveau des écoutes et d'autres mesures de surveillance, dont certaines jugées intrusives. En effet, plusieurs de ces moyens seront subordonnés à l'aval du *Tribunal administratif fédéral* (TAF*) et du chef du *Département fédéral de la défense, de la protection de la population et des sports* (DDPS) car ils entraînent une violation de la sphère privée de la personne surveillée. Parmi ces moyens figurent en premier lieu les observations de lieux privés, les écoutes ainsi que l'utilisation de chevaux de Troie fédéraux (GovWares) pour surveiller secrètement et à distance des ordinateurs.

En ce qui concerne les écoutes, la nouvelle loi autorise la surveillance d'Internet par des mots-clés. Cette pratique est dénoncée car elle ne permet pas, au moment de la récolte, de savoir si les informations interceptées proviennent d'une personne soumise à une mesure de surveillance ou non. Il est en effet nécessaire, pour effectuer le tri de ces informations, de récupérer d'abord tout le trafic Internet pour ensuite pouvoir en extraire certaines communications répondant à divers critères.

Ainsi, cette façon de procéder mettrait à mal la sphère privée car elle permettrait et nécessiterait d'opérer une surveillance de masse de ce réseau et donc d'espionner sans fondement et sans autorisation des personnes n'ayant rien à se reprocher.

Les GovWares, abréviation de « Government Software », sont des logiciels espions destinés à la surveillance à distance de systèmes informatiques. Le but principal est de pouvoir procéder à l'écoute de communications cryptées, de « rechercher les informations […] qui ont été transmises à partir de ces systèmes »[9] ou de « perturber, empêcher ou ralentir l'accès à des informations »[10].

En effet, les technologies de cryptage actuelles proposent des algorithmes suffisamment puissants pour empêcher un décryptage par *force brute**. Il devient donc nécessaire de pouvoir accéder à ces informations avant qu'elles ne soient rendues illisibles, c'est-à-dire sur le dispositif qui les transmet ou sur celui qui les reçoit, après que ce dernier les ait décryptées.

Le risque de dérives existe, et notamment le fait que ces dispositifs soient utilisés par exemple pour surveiller un local par le microphone et/ou la caméra de l'ordinateur cible, bien que ceci ne soit pas autorisé par la loi. Pour éviter cela, des mesures pourraient être prises afin de contrôler la légalité de la surveillance, telles que la journalisation exhaustive[11] des opérations. Il est en effet particulièrement important de garantir que l'usage de ces moyens sera légale et légalement autorisée car, dans le cas contraire, il existe un risque que les informations récoltées ne puissent pas être

[9] LRens art. 26 al. 1 let. d
[10] ibid.
[11] La journalisation consiste en l'inscription dans un fichier de l'ensemble des opérations effectuées, en l'occurrence par un programme informatique, à des fins de contrôle.

utilisées comme moyen de preuve devant un tribunal[12], ce qui amènerait, en l'absence d'autre éléments, à faire acquitter un terroriste potentiel.

Des dispositifs de ce type seront également mis à disposition du *Service de surveillance de la correspondance par poste et télécommunications* (Service SCPT*), dans le cadre de la révision de la *Loi fédérale sur la surveillance de la correspondance par poste et télécommunications* (LSCPT*). En revanche, contrairement au SRC, ce service ne pourra mettre en œuvre de tels systèmes que sur ordre du Ministère public et après autorisation par un tribunal des mesures de contrainte. Il s'agit là d'une différence de poids, valable d'ailleurs pour les autres mesures de surveillance, entre le Service SCPT et le SRC. En effet, le Service SCPT agit sur ordre des autorités judiciaires mais n'est pas proactif, alors que le SRC, lui, demande les autorisations aux juges au lieu de recevoir leurs instructions. Il y a donc un fonctionnement totalement inversé entre ces deux entités et c'est une des raisons qui provoque la méfiance vis-à-vis du renseignement. Par ailleurs, une collaboration entre les deux départements dont dépendent ces services (DDPS pour le SRC et *Département fédéral de justice et police*, DFJP, pour le Service SCPT) en vue de l'acquisition d'un GovWare commun n'est apparemment pas à l'ordre du jour.[13]

2.2. Pourquoi un référendum ?

L'inscription de ces mesures dans une loi a amené les Verts, les Jeunesses socialistes et d'autres associations de lutte pour les droits fondamentaux à lancer un référendum, réunis au sein d'un mouvement, baptisé *Alliance contre l'Etat fouineur**, que d'autres partis et organisations, telles que Syndicom, le Parti socialiste ou le *Groupe pour une Suisse sans Armée* (GSSA*), ont ensuite rejoint.

Le référendum a formellement abouti le 2 février 2016 avec 56'055 signatures validées sur 56'347 déposées[14]. Il a donc été décidé de soumettre la loi au vote du peuple le 25 septembre 2016, soit, par hasard, un an jour pour jour après son adoption au Parlement.

Les événements, et notamment les attentats au Bataclan, ont lancé le débat sur le bien-fondé du référendum. En effet, la question a été posée de savoir s'il n'était pas irresponsable de le maintenir vu le climat.[15]

---

[12] **Service SCPT *[En ligne]***, https://www.li.admin.ch/fr/documentation/faq (site consulté le 07 septembre 2016)
[13] ibid.
[14] Communiqué de presse de la Chancellerie fédérale du 04 février 2016 et Feuille fédérale FF 2016 700
[15] **AUBERT Laurent**, « L'« Etat fouineur » fait-il plus peur que les attentats ? », *in* Tribune de Genève, 25 novembre 2015, p. 3

3. Une loi à l'encontre des principes démocratiques

Le but principal de la LRens est de réviser le cadre légal actuel pour offrir plus de moyens au SRC afin d'agir de manière précoce et préventive. Selon Hugues Hiltpold, conseiller national PLR, cela est nécessaire pour éviter que « la Suisse [ne devienne] la plaque tournante de réseaux [terroristes] […] car les criminels vont à l'endroit où ils ont le moins de risque d'être attrapés. »[16] Cependant, cette loi est sujette à controverse pour plusieurs raisons notamment, d'un point de vue juridique, son manque de précision. Comme le soulève François Charlet, juriste spécialisé en droit des technologies, il s'agit d'une loi très technique avec beaucoup de renvois à des articles qui eux-mêmes renvoient à d'autres ; mais surtout, il manque les définitions des termes qui y sont utilisés. Il n'existe pas comme dans d'autres lois, un article qui définit ce que sont le « terrorisme », l'« urgence », la « menace grave et imminente »[17]. La loi pourrait donc être interprétée de plusieurs manières, ce qui crée une incertitude juridique.

Concernant les atteintes aux droits fondamentaux, il est évident que certaines des mesures qui pourraient être prises seront extrêmement intrusives, notamment en matière de protection de la sphère privée. Ainsi, la question principale qui se pose n'est pas de savoir si la loi porte atteinte aux droits fondamentaux, mais plutôt dans quelle mesure et si cela est proportionnel au but poursuivi. S'il ne fait aucun doute que la sécurité, face au terrorisme notamment, doit être assurée, il est légitime de se poser la question de l'adéquation des mesures envisagées et du service qui serait chargé de les mettre en œuvre.

3.1. Démocratie et collusion

Notre pays est souvent cité en exemple pour sa démocratie directe et la grande marge de manœuvre dont disposent les citoyennes et les citoyens dans la vie politique. Cependant, le fonctionnement d'un tel système nécessite une transparence d'autant plus grande. En effet, pour pouvoir apprécier correctement une situation donnée, le peuple doit disposer des informations qui lui permettent de le faire. Cela est particulièrement important du point de vue du contrôle démocratique des services de l'Etat. Ces institutions étant financées par les impôts pour être mises à la disposition des résidents, il est juste que ces derniers puissent savoir ce qui est fait de leur argent et comment travaillent celles et ceux qui veillent sur eux. Pour François Charlet, « il faudrait trouver un compromis entre la sécurité nationale et la transparence » car « [nous payons] nos anges gardiens mais j'aimerais savoir comment ils [travaillent]. »[18]

Ce besoin de contrôle démocratique et de transparence va à l'encontre du secret entretenu autour des services de renseignement et, dans le cas particulier de la Suisse, du SRC. En effet, les actions de ces entités nécessitent, pour être menées à bien, de pouvoir être réalisées de manière discrète. C'est d'ailleurs le rôle des services *secrets*. Les deux – transparence et discrétion – ne sont pourtant pas totalement incompatibles. Il est évident qu'un service tel que le SRC ne peut pas être aussi transparent que d'autres vu les intérêts qu'il défend. Cependant, il faut distinguer ce qui porte objectivement atteinte à la sécurité nationale – tel que la divulgation des noms des personnes surveillées alors que la surveillance est en cours – et des données brutes qui permettraient de prendre la mesure du travail réalisé sans trahir le *secret défense*.

---

[16] **HILTPOLD Hugues**, conseiller national, interview le 03 août 2016
[17] **CHARLET François**, juriste spécialisé en droit des technologies, interview le 18 août 2016
[18] ibid.

Il serait par exemple imaginable – comme certaines personnes l'avaient demandé lors de la procédure de consultation[19] – de publier un rapport présentant les chiffres bruts concernant le nombre de surveillances demandées, autorisées, effectuées, les types de crimes concernés, etc.

Pour pallier à l'absence de tels contrôles, des mesures sont prévues dans la loi, comme la création d'une *autorité de surveillance indépendante*, la haute surveillance parlementaire ou l'autorisation de certaines mesures de recherche par le TAF et le chef du DDPS. Ces mesures de contrôle sont cependant relativement faibles en regard des activités à surveiller. De plus ces entités ne sont pas forcément les mieux placées pour garantir un contrôle efficace.

Tout d'abord, concernant l'autorité de surveillance indépendante instituée par l'art. 76 de la loi, on constate en premier lieu, comme le relève Lisa Mazzone, conseillère nationale verte, que son président est nommé par le Conseil fédéral[20], sur proposition du DDPS, donc par les personnes qu'il devra surveiller. Il n'est pas irréaliste d'imaginer – bien que, par la suite, l'autorité soit indépendante – que la nomination de son chef fera l'objet d'un choix avant tout politique et que ce ne sera pas le plus farouche opposant au SRC qui sera porté à ce poste. Par rapport à son travail, l'autorité en question devra « [informer] le DDPS de ses activités dans un rapport annuel à publier. »[21] ; on imagine donc un document librement accessible au public et non pas réservé à une catégorie restreinte de personnes. Cependant, comme seul le DDPS est explicitement mentionné, la prudence est de mise ; d'autant plus vu l'al. 6 qui précise que l'autorité transmettra le résultat de ses contrôles *au DDPS*. Les informations concernant ce rapport sont donc assez vagues même si, selon la brochure d'information, « [l']autorité […] publiera chaque année un rapport sur ses activités. »[22]. Pour accomplir son travail, l'entité aura de plus accès « en ligne aux données sensibles »[23]. A moins que tous les membres de cet organe ne soient des experts de la sécurité informatique qui sachent se protéger efficacement lors de telles opérations, cela ouvre une brèche dans la sécurité des données détenues par le SRC. D'une manière générale, le simple fait de stocker ces dernières sur des serveurs reliés à internet constitue une faille en lui-même.

Concernant la *haute surveillance parlementaire*, il s'agit d'une mesure déjà existante qu'il est important de conserver pour maintenir un certain contrôle par des représentants du peuple sur le SRC. Il ne faut cependant pas oublier que ces personnes ne sont pour la plupart pas expertes de la sécurité ni des questions de renseignement, dans la mesure où la Suisse dispose d'un parlement de milice. Il convient donc de relativiser le rôle de garant de cette surveillance sachant que les membres du Conseil national et du Conseil des Etats qui l'exerceront sont également sollicités dans d'autres commissions comme en dehors de leur mandat parlementaire.

Enfin, concernant non plus les contrôles après coup mais les autorisations de *mesures de recherche soumises à autorisation*, c'est le TAF qui devrait statuer sur les demandes, puis le chef du DDPS qui devrait les avaliser. La procédure d'autorisation (définie aux art. 29 et 30 LRens) suivrait chronologiquement l'ordre suivant:

---

[19] Voir les positions de DigGes p. 37 et de PP2 p. 64 dans : **SRC**, *Loi sur le renseignement (LRens) Rapport sur les résultats de la procédure de consultation*, septembre 2013
[20] **MAZZONE Lisa**, conseillère nationale, interview le 01 septembre 2016
[21] LRens, art. 78 al. 3
[22] **Chancellerie fédérale**, *Votation populaire du 25 septembre 2016 Explications du Conseil fédéral*, Berne, Chancellerie fédérale, 2016, p. 28
[23] LRens, art. 78 al. 5

1. Demande du SRC au TAF
2. Décision du TAF
3. Aval du chef du DDPS, après *consultation* des chef-fe-s du *Département fédéral des affaires étrangères* (DFAE) et du DFJP (Les chef-fe-s de ces trois départements constituent la *Délégation du Conseil fédéral pour la sécurité**)

Si, de prime abord, il paraît rassurant que les mesures en questions soient soumises à une autorisation judiciaire et une autorisation politique, la lecture détaillée et attentive de la loi fait apparaître les faiblesses de ce système. Il faut en premier lieu noter que le « président de la cour compétente du TAF statue en tant que juge unique »[24], ce qui ne permet pas une confrontation des points de vue juridique tel que ce serait le cas si plusieurs juges devaient trancher. De plus, il faut remarquer que la cour compétente n'est pas définie, ce qui viendra probablement ensuite dans l'ordonnance d'application mais il aurait été intéressant et plus sûr de l'inscrire directement dans la loi ; cela rejoint un des problèmes principaux de la LRens : son manque de définitions. En second lieu, il faut noter le fait que le chef du DDPS ne devra que *consulter* ses collègues du DFAE et du DFJP, cela ne leur donnant pas la capacité de rendre une décision contraignante. Rappelons encore que la principale motivation de cette loi est la lutte contre le terrorisme et qu'il est assez illusoire de penser qu'un conseiller fédéral prenne le risque de ne pas avaliser une demande de surveillance au risque de voir un terroriste commettre un attentat et causer potentiellement de nombreuses victimes.

Par ailleurs, pour en revenir au TAF, il est intéressant de remarquer que l'art. 83 traitant des droits de recours précise en son al. 1 que « Toute décision rendue par une autorité fédérale en vertu de la présente loi peut faire l'objet d'un recours devant le TAF. ». Si Hugues Hiltpold estime que « [le fait de pouvoir faire opposition] est un garant de dérives »[25], cela pose un problème de collusion, voire de conflit d'intérêt. En effet, dans le cas des recours contre les surveillances, comment un tribunal ayant autorisé la mesure pourrait-il traiter de manière équitable et impartiale un recours contre sa propre décision ? La question de la collusion se pose ici de manière concrète car le premier cas se présentant dans une telle situation pourrait aboutir à une décision d'une instance supérieure au TAF qui invaliderait les jugements précédents en raison de ces conflits d'intérêt, ce qui pourrait former une dangereuse jurisprudence dans le cas, par exemple, où la Cour européenne des droits de l'Homme (CEDH) venait à reconnaître le conflit d'intérêt en question.

Il est d'ailleurs important de noter que, lors de la procédure de consultation sur le projet de loi, le TAF lui-même a déclaré « qu'il pourrait être problématique, dans certains cas, d'interjeter recours à la chambre compétente contre des décisions rendues justement par le président de la chambre concernée »[26]. Pour sa part, le Tribunal fédéral (TF) ajoute que « le droit de recours proposé est contraire aux voies de recours générales du Tribunal fédéral. »[27] Il est inquiétant de constater que les prises de position de deux des plus hautes instances judiciaire du pays ont été ignorées et même que le droit de recours prévu a été affaibli entre le projet de loi et le texte voté au Parlement. En effet, le projet initial prévoyait à l'art. 71 al. 1 de pouvoir intenter un recours contre « toute décision rendue par une autorité fédérale […] et tout ordre d'effectuer une mesure de recherche soumise à autorisation »[28], alors que le texte adopté au vote final ne parle

---

[24] LRens, art. 29 al. 2
[25] **HILTPOLD Hugues**, op. cit., n. 16
[26] **SRC**, op. cit., n. 19, p. 61
[27] ibid.
[28] *Loi sur le renseignement (LRens)* projet du 08.03.2016 soumis à la procédure de consultation

plus que des décisions rendues par une autorité fédérale[29] et qu'il reste indiqué à l'al. 3 que « le délai de recours contre l'ordre d'effectuer une mesure de recherche soumise à autorisation commence à courir le jour qui suit la notification de la mesure », ce qui sous-entend que ce type de décisions pourrait tout de même être sujet à recours. De nouveau, on retrouve ici un problème de clarté et de contradictions entre dispositions, qui est récurrent tout au long de la lecture de la loi.

Le Conseil fédéral n'a sciemment pas tenu compte des observations du TAF et du TF comme le démontre son message adressé au Parlement pour appuyer le projet de loi et dans lequel il explique avoir décidé de ne pas suivre la proposition du TAF (qui envisageait de confier les recours au *Tribunal pénal fédéral*, TPF) ceci en argumentant que « [le Conseil fédéral tenait] aussi à concentrer les compétences juridiques et techniques pour l'appréciation des questions liées au renseignement au sein du Tribunal administratif fédéral. »[30] et que « les avantages de la concentration de la procédure dans le domaine du droit administratif l'[emportaient] clairement »[31] sans avoir pris la peine de détailler lesdits avantages. De même, alors que le rapport sur la procédure de consultation reconnaît que « l'on ne résoudrait pas davantage [le] problème [de conflits d'intérêts] en instituant une autre chambre du Tribunal administratif fédéral pour recevoir ledit recours »[32], le message du Conseil fédéral répond avec légèreté qu'« une réglementation appropriée des compétences au sein du Tribunal administratif fédéral permettra le cas échéant d'éviter d'éventuels conflits d'intérêts »[33]. La position du TF est, quant à elle, totalement passée sous silence alors qu'elle rejoint celle du TAF, ce qui devrait interpeller d'autant plus sachant que le TF est la plus haute instance judiciaire nationale.

3.2. Le secret, une part de l'identité suisse

En Suisse, contrairement à d'autres pays, le chiffrement[34] des communications n'est pas un délit. Lié à une certaine tradition du secret, notamment bancaire, cette situation a permis l'implantation de certaines entreprises sur sol helvétique dans le but de profiter des lois protégeant efficacement les informations. La loi et les conditions amènent donc en l'occurrence un avantage concurrentiel à notre pays.

On peut citer dans le domaine des communications l'exemple de Protonmail qui déclare sur sa page d'accueil :

> *« ProtonMail est basé en Suisse et tous nos serveurs sont situés en Suisse. Cela signifie que toutes les données de l'utilisateur sont protégées par des lois strictes de confidentialité Suisse (sic). »*[35]

Dans le cas d'espèce, la Suisse et sa législation sont clairement un atout marketing mis en avant. La Suisse devient ainsi une sorte de coffre-fort numérique. Vu cette tradition du secret entretenue depuis de nombreuses années, l'acceptation de la LRens en tant que loi allant à l'encontre de la sphère privée dénoterait un changement,

---

[29] LRens art. 83 al. 1
[30] **Conseil fédéral**, *Message concernant la loi sur le renseignement* du 19 février 2014 (FF 2014 2029, p. 2131)
[31] ibid.
[32] **SRC**, op. cit., n. 19, p. 61
[33] **Conseil fédéral**, op. cit., n. 30, p. 2131
[34] Le chiffrement consiste à rendre illisible ses communications en utilisant des techniques et algorithmes permettant d'en dissimuler le contenu.
[35] Proton Technologies AG, **Protonmail *[En ligne]***, https://protonmail.com/fr/ (site consulté le 1er septembre 2016)

ou du moins une évolution, dans la mentalité de la population sans signifier pour autant une volonté d'abandonner cette tradition du secret ; comme le relève Hugues Hiltpold « ce qui est bouleversant dans la mentalité suisse est de donner la possibilité d'avoir une action proactive et pas uniquement réactive. »[36]. Dans cette évolution, le contexte général en Occident joue vraisemblablement un rôle fondamental, notamment les actes terroristes commis par les djihadistes. Pour prendre l'exemple d'un pays voisin, selon le Huffington Post, 1700 Français-es combattent dans les organisations djihadistes.[37] La situation en Suisse se présente de manière bien différente puisque seuls 77 personnes sont parties rejoindre des zones de combat depuis 2001.[38]

De plus, il faut noter que le chiffrement des communications, présenté comme un obstacle par les services de sécurité, est un outil essentiel de notre fonctionnement démocratique. En effet, c'est le chiffrement qui permet aux autorités de communiquer, aux journalistes de protéger leurs sources, aux avocats de communiquer avec leurs clients de manière confidentielle ou encore aux lanceurs d'alerte de mettre à disposition du public, tout en se protégeant, des informations dont il devrait prendre connaissance. Toutes ces activités sont indispensables au fonctionnement de nos démocraties et le cryptage fait partie intégrante de ces activités. Dès lors, que certains appellent à supprimer un élément aussi fondamental est pour le moins inquiétant et pourra potentiellement porter atteinte à la formation de l'opinion dans la mesure où les personnes qui auraient des informations à mettre à disposition du public pourraient décider de se censurer car la transmission de ces données en clair pourrait les exposer à des poursuites ou, dans certains pays, à des jugements bien plus expéditifs.

S'il faut cependant reconnaître que le chiffrement peut donner une certaine latitude aux criminels pour fomenter des crimes, il ne faut pas non plus oublier qu'il est possible pour eux de se passer des nouvelles technologies. En effet, rien ne les empêcherait de se rencontrer physiquement ou de se transmettre des messages sur supports physiques, précisément sur le modèle utilisé par les services secrets. Par exemple l'usage d'une *boîte aux lettres morte** permet de laisser un message dans un endroit discret dont seuls les deux correspondants connaissent l'emplacement. L'auteur y dépose le document et le destinataire le reprend quelque temps plus tard. L'avantage de ce système étant de permettre les échanges sans rencontre physique, cloisonnant ainsi le réseau. Le seul moyen d'intercepter la communication est donc de suivre l'auteur – ce qui nécessite de l'identifier au préalable – et de faire une copie du message entre le dépôt et la récupération, pour éviter que les personnes surveillées ne se rendent compte de la surveillance, ou de découvrir par hasard – ou par une fouille méticuleuse – le lieu de dépôt. Il s'agit là de renseignement de terrain et non de surveillance des télécommunications. Il est donc nécessaire pour cela de disposer de moyens humains importants plutôt que de pouvoirs informatiques étendus.

3.3. Jusqu'où les atteintes aux droits fondamentaux sont-elles proportionnées aux impératifs de sécurité ?

Ainsi, les réseaux criminels, et terroristes en particulier, ont la possibilité de ne plus utiliser de moyens de communication pouvant être facilement surveillés. D'une part, par les rencontres physiques, d'autre part par l'usage de technologies cryptées. Dans ce dernier cas seulement, l'utilisation éventuelle de chevaux de Troie pourrait se

---

[36] **HILTPOLD Hugues**, op. cit., n. 16
[37] **Le Hunffington Post**, op. cit., n. 5
[38] **SRC *[En ligne]***, http://www.vbs.admin.ch/content/vbs-internet/fr/ueber-das-vbs/organisation-des-vbs/die-verwaltungseinheiten-des-vbs/-der-nachrichtendienst-des-bundes.download/vbs-internet/fr/documents/servicederenseignement/djihad/Zahlen-Dschihadreisende-August-2016-f.pdf (document consulté le 1er septembre 2016)

justifier, à des conditions strictes vu la grave atteinte à la sphère privée qui en découle. Il ne doit pas être question d'utiliser ce type d'instruments pour des délits mineurs. C'est pourtant ce que craignent les opposants à la loi puisqu'il n'existe pas de liste exhaustive des infractions pouvant donner lieu à de telles mesures. Il s'agit là d'un des points faibles de la loi alors que, dans le cadre d'une procédure judiciaire, une mesure telle qu'une surveillance de la correspondance par poste ne peut être autorisée que pour la poursuite d'infractions clairement nommées.[39]

Cependant, même l'usage de ces logiciels espions ne suffira pas car les terroristes ont toujours une longueur d'avance. A la fois sur le plan technique mais aussi sur le plan décisionnel. En effet, ce sont eux qui choisissent le moment, le lieu et la forme de leur action en frappant par surprise. Elle peut toucher n'importe qui, n'importe quand. C'est d'ailleurs ce qui fait peur avec cette forme de violence puisqu'en termes réels, statistiques de pertes en vie humaines, le terrorisme est une cause négligeable de décès.[40] De cette longueur d'avance découle le fait que le terrorisme ne pourra être éradiqué par des moyens de défense militaire ou par des services de police ce qui amène à analyser le bien-fondé et la proportionnalité de la loi par rapport au but visé et aux conséquences.

Une telle analyse doit se fonder sur des bases claires et choisir les principes avec lesquels cette proportionnalité sera mise en comparaison car cela serait un travail bien trop important que d'analyser la LRens article par article pour y déceler toutes les atteintes potentielles. Le but de l'analyse suivante est donc de fournir un aperçu de cette proportionnalité sur deux éléments centraux, à savoir la protection des données et la présomption d'innocence.

3.3.1. Protection des données : de vraies garanties ?

Un des points fondamentaux de la protection des données est le *droit d'accès* qui consiste à pouvoir demander à toute autorité ainsi qu'à toute personne privée si des données personnelles nous concernant sont traitées. La procédure fait l'objet d'une loi et d'une ordonnance.[41]

Dans la LRens, les dispositions relatives à la protection des données font l'objet d'une section spéciale de la loi. Selon le Conseil fédéral, « [La LRens] renforce au surplus les droits des citoyens vis-à-vis du SRC, en prévoyant notamment un droit d'accès aux données »[42], ce qui sous-entend que cette disposition serait nouvelle. Or il n'en est rien ; un droit d'accès aux données personnelles existe déjà dans la LMSI à l'art. 18. Au contraire, l'art. 63 LRens est plus restrictif en matière de droit d'accès que la règle qu'il envisage de remplacer. Si l'art. 18 al. 2 LMSI prévoit de pouvoir différer la réponse dans certains cas précis, la LRens a remplacé cette liste exhaustive par un simple renvoi à l'art. 6 qui lui-même prévoit bien d'avantage de cas. Le nombre de situations dans lesquelles le SRC pourra différer sa réponse est donc plus important dans la nouvelle loi que dans l'ancienne. De plus, l'art. 6 prévoit l'ensemble des tâches du SRC. Ce n'est que dans les cas qui y sont prévus que le SRC pourra traiter des données personnelles. Il est particulièrement intéressant de noter le cas prévu à l'art. 63 al. 2 let. c « [Le SRC diffère sa réponse s'il] ne traite aucune donnée concernant le

---

[39] Voir *Code de procédure pénale suisse* du 5 octobre 2007 (CPP, RS 312.0) art. 269 al. 2

[40] On pourrait nuancer dans le cas du nombre important de morts dans les attentats du 11 septembre 2001 mais, ramené au nombre d'habitants du pays touché, cela reste faible proportionnellement.

[41] *Loi fédérale sur la protection des données* (LPD, RS 235.1) et *Ordonnance relative à la loi fédérale sur la protection des données* (OLPD, RS 235.11)

[42] **Chancellerie fédérale**, op. cit., n. 22, p. 31

requérant. ». Dès lors, le SRC pourra différer sa réponse dans les cas où il traite des données comme dans les cas où il n'en traite pas (ceci est déjà le cas en vertu de l'art. 18 al. 2 let. c LMSI). Ainsi, lors d'une demande d'accès, soit le SRC peut justifier le report de la réponse parce qu'il traite des données personnelles dans le cadre de ses activités légales, soit il reporte sa réponse parce qu'il ne traite aucune donnée, soit il transmet les données, ce qui signifierait implicitement qu'il ne les traitait pas dans le cadre des activités de l'art. 6 et qu'il les traitait donc de manière illégale.

Le point positif relevé par François Charlet, mais encore une fois non révolutionnaire puisqu'il existait déjà, est de pouvoir demander au Préposé fédéral à la protection des données et à la transparence (préposé) de vérifier si les conditions invoquées par le SRC sont conformes à la réalité et à la loi, puis de pouvoir encore aller devant le TAF en dernier recours.[43]

Concernant la transmission des données personnelles, le SRC pourra transmettre ces dernières à des autorités étrangères même si l'Etat destinataire n'assure pas un niveau de protection des données adéquat, à condition que la Suisse entretienne avec cette nation des relations diplomatiques et qu'une des conditions visées à l'art. 61 al. 2 se trouve remplie. La let. d de cet alinéa est particulièrement intéressante puisqu'elle permet de transmettre les données si la personne « a donné au préalable son consentement à la communication ou les circonstances permettent de présumer de manière certaine ce consentement ». De plus, il convient de rappeler l'art. 70 LRens qui précise que le Conseil fédéral possède la compétence de signer des traités internationaux sur la collaboration du SRC ce qui pourra l'amener à transmettre plus de données à l'étranger.

L'art. 5 al. 5 interdit au SRC de traiter des données relatives à l'exercice des droits politiques, de la liberté d'opinion, d'association ou de réunion *en Suisse*. Cependant, l'al. 6 prévoit des exceptions dans le cas où une personne ou une organisation utiliserait ces droits dans des buts terroristes, d'espionnage ou d'extrémisme violent. De nouveau, la loi prévoit ici une disposition et immédiatement un certain nombre d'exceptions. De plus on constate que ces règles ne s'appliquent qu'à la Suisse ce qui signifie qu'à l'étranger il n'y aurait pas besoin de rentrer dans le cas d'une des exceptions de l'al. 6 pour pouvoir surveiller ces activités. On peut alors se demander ce qui se passerait, par exemple, dans le cas d'une association ayant des activités internationales. Les membres suisses de cette organisation qui se déplaceraient à l'étranger pour des réunions pourraient-ils être surveillés ? Et quid des droits politiques des Suisses de l'étranger qui participent pourtant aux votations et ont donc des activités politiques en lien avec notre pays ? La LRens devrait non seulement protéger les activités politiques de toute personne en Suisse mais également celles des citoyennes et citoyens suisses où qu'ils se trouvent dans le monde.

3.3.2. Soupçon généralisé : une menace pour la présomption d'innocence ?

Contrairement aux autorités de poursuite pénale, le SRC agit de manière préventive. Il a besoin pour cela de moyens modernes. Cependant, il n'est pas autorisé à intervenir lui-même, ce qui est une bonne chose pour éviter des interventions illégales. Il doit donc passer par des autorités telles que la police. Par exemple, pour interroger une personne, il doit la faire appréhender par un corps de police cantonal (LRens art. 24).

Ceci implique aussi que le SRC, une fois les informations probantes récoltées, doit les transmettre sans délai aux autorités pénales, ce qui nécessite une forte collaboration

---

[43] **CHARLET François**, op. cit., n. 17

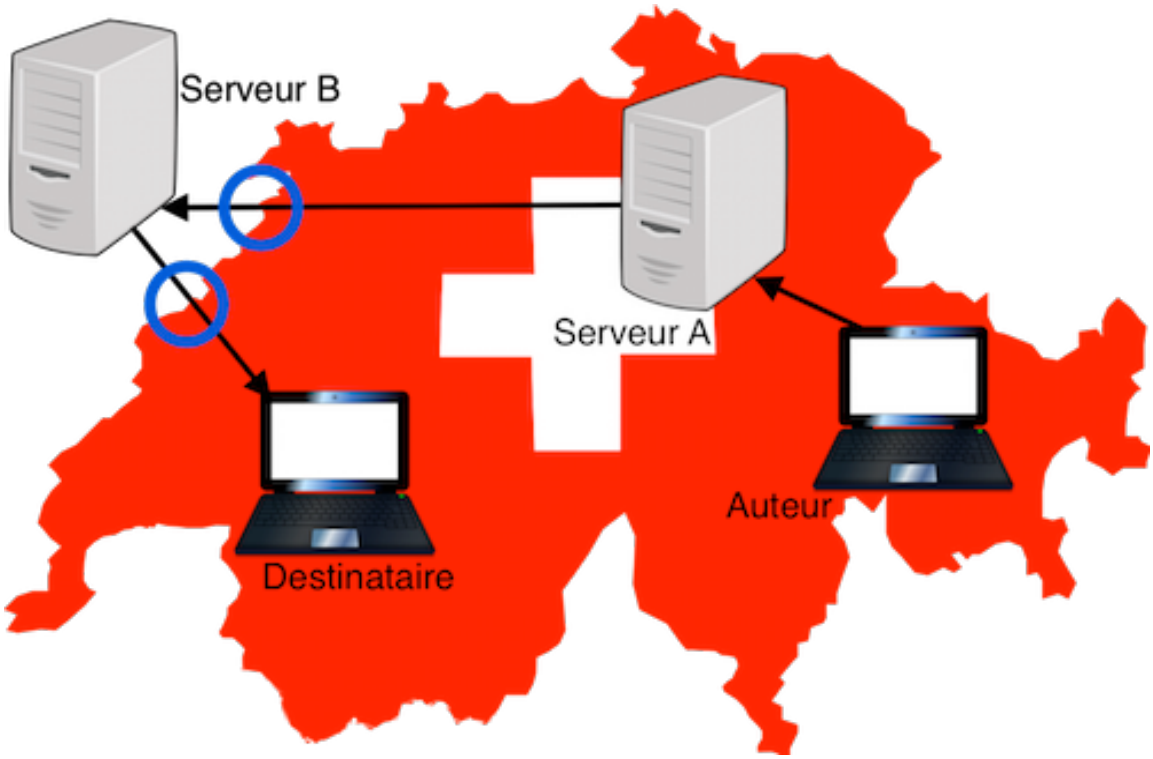
entre les différents services. Selon Lisa Mazzone, il existerait ici un risque que le SRC garde les enquêtes trop longtemps ce qui aurait pour conséquence que les autorités ayant qualité pour intervenir pourraient ne plus en avoir le temps, les empêchant de prévenir à temps les actes des personnes surveillées.[44]

Certaines dispositions de la loi, comme l'exploration du réseau câblé, remettent également en question la présomption d'innocence. L'exploration du réseau câblé consiste à intercepter l'ensemble des communications contenant certains mots-clés. Seules les communications internationales seraient concernées, cela signifie que celles dont l'auteur comme le destinataire se trouvent en Suisse ne pourraient pas être utilisées ; cela n'empêche pas qu'elles soient tout de même interceptées mais elles devraient ensuite être détruites et ne pourraient pas être transmises au SRC, Cependant, des données relatives à des personnes se trouvant en Suisse pourront être transmises de manière anonymisée si elles sont nécessaires à apprécier la situation à l'étranger (LRens art. 42 al. 2). En revanche, si les données concernent une menace concrète, elles seront transmises telles quelles, même si elles concernent des événements ayant lieu en Suisse. Au-delà de ces subtilités juridiques, la principale difficulté à saisir ici est que le mail en tant que message (exemple pris le plus souvent) ne constitue pas lui-même la communication. En réalité, l'envoi d'un mail en requière au minimum trois:

1. De l'ordinateur de l'auteur à son serveur de messagerie
2. Du serveur de l'auteur à celui du destinataire
3. Du serveur du destinataire à l'ordinateur du destinataire

Cela constitue donc plusieurs communications et, en supposant que l'un des serveurs se trouve à l'étranger, cela permet d'intercepter à deux moments le message comme le montre le schéma ci-après. Même en sachant que le message ne pourrait pas être utilisé, il pourrait tout de même être intercepté, ce qui en soi pose déjà problème puisqu'on se retrouve ici *de facto* dans le cas d'une surveillance à grande échelle.

[44] **MAZZONE Lisa**, op. cit., n. 20



Même si l'auteur et le destinataire du message se trouvent en Suisse, il se peut que la communication transite par l'étranger et soit interceptée.[45]

De nos jours, personne ne peut se vanter de ne communiquer numériquement qu'avec la Suisse. Le simple fait d'effectuer une recherche sur Google nous met en communication avec des serveurs situés aux Etats-Unis. De même, nombre de sites suisses utilisent des outils comme *Google analytics*, fourni par Google, et transmettent par conséquent des informations également aux Etats-Unis. D'autres services très populaires tels que Whatsapp ou Facebook passent tous par des communications transfrontières de données. Il faut retenir qu'en termes d'interception ce ne sont pas uniquement la position de l'auteur et celle du destinataire du message qui sont déterminantes mais également celle de *tous* les intermédiaires, qui peuvent être parfois très nombreux.

Le fait que le SRC puisse agir de manière préventive avec de telles mesures met en danger la présomption d'innocence. En effet, au lieu de rechercher des preuves contre l'auteur d'une infraction pour le punir, le SRC pourra chercher si des personnes représentent une menace. Cela renverse totalement le principe d'intervention judiciaire en permettant de chercher des preuves d'une infraction qui n'existe pas encore. Alors que, lors d'une procédure judiciaire, le prévenu peut se faire entendre et donner sa version des faits, le droit à se défendre, dans le cadre d'une investigation secrète, cela n'est pas possible puisque la mesure est effectuée à l'insu de la personne concernée. Dans le cas où aucun élément probant n'est trouvé, la personne aura vu sa vie fouillée et analysée sans aucun résultat. En admettant que les recherches effectuées par le SRC se basent sur des indices sérieux, ce qui n'empêche pas qu'ils puissent se révéler inexacts, elles équivaudraient à mettre en cause et donc à accuser une personne qui n'aurait potentiellement rien à se reprocher. Dans le cadre des mesures de recherche soumises à autorisation, les personnes concernées *devraient* être informées qu'elles ont fait l'objet d'une surveillance et elles auront donc la possibilité

[45] Montage réalisé à partir d'images internet

d'intenter une action judiciaire pour faire reconnaître le caractère éventuellement abusif de la mesure. En revanche, dans le cas d'un renseignement obtenu sans passer par une mesure soumise à autorisation, la personne ne sera pas informée, à moins d'avoir au préalable effectué une demande d'accès selon l'art. 63. Et encore, elle ne le serait potentiellement que de nombreuses années plus tard. Cependant, le simple fait de se renseigner sur une personne indique déjà une suspicion et devrait donc appeler automatiquement un droit à se défendre, ceci dans tous les cas de figure. De plus, le fait pour le SRC de devoir informer dans tous les cas les personnes concernées et donc d'être en mesure de justifier l'ensemble de ses activités le forcerait à se concentrer sur ses tâches les plus pertinentes.

3.3.3. Manque de précisions et abus potentiels

Le curseur entre sécurité et liberté doit être placé de manière équilibrée et, dans le cas de la LRens, c'est surtout le SRC qui décidera de ce qu'il considère comme un équilibre adéquat. En effet, il n'est pas prévu qu'une entité doive autoriser les surveillances et autres activités du SRC particulièrement par rapport à la protection des données. Le TAF ne le fera que vis-à-vis de la loi sans prendre en compte spécialement cet aspect particulier. La Digitale Gesellschaft pointe d'ailleurs dans la procédure de consultation le fait qu'« il manque ici la garantie d'une représentation efficace des intérêts à la protection de la sphère privée. »[46] Dans ce domaine, seuls des contrôles *a posteriori* seront effectués. Il existe donc un risque de déséquilibre et de partialité dans l'appréciation de la pertinence des données saisies.

Dans le contexte d'un service au fonctionnement secret, la prévention des abus passe, outre des mesures de surveillance opérées par d'autres organes indépendants, par une réglementation précise dont l'interprétation univoque limite autant que possible les écarts par rapport à la volonté du législateur. La LRens ne répond pas à ce critère. Elle est en effet truffée de formulations vagues et souffre d'un manque récurrent de définitions. L'interprétation de ce que signifie les mots « informations pertinentes » ou « menace imminente » relèvera en grande partie du bon vouloir du SRC, éventuellement dans une certaine mesure de la jurisprudence, si ses décisions venaient à être parfois invalidées par une instance judiciaire délibérant de manière publique.

[46] **SRC**, op. cit., n. 19, p. 37

4. Votation populaire : pourquoi un tel résultat ?

Le 25 septembre 2016, le peuple suisse s'est prononcé sur la LRens suite à un référendum. De ce vote est sorti un résultat net : 65,5% d'opinions favorables contre 34,5, avec une participation de 41,8%.[47] Ce résultat est supérieur de plus de 10 points au dernier sondage de l'institut gfs.bern[48] qui prédisait, le 14 septembre, 53% en faveur de la loi, 35% contre et 12% d'indécis.

L'argument le plus porteur de la campagne en faveur de la loi a évidemment été l'inquiétude suscitée par les actes commis en Europe dans les semaines ayant précédé la votation, laquelle a abouti à une victoire de la peur et des déclarations alarmistes des partisans du *sécuritarisme* et les amalgames, tels l'affirmation du Conseiller fédéral Guy Parmelin, qui a estimé que « refuser la nouvelle loi, [c'était] se rendre complice d'un futur attentat. »[49] Les partisans de la loi ont amené le débat sur un registre émotionnel et ont simplement agité en réponse aux craintes légitimes d'un Etat fouineur des mesures de surveillance renforcées.

Il ne faut pas oublier les multiples dérapages dont ont été victimes – ou même se sont rendus coupables – les services de sécurité suisses. L'affaire des fiches dans les années 1989-1990, la collaboration d'un agent du SRC dans l'affaire Giroud, le vol de données par un informaticien du service. A chaque fois, les politiques ont su brandir que les conclusions de ces affaires avaient été tirées et des mesures prises. Jusqu'à quand encore pourront-ils servir cette réponse toute faite ?

La LRens, comme l'a relevé Lisa Mazzone, « est une loi efficace pour une votation »[50] dans le sens où elle répond de manière quasi immédiate à un sentiment, un réflexe primaire de survie : la peur. En revanche, expliquer les raisons pour lesquelles ce qui est présenté comme efficace doit être refusé constitue un travail fastidieux. Il est clair que la LRens ne règlera pas le problème de fond, à savoir l'engagement de certaines personnes dans les groupes terroristes. Les causes de ce phénomène sont bien plus profondément ancrées et la surveillance n'aura pas d'incidence sur elles. Seules des réformes sociales adéquates permettant de donner un espoir et un avenir aux personnes tentées par ces formes de violence auront une chance d'endiguer ce qui est aujourd'hui devenu un phénomène de société.

---

[47] **Chancellerie fédérale** ***[En ligne]*** https://www.admin.ch/ch/f/pore/va/20160925/det607.html (site consulté le 06 octobre 2016)

[48] **LONGCHAMP Claude** [et al.], *Rapport succinct sur la seconde vague d'enquête «SRG Trend» relative à la votation du 25 septembre 2016*, Berne, gfs.bern, 14 septembre 2016

[49] **Le Courrier** ***[En ligne]*** http://www.lecourrier.ch/142715/les_gros_moyens_contre_le_terrorisme (site consulté le 06.10.2016). La citation initiale est « On n'a pas le droit en ne faisant rien de se rendre indirectement complice d'un attentat, au nom de la préservation absolue de la sphère privée, à laquelle je suis pourtant attaché. » (**Le Matin Dimanche** ***[En ligne]*****,** http://www.lematindimanche.ch/read/ch.lematindimanche.ipad.LMD20160828/acteurs/Ne-rien-faire-c-est-indirectement--se-rendre-complice-d-un-attentat-690381068 (site consulté le 24 octobre 2016)) mais elle a été reprise plusieurs fois, avec une formulation modifiée, dans de nombreux médias. (Voir annexe II)

[50] **MAZZONE Lisa**, op. cit., n. 20

Conclusion

La nouvelle Loi fédérale sur le renseignement porte donc atteinte de manière non négligeable aux droits fondamentaux garantis par la Constitution fédérale et en particulier au respect de la sphère privée (art. 13 Cst.), à la présomption d'innocence (art. 32 al. 1 Cst.), à la liberté d'expression (art. 16 al. 2 Cst.), à la liberté de réunion et d'association (art. 22 et 23 Cst.) ainsi qu'à l'indépendance et à l'impartialité des tribunaux (art. 29 al. 1 et 30 al. 1 Cst.).

Le respect de la sphère privée est mis à mal par les méthodes agressives de renseignement qui pourront être utilisées. La pose de micros ou de caméras dans un lieu privé, l'introduction de chevaux de Troie dans un ordinateur ne vont pas sans poser de questions. S'il est possible d'admettre la surveillance de personnes suspectées en échange de *réelles* garanties en matière de respect du droit, la surveillance indirecte des membres de la famille ou simplement des autres personnes qui se trouveraient dans le lieu est déjà beaucoup plus discutable. Comment surveiller uniquement le suspect en garantissant les droits des tiers ? Voilà une question en suspens.

La présomption d'innocence est automatiquement attaquée lorsque sont mises en place des mesures préventives. La décision de surveillance ne peut alors se baser que sur des soupçons ou la délation. Si, dans le cadre d'une procédure judiciaire, un accusé peut se défendre et donner sa version des faits, lors d'interventions préventives, il est nécessaire de mettre en place un contrôle strict permettant la mise en balance de manière équitable des différents intérêts en présence.

Sur ce point, la participation du Tribunal administratif fédéral est présentée comme un moyen de contrôle efficace. Cette affirmation se base sur le fait que les tribunaux sont indépendants. Cependant, les actions de renseignement sont dirigées en grande partie – notamment concernant les recherches à l'étranger, même si dans ces cas aucun contrôle judiciaire n'aura lieu – par des besoins politiques qu'un tribunal n'est pas à même de contester sur le fond. Le risque existe donc de voir le pouvoir judiciaire n'avoir plus qu'un rôle de garant des actions de l'exécutif. De plus, la présence de la même entité dans les procédures d'autorisation et de recours amène collusion voire conflit d'intérêt et nuit donc à l'impartialité des tribunaux.

Les libertés de réunion et d'association sont également directement menacées par la possibilité d'interdire certaines organisations. Si cela peut se comprendre au vu des impératifs de sécurité et de l'activité attestée de certains groupes, la plus grande retenue devra rester de mise dans ce domaine.

La population prend de manière croissante conscience de la surveillance exercée sur elle, autant par les acteurs gouvernementaux que par les sociétés privées. La restriction de la liberté ne passe pas uniquement par une punition en cas d'acte illégal. Déterminer, sur la base des mails d'une personne, les produits qu'elle serait susceptible de rechercher et les lui faire acheter à un certain vendeur en lui affichant les publicités de ce fournisseur uniquement constitue également une forme de restriction de nos libertés : celles de choisir ce que nous faisons, de choisir avec qui. De même, la menace de surveillance par les autorités amène les gens à une certaine autocensure et donc à restreindre eux-mêmes leur propre liberté.

Nous devons agir autant contre le terrorisme que contre la surveillance car renoncer à nos libertés aujourd'hui c'est renoncer au droit de mener notre vie comme nous l'entendons dans un environnement propice mais c'est aussi, en choisissant le repli, renoncer à notre devoir de combattre celles et ceux qui nous veulent du mal ; c'est

s’incliner face à la peur et préférer abandonner ce qui nous différencie plutôt que de clamer haut et fort notre volonté de résistance.

Un travail intéressant sera à mener dans les prochaines années pour contrôler la façon dont seront appliquées les dispositions votées par le peuple. Ce travail sera l’œuvre des autorités de surveillance mises en place mais également celui des médias et des citoyennes et citoyens. L’opinion publique a tendance à se désintéresser et à oublier rapidement. Il est nécessaire que certaines personnes motivées maintiennent la pression sur les services de sécurité et les politiques et soient prêtes à intervenir en cas de dérives. Rien ne peut remplacer un contrôle citoyen et public sur des questions aussi sensibles.

Même si la loi a été acceptée par le peuple, il ne faut pas perdre de vue que le Parlement conserve le pouvoir – et même le devoir – de la modifier s’il apparaissait des problèmes dans sa mise en œuvre. Il reviendra au peuple d’amener ses représentants à respecter leurs promesses de retenue dans l’application de leur pouvoir et de réclamer les contrôles et le peu de transparence qui lui ont été promis.

Bilan personnel

Ce travail a permis d'analyser une loi particulièrement complexe et qui aura un impact sur notre quotidien. D'un côté, cet impact pourrait être bénéfique : une protection efficace contre les attentats, de l'autre, il pourrait être négatif : une surveillance de masse de la population. Les conséquences dépendront en grande partie de la mise en œuvre future de la Loi sur le renseignement et des priorités des personnes qui dirigeront les activités du Service de renseignement de la Confédération.

Malheureusement, il semblerait qu'une partie des gens tolèrent la surveillance en tenant un discours du type « je n'ai rien à cacher » ou « de toute façon, nous sommes déjà surveillés ». Expliquer les méfaits du renseignement constitue donc une difficulté majeure. S'agissant d'un sujet complexe où se mêlent libertés, relations internationales, sécurité et bien d'autres domaines, apprécier les besoins et les conséquences relève d'un travail d'équilibriste requérant une compréhension et des compétences multiples. Il est dès lors d'autant plus important que les personnes convaincues de l'inviolabilité des droits fondamentaux continuent à veiller.

Un travail de maturité tel que celui-ci ne peut évidemment pas aborder l'ensemble des points litigieux ou proposer une analyse exhaustive d'une loi aussi complexe. Il n'a par exemple pas été possible, pour des questions de temps, de réaliser une analyse sémantique d'un article ce qui aurait cependant constitué un exemple parlant des problèmes de définitions dans la LRens. Il propose en revanche un condensé de réflexions critiques sur les plans juridiques et politiques, qui sont, dans le cas du renseignement, intimement liés.

Bien d'autres points pourraient faire l'objet d'une critique ou du moins être mis en perspective. Un travail de ce type ouvre des portes et des pistes de réflexion plus avancées qu'il serait intéressant d'explorer de manière systématique et en profondeur. Il vise à expliquer de manière relativement concise les points négatifs de la loi, ses défenseurs ayant déjà donné les arguments positifs en sa faveur.

Comprendre et analyser les subtilités juridiques d'une telle loi et rédiger un dossier comme celui-ci nécessite beaucoup de recherches et de confrontations de points de vue ainsi que de modifications et relectures suivant l'évolution du contexte afin de rester au plus près des développements de l'actualité. Je tiens donc ici à remercier les personnes qui ont soutenu cette démarche, et particulièrement :

- Delphine Schaller pour m'avoir suivi dans la rédaction de ce travail
- François Charlet pour avoir répondu à mes questions sur la LRens d'un point de vue juridique
- Lisa Mazzone et Hugues Hiltpold pour m'avoir présenté leur position respective sur la loi

Lexique

Alliance contre l'Etat fouineur : Alliance formée de plusieurs organisations ayant lancé le référendum contre la LRens

Boîte aux lettres morte : Lieu convenu d'avance où peuvent être déposés des messages ou des documents afin d'échanger des informations sans rencontre entre l'expéditeur et le destinataire

Délégation du Conseil fédéral pour la sécurité : Commission du Conseil fédéral formée des chef-fe-s du DDPS, du DFAE et du DFJP, spécialisée dans les questions de sécurité

Force brute : Par « force brute » on entend une tentative d'accès à une information (découverte de mot de passe, décryptage, etc) par l'essai systématique de toutes les combinaisons possibles. Dans le cas d'un mot de passe, le test de toutes les suites de caractères possibles

GCHQ : *Government Communications Headquarters*, service de renseignement britannique spécialisé dans le renseignement électronique

GSSA : *Groupe pour une Suisse sans Armée*, membre de l'*Alliance contre l'Etat fouineur*

LFRC : *Loi fédérale sur le renseignement civil*, du 3 octobre 2008, entrée en vigueur le 1er janvier 2010

LMSI : *Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure*, du 21 mars 1997, entrée en vigueur le 1er juillet 1998

LRens : *Loi fédérale sur le renseignement*, votée le 25 septembre 2015 au Parlement et acceptée par référendum le 25 septembre 2016
Lors de citations de dispositions de la loi, la version utilisée est, sauf indication contraire, celle adoptée au vote final par le Parlement et publiée dans la Feuille fédérale sous la référence FF 2015 6597.

LSCPT : *Loi fédérale sur la surveillance de la correspondance par poste et télécommunications*, révisée par le Parlement en 2016 et contre laquelle un référendum (n'ayant pas abouti) a été lancé

NSA: *National Security Agency*, agence de renseignement des Etats-Unis

Service SCPT : *Service de surveillance de la correspondance par poste et télécommunications*, chargé d'effectuer les mesures de surveillance ordonnées dans le cadre d'enquêtes judiciaires

SRC : *Service de renseignement de la Confédération* dont l'activité sera encadrée par la *LRens*

TAF : *Tribunal administratif fédéral* qui devra autoriser les mesures de recherche soumises à autorisation prévues dans la *LRens*

USA Patriot Act : *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, loi américaine offrant aux services de sécurité des Etats-Unis plus de pouvoirs en matière de surveillance.

Bibliographie

Internet

DDPS ***[En ligne]****,*
http://www.vbs.admin.ch/internet/vbs/fr/home/themen/ndb/uebersicht.html
(consulté le 07 février 2016)

DDPS ***[En ligne]****,*
http://www.vbs.admin.ch/internet/vbs/fr/home/themen/ndb/faq.html#parsys_48129
(consulté le 07 février 2016)

Chancellerie fédérale ***[Communiqué de presse en ligne]****,*
https://www.news.admin.ch/message/index.html?lang=fr&msg-id=60550
(diffusé et consulté le 04 février 2016)

Chancellerie fédérale ***[En ligne]***
https://www.admin.ch/ch/f/pore/va/20160925/det607.html
(consulté le 06 octobre 2016)

Groupe Altice Média, **L'express** ***[En ligne],*** http://lexpansion.lexpress.fr/high-tech/operation-tempora-comment-les-britanniques-depassent-les-americains-pour-espionner-internet_1434134.html (site consulté le 11 septembre 2016)

Le Courrier ***[En ligne]***
http://www.lecourrier.ch/142715/les_gros_moyens_contre_le_terrorisme
(consulté le 06 octobre 2016)

Le Huffington Post SAS, **Le Huffington Post** ***[En ligne]***,
http://www.huffingtonpost.fr/2015/12/08/jihadistes-syrie-combattants-etrangers-nombre-origine-etat-islamique-daech_n_8747236.html
(consulté le 1er septembre 2016)

Services du Parlement, **Le Parlement suisse** ***[En ligne]*****,**
https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20140022
(consulté le 10 septembre 2016)

Pixabay ***[En ligne]*** https://pixabay.com/p-157424/?no_redirect
(consulté le 10 septembre 2016)

Pixabay ***[En ligne]*** https://pixabay.com/p-567943/?no_redirect
(consulté le 10 septembre 2016)

Proton Technologies AG, **Protonmail** ***[En ligne]***, https://protonmail.com/fr/
(consulté le 1er septembre 2016)

Radio Télévision Suisse, **RTS** ***[En ligne]***, http://www.rts.ch/info/monde/7279618-la-turquie-se-met-la-russie-a-dos-apres-avoir-abattu-un-de-ses-avions.html
(consulté le 11 septembre 2016)

SRC ***[En ligne]***, http://www.vbs.admin.ch/content/vbs-internet/fr/ueber-das-vbs/organisation-des-vbs/die-verwaltungseinheiten-des-vbs/-der-nachrichtendienst-des-bundes.download/vbs-internet/fr/documents/servicederenseignement/djihad/Zahlen-Dschihadreisende-August-2016-f.pdf (document consulté le 1er septembre 2016)

Service SCPT ***[En ligne]***, https://www.li.admin.ch/fr/documentation/faq
(consulté le 07 septembre 2016)

Wikimedia ***[En ligne]***
https://upload.wikimedia.org/wikipedia/commons/thumb/6/6f/CARTE_DRAPEAU_SUISSE.svg/1280px-CARTE_DRAPEAU_SUISSE.svg.png (consulté le 10 septembre 2016)

Publications officielles

Chancellerie fédérale, *Votation populaire du 25 septembre 2016 Explications du Conseil fédéral*, 2016

Chancellerie fédérale, *Référendum contre la loi fédérale du 25 septembre 2015 sur le renseignement (LRens) Aboutissement* (FF 2016 700), 02 février 2016

Conseil fédéral, *Message concernant la loi sur le renseignement* (FF 2014 2029), 19 février 2014

SRC, *Loi sur le renseignement (LRens) Rapport sur les résultats de la procédure de consultation*, septembre 2013

Lois

Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI, RS 120)

Loi fédérale sur le renseignement civil (LFRC, RS 121)

Loi fédérale sur le renseignement (LRens, non encore inscrite au Recueil systématique)

Loi sur le renseignement (LRens) projet du 08.03.2016

Loi fédérale interdisant les groupes « Al-Qaïda » et « Etat islamique » et les organisations apparentées (RS 122, votée le 12 décembre 2014, en vigueur du 1er janvier 2015 au 31 décembre 2018)

Débats et conférences

BADINTER Robert [conférence] « le terrorisme et la loi », 11 novembre 2015 dans le cadre de la 48e session des Rencontres Internationales de Genève (enregistrement vidéo de la conférence *[En ligne] : https://mediaserver.unige.ch/fichiers/view/91605*)

Interviews

HILTPOLD Hugues, conseiller national, interview le 03 août 2016

CHARLET François, juriste spécialisé en droit des technologies, interview le 18 août 2016

MAZZONE Lisa, conseillère nationale, interview le 1er septembre 2016

Publications statistiques

LONGCHAMP Claude [et al.], *Rapport succinct sur la seconde vague d'enquête «SRG Trend» relative à la votation du 25 septembre 2016*, Berne, gfs.bern, 14 septembre 2016

Articles de presse

AUBERT Laurent, « L'« Etat fouineur » fait-il plus peur que les attentats ? », *in* Tribune de Genève, 25 novembre 2015, p. 3

MISSON Joëlle, « La Suisse dans le viseur des terroristes », *in GHI*, 21-22 janvier 2015, p. 3

Annexes

Annexe I: Articles de loi

Article 18 alinéas 1 et 2 LMSI

Art. 18[59] Droit d'accès

[1] Le droit d'accès est régi par les art. 8 et 9 de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[60], sous réserve des al. 2 à 8.

[2] Lorsqu'une personne demande si le SRC traite des données la concernant dans le système d'information prévu à l'art. 15 al. 3, le SRC diffère sa réponse dans les cas suivants:

a. les données traitées la concernant sont liées à des intérêts prépondérants, dûment motivés et consignés, qui exigent le maintien du secret:
   1. lorsque l'exigent la détection précoce et la lutte contre les dangers liés aux activités suivantes:
      a. le terrorisme,
      b. le service de renseignements prohibé,
      c. l'extrémisme violent,
      d. les actes préparatoires relatifs au commerce illicite d'armes et de substances radioactives,
      e. le transfert illégal de technologie;
   2. lorsqu'il s'agit d'une poursuite pénale ou d'une autre procédure d'instruction;

b. les intérêts prépondérants d'un tiers l'exigent;

c. aucune donnée la concernant n'est traitée.

Article 63 alinéas 1 et 2 LRens

Art. 63 Droit d'accès

[1] Le droit d'accès aux données saisies dans les systèmes d'information PES et Quattro P, dans le portail ROSO, et dans les systèmes d'information distincts visés aux art. 36, al. 5, et 58 et aux données administratives enregistrées dans le système GEVER SRC est régi par la LPD[21].

[2] Lorsqu'une personne demande si le SRC traite des données la concernant dans les systèmes IASA SRC, IASA-EXTR SRC, INDEX SRC ou SICO, dans le système de stockage des données résiduelles ou dans le système GEVER SRC, le SRC diffère sa réponse:

a. si et pour autant que les données traitées au sujet de cette personne sont liées à des intérêts prépondérants, dûment motivés par le SRC, qui exigent le maintien du secret pour une des raisons suivantes:
   1. l'accomplissement des tâches visées à l'art. 6 l'exige,
   2. une poursuite pénale ou une autre procédure d'instruction l'exige;

b. si et pour autant que les intérêts prépondérants d'un tiers exigent le maintien du secret;

c. si le SRC ne traite aucune donnée concernant le requérant.

Annexe II: **Revue de presse**

Citation de Guy Parmelin (évolution dans divers médias de façon chronologique)

Version publiée dans *Le Matin Dimanche* le 28 août 2016

> Avec la future loi, nous pourrons comparer la Suisse avec la Belgique ou certains pays nordiques. Tous les spécialistes du renseignement qui ont participé à son élaboration sont d'accord pour dire que c'est un minimum, mais que cela va grandement améliorer la situation. On n'a pas le droit en ne faisant rien de se rendre indirectement complice d'un attentat, au nom de la préservation absolue de la sphère privée, à laquelle je suis pourtant attaché.

Extrait d'une interview accordée par Guy Parmelin au journal Le Matin Dimanche *et publié le 28 aout 2016*

Le Matin Dimanche *[En ligne]*, http://www.lematindimanche.ch/read/ch.lematindimanche.ipad.LMD20160828/acteurs/Ne-rien-faire-c-est-indirectement--se-rendre-complice-d-un-attentat-690381068 (consulté le 24 octobre 2016)

Version disponible sur le site internet de la RTS

> **"On ne peut rien exclure", a averti le ministre de la Défense Guy Parmelin dans Le Matin dimanche et le Blick au sujet de la menace terroriste en Suisse. Il assure "continuer à mener des évaluations".**
>
> "Avant même les attentats de cet été, les analyses parlaient déjà de menace élevée", remarque l'élu UDC. Il reconnaît que "la situation est plus mouvante, non seulement en Suisse, mais dans le monde entier".
>
> Guy Parmelin note que la Suisse ne combat pas les groupes djihadistes, mais qu'elle abrite des missions diplomatiques de pays engagés dans la coalition internationale qui lutte contre l'EI et Al-Qaïda.
>
> **"Indirectement complices"**
>
> "Il est de notre devoir de veiller à la sécurité de ces représentations, mais aussi à celle de nos concitoyens qui se retrouveraient par hasard au mauvais endroit au mauvais moment", explique-t-il, faisant référence à des Suisses tués à Louxor en 1997 et à Ouagadougou au début de l'année.
>
> Guy Parmelin a aussi défendu le renforcement de la loi sur le renseignement, en votation le 25 septembre. "On n'a pas le droit en ne faisant rien de se rendre indirectement complice d'un attentat, au nom de la préservation absolue de la sphère privée", a-t-il souligné.

Article publié par la RTS le 28 août 2016 et faisant référence à l'interview précédente

RTS *[En ligne]*, http://www.rts.ch/info/suisse/7972353-la-menace-d-attentat-a-augmente-en-suisse-estime-guy-parmelin.html (consulté le 23 octobre 2016)

Version publiée dans *24 heures* le 12 septembre 2016

Vous avez dit que refuser la nouvelle loi, c'est se rendre complice d'un futur attentat. Les mots ont-ils dépassé votre pensée?
Non. Prenons un exemple. On nous signale un terroriste dans une gare de Suisse. C'est dans un espace public, nous pouvons le surveiller. L'homme regagne sa chambre hôtel. Impossible pour l'Etat de continuer sa surveillance. Admettons maintenant que cette personne commette ensuite un attentat avec de nombreuses victimes. Avec la nouvelle loi, on aurait pu tout mettre en œuvre pour tenter d'empêcher cela.

Vous présentez des opposants politiques comme des complices indirects de terroristes, l'attaque est un peu forte...
Non, il faut regarder la réalité en face. Et ce seront peut-être les mêmes personnes qui diront après l'attentat: "Mais qu'a fait la police?" Eh bien les pouvoirs publics n'auront pas pu agir faute d'informations. C'est dans ce sens là que je maintiens qu'il s'agit d'une complicité indirecte.

Extrait d'une interview de Guy Parmelin à 24 heures *dans laquelle le journaliste fait allusion aux propos tenus dans l'interview du 28 août 2016*

24 heures *[En ligne]*, http://www.24heures.ch/suisse/parmelin-persiste-complices-terroristes/story/18068908 (consulté le 24 septembre 2016)

Version publiée dans la *Tribune de Genève* le 12 septembre 2016

données qui le concernent seront anonymisées avant d'être transmises au SRC. Le SRC aura 22 postes supplémentaires avec la nouvelle loi. Mais ces effectifs peuvent encore augmenter si la situation sécuritaire devait s'aggraver.

Vous avez dit que refuser la nouvelle loi, c'est se rendre complice d'un futur attentat. Les mots ont-ils dépassé votre pensée?
Non. Prenons un exemple. On nous signale un terroriste dans une gare de Suisse. C'est dans un espace public, nous pouvons le surveiller. L'homme regagne sa chambre hôtel. Impossible pour l'Etat de continuer sa surveillance. Admettons maintenant que cette personne commette ensuite un attentat avec de nombreuses victimes. Avec la nouvelle loi, on aurait pu tout mettre en œuvre pour tenter d'empêcher cela.

Vous présentez des opposants politiques comme des complices indirects de terroristes. Vous y allez un peu fort...
Non, il faut regarder la réalité en face. Et ce seront peut-être les mêmes personnes qui diront après l'attentat: «Mais qu'a fait la police?» Eh bien, les pouvoirs publics n'auront pas pu agir, faute d'informations. C'est dans ce sens-là que je maintiens qu'il s'agit d'une complicité indirecte.

Extrait d'une interview de Guy Parmelin à la Tribune de Genève *dans laquelle le journaliste fait allusion aux propos tenus dans l'interview du 28 septembre 2016*

GROSJEAN Arthur, « Guy Parmelin : « En cas de dérapage, les autorités agiront très vite » », *in Tribune de Genève*, 12 septembre 2016, p. 4

Version de l'interview du 12 septembre 2016 disponible sur le site internet du DDPS

Vous avez dit que refuser la nouvelle loi, c'est se rendre complice d'un futur attentat. Les mots ont-ils dépassé votre pensée?

Non. Prenons un exemple. On nous signale un terroriste dans une gare de Suisse. C'est dans un espace public, nous pouvons le surveiller. L'homme regagne sa chambre hôtel. Impossible pour l'Etat de continuer sa surveillance. Admettons maintenant que cette personne commette ensuite un attentat avec de nombreuses victimes. Avec la nouvelle loi, on aurait pu tout mettre en oeuvre pour tenter d'empêcher cela.

Vous présentez des opposants politiques comme des complices indirects de terroristes. Vous y allez un peu fort...

Non, il faut regarder la réalité en face. Et ce seront peut-être les mêmes personnes qui diront après l'attentat: «Mais qu'a fait la police?» Eh bien, les pouvoirs publics n'auront pas pu agir, faute d'informations. C'est dans ce sens-là que je maintiens qu'il s'agit d'une complicité indirecte.

Extrait de l'interview réalisée par 24 heures*, version publiée sur le site internet du DDPS*

DDPS ***[En ligne]*****,** http://www.vbs.admin.ch/fr/themes/recherche-renseignements/loi-renseignement.detail.news.html/interviews/2016/160912f.html
(consulté le 23 octobre 2016)

Version publiée dans *Le Courrier* le 26 septembre 2016

La conseillère nationale Lisa Mazzone (verts, GE) se disait satisfaite, dimanche, d'avoir au moins pu mener «un débat important pour les droits fondamentaux malgré des discussions basées sur la peur». Elle reproche également certains dérapages survenus durant la campagne. En ligne de mire, l'affirmation de Guy Parmelin selon laquelle «refuser la nouvelle loi» équivalait à «se rendre complice d'un futur attentat». «On nous a accusés de crime, c'est grave.»

Extrait d'un article publié par Le Courrier *le 26 septembre 2016 dans lequel Lisa Mazzone fait référence aux propos tenus par Guy Parmelin dans l'interview du 28 septembre 2016*

Le Courrier ***[En ligne]***
http://www.lecourrier.ch/142715/les_gros_moyens_contre_le_terrorisme
(consulté le 06 octobre 2016)

Annexe III: Questions des interviews

1. Qu'est-ce que la nouvelle loi change par rapport à la situation précédente ?
2. N'est-ce pas une simple légitimation de pratiques déjà existantes ?
3. Offre-t-elle vraiment plus de pouvoirs au SRC ou s'agit-il d'une simple fusion/modification/éclaircissements de la loi existante ?
4. Qu'est-ce que la LRens aura comme conséquence sur le citoyen lambda ?
5. On entend souvent que de toute façon nous sommes déjà surveillés, cela est-il vrai ? La LRens le permet-elle ?
6. La LRens met des restrictions à l'application de la LPD, cela pose-t-il problème ? Et en quoi ?
7. Le fait que le SRC puisse renoncer à informer une personne qui a fait l'objet d'une surveillance pose-t-il problème ? Les motifs qui peuvent être invoqués pour cela sont-ils pertinents ?
8. Le contrôle des mesures soumises à autorisation par le TAF est présenté comme une sécurité, l'est-il vraiment ? Et le fait que la demande soit examinée par le « président de la cour compétente du TAF […] en tant que juge unique » (art. 28 al. 2) ?
9. La LRens parle des activités du SRC sur territoire national, qu'en est-il des opérations extérieures ?
10. Que se passe-t-il si je suis en Suisse mais que je téléphone à l'étranger ? La LRens s'applique-t-elle ? Si non, ne se retrouve-t-on pas là dans une situation analogue à celle des USA qui n'ont pas besoin d'obtenir de mandat pour surveiller les communications vers l'international ?
11. Vu les dérogations prévues et les moyens, pour le SRC, de contourner les restrictions, cette loi n'est-elle qu'une parodie de législation ?
12. Cette loi s'attaque-t-elle à l'état de droit ? Les fondements de la démocratie sont-ils (suffisamment) protégés ?
13. Cette menace de surveillance pourrait-elle peser sur la détermination des citoyen-ne-s à exprimer leur opinion ? Pourrait-on dériver vers une autocensure due à une suspicion d'être surveillé ?
14. Les outils de cryptographie que nous connaissons actuellement seront-ils suffisamment puissants pour empêcher l'interception/le déchiffrage de nos communications par le SRC ? Avons-nous, en tant que citoyen-ne les moyens de nous protéger de l'Etat ?
15. Existe-t-il un risque de privatisation du renseignement en Suisse, tel que c'est le cas aux USA avec des entreprises sous-traitantes de la NSA notamment ?
16. Y a-t-il réellement des raisons de s'inquiéter de cette nouvelle loi ? Si oui, lesquelles ?
17. Les récents attentats à Paris et Bruxelles ne prouvent-ils pas que nous devons renforcer notre sécurité ?
18. On entend souvent dire qu'il ne faut pas abandonner nos droits fondamentaux pour plus de sécurité, les deux (sécurité et liberté) sont-ils donc incompatibles ? Ou complémentaires ?
19. Dans le cas d'une surveillance lancée par une procédure d'urgence et non-autorisée par le TAF, les données récoltées devront être détruites, comment, à l'ère du numérique, être sûr que ce sera le cas alors que certains logiciels permettent de récupérer des données effacées plusieurs fois ?
20. Si une surveillance ne donnait pas de résultats, aucun action en justice ne pourrait avoir lieu, qu'adviendrait-il des données ? La personne concernée serait-elle informée ? Pourrait-elle obtenir la liste des données récoltées et exiger leur destruction ?
21. Les personnes qui n'étaient pas directement visées par la mesure mais qui ont été touchées (les correspondants, membres de la famille utilisant le même téléphone, …) auraient-ils qualité pour agir en justice (nécessite de savoir de qui les communications ont été interceptées, donc d'en obtenir la liste) ? Avec les mêmes droits et chances de succès que la personne concernée ? Les membres de la famille devraient-ils agir séparément ou l'un d'entre eux pourrait-il agir au nom de tous ?
22. Comment vérifier l'utilisation des GovWares ? Ils devraient générer une journalisation complète, comment garantir que cette dernière ne puisse pas être modifiée après coup ? L'utilisation de logiciels libres serait-elle envisageable ?