

# L'échange et l'utilisation des informations récoltées par les services de renseignement belges

Mémoire réalisé par

**Sébastien Noirhomme**

Promotrice

**Professeure Maria Luisa Cesoni**

Année académique 2017-2018

**Master en criminologie à finalité spécialisée : criminologie de l'intervention**



Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation\*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

## Avant Propos

Au terme de cette recherche, je tiens à remercier les personnes suivantes qui m'ont permis de réaliser ce mémoire :

Madame Luisa Cesoni, promotrice de ce mémoire, professeur à l'Université catholique de Louvain (UCL), pour ses conseils avisés, mais également pour son implication et sa disponibilité tout au long de l'année, lors de la réalisation et de la rédaction de ce document ;

Le Lieutenant-Colonel Goemanne, mon maitre de stage au sein de la Défense, pour ses remarques et ses remises en question toujours pertinentes, mais également pour ses conseils prodigués et ses relectures attentives ;

Tous les professionnels que j'ai eu la chance d'interroger, pour le temps consacré aux entretiens et pour les informations données qui sont précieuses et rendent ce mémoire unique : Madame P. Somers, substitute du procureur du Roi au parquet fédéral, Monsieur G. Dallemagne, député fédéral, Monsieur P. Pétry, directeur général adjoint de la Sûreté de l'Etat, le Juge d'instruction, le membre de la Sûreté de l'Etat, le membre du Service général du renseignement et de la sécurité, le membre de l'Organe pour la coordination et l'analyse de la menace, et les membres du ministères des Affaires étrangères ;

Madame Anne Desmarets, pour l'aide apportée ;

Madame Pascale Berryer, pour sa relecture attentive ;

Mes parents, Philippe Noirhomme et Véronique Delens pour leur soutien indéfectible durant tout mon parcours académique.

## Lexique des abréviations

BIM : *Bijzondere inlichtingenmethoden*, équivalent à MRD

BNG : Banque national générale

DGSI : Direction générale de la sécurité extérieure

CGRA : Commissariat général aux réfugiés et aux apatrides

CNS : Conseil national de sécurité

Comité de coordination : Comité de coordination du renseignement et de la sécurité

Comité R : Comité permanent R

Comité stratégique : Comité stratégique du renseignement et de la sécurité

CSIL : Cellule de sécurité intégrale locale

FTF : Foreign Terrorist Fighter

GIA : Groupe interforces antiterroriste

JIB : Joint information box

MRD : méthodes de recueil de données, équivalent à BIM

OCAM : Organe de coordination pour l'analyse de la menace

Plan R : Plan Radicalisme

SGRS : Service général de renseignement et de sécurité

TFL : Task Force locale

TFN : Task Force nationale

VSSE : *Veiligheid van de Staat* – Sûreté de l'Etat

## Table des matières

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Avant Propos.....                                                       | 4  |
| Lexique des abréviations.....                                           | 5  |
| Table des matières.....                                                 | 6  |
| Introduction.....                                                       | 10 |
| Chapitre I – Les théories et concepts du renseignement.....             | 12 |
| I.1. Définir le renseignement.....                                      | 12 |
| I.1.1. La fonction du renseignement .....                               | 13 |
| Figure I : l’action préventive et l’action préemptive.....              | 15 |
| I.1.2. Les différents types et formes de renseignement.....             | 16 |
| I.1.3. Les différentes structures du renseignement.....                 | 17 |
| I.2. Le cycle du renseignement .....                                    | 20 |
| I.2.1. Le cycle « classique » du renseignement.....                     | 20 |
| Figure II : Le cycle du renseignement .....                             | 21 |
| I.2.2. Les critiques du cycle du renseignement .....                    | 22 |
| I.3. Les niveaux et les obstacles à la coopération .....                | 24 |
| I.3.1. Les niveaux de la coopération .....                              | 24 |
| I.3.2. Les obstacles à la coopération .....                             | 25 |
| Chapitre II – Les acteurs du renseignement belge .....                  | 27 |
| II.1. La Sûreté de l’Etat.....                                          | 28 |
| II.1.1 L’organisation .....                                             | 29 |
| II.1.2. Les missions .....                                              | 30 |
| II.2. Le Service général de renseignement et de sécurité (SGRS) .....   | 32 |
| II.2.1. L’organisation .....                                            | 32 |
| II.2.2. Les missions .....                                              | 32 |
| II.3. L’Organe de coordination pour l’analyse de la menace (OCAM) ..... | 35 |
| II.3.1. L’organisation .....                                            | 36 |

|                                                                                                                                                                                                                         |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| II.3.2. Les missions .....                                                                                                                                                                                              | 36 |
| II.4. Le Comité permanent R.....                                                                                                                                                                                        | 39 |
| II.4.1. L'organisation.....                                                                                                                                                                                             | 40 |
| II.4.2. Les missions .....                                                                                                                                                                                              | 41 |
| II.5. Les différents conseils et comité liés au renseignement.....                                                                                                                                                      | 43 |
| II.5.1. Le Conseil national de Sécurité (CNS) .....                                                                                                                                                                     | 43 |
| II.5.2. Le Comité stratégique de renseignement et de la sécurité .....                                                                                                                                                  | 43 |
| II.5.3. Le Comité de coordination du renseignement et de la sécurité.....                                                                                                                                               | 44 |
| II.6. Le monde du renseignement belge .....                                                                                                                                                                             | 45 |
| Figure III : Entités représentées, de manière permanente ou non permanente, au<br>Comité de coordination du renseignement et de la sécurité ou ayant un accès,<br>direct ou indirect, à la base de données « FTF »..... | 47 |
| Chapitre III – Le cadre politico-juridique du recueil, de l'échange et de l'utilisation des<br>données.....                                                                                                             | 48 |
| III.1. Les méthodes de recueil de données (MRD ou BIM).....                                                                                                                                                             | 48 |
| III.1.1. Les méthodes ordinaires de recueil de données .....                                                                                                                                                            | 48 |
| III.1.2. Les méthodes spécifiques de recueil de données .....                                                                                                                                                           | 50 |
| III.1.3. Les méthodes exceptionnelles de recueil de données .....                                                                                                                                                       | 51 |
| III.2. Le contrôle des MRD .....                                                                                                                                                                                        | 52 |
| III.2.1. Le contrôle des méthodes de recueil de données par la Commission BIM<br>.....                                                                                                                                  | 52 |
| III.2.2. Le contrôle des MRD par le Comité R.....                                                                                                                                                                       | 53 |
| III.2.3. Les principes régissant l'autorisation et le contrôle des MRD .....                                                                                                                                            | 54 |
| III.3. La protection du secret .....                                                                                                                                                                                    | 56 |
| III.3.1. La classification et l'habilitation.....                                                                                                                                                                       | 57 |
| III.3.2. Le besoin d'en connaître (need-to-know) .....                                                                                                                                                                  | 58 |
| III.3.3. La règle du tiers service (originator control).....                                                                                                                                                            | 59 |
| III.3.4. Le need-to-share.....                                                                                                                                                                                          | 60 |

|                                                                                                                 |    |
|-----------------------------------------------------------------------------------------------------------------|----|
| III.4. Le cadre juridique de l'échange des informations .....                                                   | 61 |
| III.4.1. L'échange entre les services de renseignement .....                                                    | 61 |
| III.4.2. L'échange entre les services de renseignement et les autres services<br>publics .....                  | 61 |
| III.4.3. L'échange entre les services de renseignement et les services étrangers                                | 69 |
| III.5. Le cadre juridique de l'utilisation des informations .....                                               | 69 |
| III.5.1. L'utilisation politique des informations .....                                                         | 70 |
| III.5.2. L'utilisation judiciaire des informations .....                                                        | 70 |
| III.5.3. L'utilisation administrative des informations .....                                                    | 76 |
| Chapitre IV – L'état des lieux de l'échange d'informations des services de renseignement<br>.....               | 78 |
| IV.1. L'échange d'informations entre les services de renseignement en pratique .....                            | 78 |
| IV.2. L'échange d'informations entre les services de renseignement et les services<br>publics en pratique ..... | 79 |
| IV.2.1. La relation entre les services de renseignement et les services de police<br>.....                      | 79 |
| IV.2.2. La relation entre les services de renseignement et l'administration<br>pénitentiaire.....               | 80 |
| IV.2.3. La relation entre les services de renseignement et le FOREM .....                                       | 82 |
| IV.2.4. La relation entre les services de renseignement et les autres services<br>publics .....                 | 83 |
| IV.2.5. L'implication des services de renseignement dans les plateformes de<br>concertation.....                | 85 |
| IV.3. L'échange d'informations au niveau international en pratique .....                                        | 87 |
| IV.3.1. Les relations des services de renseignement belges avec leurs homologues<br>étrangers .....             | 88 |
| IV.3.2. Le principe du tiers pays .....                                                                         | 88 |
| IV.4. Conclusion sur l'échange d'informations .....                                                             | 90 |

|                                                                                                |     |
|------------------------------------------------------------------------------------------------|-----|
| Chapitre V – L’utilisation des informations collectées par les services de renseignement ..... | 92  |
| V.1. L’utilisation politique des informations en pratique .....                                | 92  |
| V.1.1. La proximité des politiques avec les services de renseignement .....                    | 92  |
| V.1.2. L’implication des services de renseignement dans les politiques sécuritaires .....      | 94  |
| V.1.3. Le pilotage politique des services de renseignement .....                               | 96  |
| V.2. L’utilisation judiciaire des informations en pratique .....                               | 97  |
| V.2.1. L’équilibre entre l’enquête de renseignement et l’enquête judiciaire .....              | 97  |
| V.2.2. La dénonciation d’une infraction par les services de renseignement.....                 | 100 |
| V.2.3. Le témoignage d’un agent de renseignement en pratique .....                             | 100 |
| V.2.4. L’utilisation des preuves illégales en pratique .....                                   | 101 |
| V.3. L’utilisation administratives des informations en pratique .....                          | 102 |
| V.4. Conclusion sur l’utilisation des informations .....                                       | 104 |
| Conclusions .....                                                                              | 106 |
| Bibliographie.....                                                                             | 109 |
| 1. Monographie .....                                                                           | 109 |
| 2. Articles scientifiques & doctrine.....                                                      | 109 |
| 3. Textes législatifs.....                                                                     | 110 |
| 4. Jurisprudence.....                                                                          | 112 |
| 5. Mémoire .....                                                                               | 112 |
| 6. Rapports d’activités, communiqués de presse et autres sources non-scientifiques.....        | 112 |

## Introduction

Les attentats de ces dernières années, en France et en Belgique, ont mis en doute l'efficacité des services de renseignement belges. Ces derniers ont été mis sous le feu des projecteurs des médias et des politiques. Tous voulaient comprendre quels dysfonctionnements ont mené à l'échec du 22 mars 2016. Très vite, le faible échange d'informations a été pointé du doigt comme étant responsable de l'impuissance des services de renseignement à contrecarrer la menace terroriste<sup>1</sup>.

Cette attention médiatique et ma participation à un stage au sein du service militaire de renseignement, le SGRS, ont éveillé mon intérêt sur le rôle des services de renseignement en Belgique. S'il existe une littérature sur le rôle et les théories du renseignement, très peu d'ouvrages consacrent une analyse particulière sur les services de renseignement belges. Aucune étude ne permettait d'atténuer cette curiosité.

Ces raisons m'ont poussé à étudier l'importance de l'échange d'informations et l'utilité de celles-ci. Puisqu'il n'y avait pas beaucoup de littérature, il était intéressant de traiter ces deux thématiques en parallèles.

Plus précisément, cette étude tente d'établir avec quelles administrations les services de renseignement communiquent et comment ces acteurs peuvent faire usage des informations afin de cerner le rôle du renseignement belge. De plus, il y a deux objectifs secondaires. L'un est de comprendre pourquoi l'échange d'information est capital à l'efficacité de ces services. L'autre est de comparer les dispositions législatives quant à l'échange et de l'utilisation des données récoltées par les services de renseignement belges et ce qui se passe en réalité.

La réalisation de ces objectifs est rendue particulièrement difficile en raison de la culture du secret, intrinsèque au monde du renseignement et du manque de littérature à ce sujet. C'est pour ces raisons que la recherche s'est attaché à apporter des éléments de réponse sur base de l'expérience de professionnels interrogés.

---

<sup>1</sup> Christophe Lamfalussy, « La Sûreté et le SGRS ne se parlent pas assez ». La Libre Belgique, le 19 mai 2016. [En ligne] <http://www.lalibre.be/actu/belgique/la-surete-et-le-sgrs-ne-se-parlent-pas-assez-573caee735702a22d77d49a9>

Bien qu'elle ait éveillé une certaine curiosité, la menace terroriste n'est pas l'étalon de référence pour analyser le rôle des services de renseignement. Autant les éléments mis en place pour lutter contre le terrorisme que ceux instaurés pour contrecarrer les autres menaces qui préoccupent les services de renseignement seront présentés.

En pratique, le mémoire se structure en cinq chapitres. Tout d'abord, il est essentiel de se familiariser avec les théories et les concepts du renseignement pour pouvoir analyser les règles qui régissent cette discipline particulière. Ensuite, la législation belge servira de support aux deux chapitres suivants. Dans un premier temps, celle-ci permettra de présenter les acteurs du renseignement belge. Dans un second temps, elle éclairera les pratiques prévues afin de recueillir, d'échanger et d'utiliser les informations récoltées par les services de renseignement belges. Les deux derniers chapitres aborderont respectivement l'échange et l'utilisation des informations en se basant sur les clarifications apportées par les professionnels.

Je ne prétends pas à l'exhaustivité de mon analyse qui constitue, avant tout, une étude générale du rôle des services de renseignement belges.

## Chapitre I – Les théories et concepts du renseignement

### I.1. Définir le renseignement

Les auteurs s'accordent pour dire qu'il est extrêmement complexe de donner une définition précise du renseignement. Comme l'écrivent Olivier Chopin et Benjamin Oudet, « *la diversité des phénomènes observables du renseignement, la nature secrète des services et agences, la pluralité des cultures nationales, la multiplication des destinataires et consommateurs du renseignement* »<sup>2</sup> rendent difficilement opérable une unique et concise définition du renseignement. Ce mémoire n'a pas la prétention d'apporter une nouvelle définition, mais il a pour objectif d'apporter différents éclairages afin de mieux comprendre le renseignement belge.

Il est essentiel de différencier le concept étymologique de l'information de celui du renseignement. Dans l'un de ses premiers rapports d'activité, le Comité R présente avec justesse la différence entre ces deux notions en affirmant que « *l'information est un élément de connaissance susceptible d'être codé pour être conservé, traité ou communiqué. Le renseignement est un ensemble des connaissances de tous ordres sur un adversaire potentiel, utiles aux pouvoirs publics et au commandement militaire* »<sup>3</sup>. Autrement dit, un renseignement est un traitement et un recoupement d'informations.

Il est également intéressant de s'attarder sur la définition du renseignement que Sherman Kent a rédigée en 1949<sup>4</sup>. Cette définition impute trois dimensions au renseignement, qui répondent aux questions « *Quoi ? Comment ? Qui ?* ». La première dimension du renseignement est celle de la « connaissance ». En effet, le renseignement c'est, avant tout, construire une connaissance autour d'une personne, d'un objet, d'un lieu ou d'un phénomène. La seconde dimension est celle des « activités ». Cette dimension rapporte la manière dont le renseignement opère. En d'autres termes, le renseignement se définit aussi à travers le processus par lequel l'information va être analysée, travaillée et recoupée pour devenir un renseignement à destination du pouvoir politique. Ainsi, le renseignement est aussi un processus appelé « cycle du renseignement » (*Chapitre I.2*).

---

<sup>2</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». Armand Colin, 2016. p. 33.

<sup>3</sup> Comité R, « Rapport d'activité du Comité R 1996 ». p. 138.

[En ligne] <http://www.comiteri.be/images/pdf/Jaarverslagen/1996%20fr.pdf>

<sup>4</sup> Cette définition est présentée dans l'ouvrage « *renseignement et sécurité* » d'O. Chopin et de B. Oudet en 2016.

La troisième dimension se rapporte à la manière dont est organisé le renseignement dans la bureaucratie. Le renseignement n'est pas l'affaire de tous, il est confié spécialement à des administrations spécialisées dans le renseignement. En conclusion, le renseignement serait la construction de la connaissance par des administrations spécialisées selon un processus qui a pour objectif de traiter l'information afin d'éclairer le pouvoir politique.<sup>5</sup>

Enfin, il est nécessaire d'ajouter à cette définition quelques notions telles que la fonction du renseignement, les différents types et formes de renseignement, ainsi que la typologie des structures nationales.

#### *1.1.1. La fonction du renseignement*

La fonction primaire du renseignement est d'être les yeux et les oreilles du gouvernement. Idéalement, les services de renseignement fournissent des informations, autant que possible, précises, exactes, complètes et objectives au pouvoir exécutif afin que celui-ci prenne des décisions éclairées<sup>6</sup>. Néanmoins, s'il revient aux services de renseignement d'offrir une telle connaissance à l'exécutif, c'est à ce dernier de prendre les décisions et d'en assumer les responsabilités<sup>7</sup>. Dès lors, les services de renseignement ont pour vocation d'informer le gouvernement à propos d'un phénomène, d'un objet, d'une personne, d'un lieu menaçant ou menacé afin que celui-ci prenne les décisions politiques adéquates pour endiguer le phénomène.

Il y a trois fonctions essentielles du renseignement qui découlent de la théorie du « réalisme offensif » des relations internationales<sup>8</sup>. Cette théorie implique que les Etats, qui sont les acteurs centraux de cette vision, veulent connaître les intentions des autres Etats afin d'assurer leur objectif ultime : leur survie<sup>9</sup>. Cette vision du système international implique que les fonctions du renseignement sont : la prévention de la surprise stratégique, la protection de l'Etat contre ses ennemis intérieurs et extérieurs, et la sécurisation de la société démocratique afin que la population garde confiance dans les institutions étatiques<sup>10</sup>. Ce dernier objectif consiste à augmenter la capacité de l'Etat et de ses citoyens à résister à un choc qui pourrait remettre en cause son existence, c'est-à-dire sa capacité de résilience.

---

<sup>5</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». op. cit. pp. 35-39.

<sup>6</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». Lavauzelle, 2005. p. 127

<sup>7</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». Odile Jacob, 2015. p. 27.

<sup>8</sup> Ibidem. p. 25.

<sup>9</sup> Ibidem.

<sup>10</sup> Ibidem.

Il est nécessaire de souligner la différence entre le concept de « law enforcement » et d'« intelligence » comme le fait Thierry Coosemans<sup>11</sup>. Le premier concept se rattache à la fonction policière. L'objectif de celui-ci est d'arrêter les auteurs des délits et des crimes et de les juger. Ainsi, la police est organisée autour de cette finalité judiciaire. A l'inverse, la finalité du renseignement est politique. Ces deux finalités sont aussi construites autour de deux stratégies différentes que sont l'action préventive et l'action préemptive. L'action préventive relève de la mission politique qui tente de contrecarrer une situation potentiellement indésirable, alors que l'action préemptive est le devoir de la police afin d'empêcher la commission d'un fait certain et imminent. Ces deux stratégies sont justement différenciées par Jacques Baud dans le schéma suivant (voir *figure 1*)<sup>12</sup>. D'un côté, il y a « *le contre-terrorisme, qui est l'ensemble des mesures destinées à combattre le terrorisme en amont de l'action terroriste. Il est la composante préventive de l'action et implique une combinaison de mesures politiques, des méthodes très pointues d'infiltration des réseaux et de recherche de renseignement active à l'étranger, etc. Il nécessite un personnel peu nombreux, mais très spécialisé, ainsi qu'une étroite coopération internationale* »<sup>13</sup>. De l'autre, il y a « *l'antiterrorisme, qui rassemble les moyens de la lutte en aval de l'action terroriste. Il est la composante préemptive et réactive de l'action, et résulte souvent d'un échec (ou d'un défaut) d'une stratégie de contre-terrorisme. Il implique généralement des structures plus lourdes, un système de surveillance important nécessitant des moyens techniques coûteux et une présence en personnel importante. Il exige également une capacité d'intervention spécialisée, que l'on trouve généralement dans les corps de police ou dans les forces paramilitaires* »<sup>14</sup>. En bref, le renseignement a une fonction de prévention, alors que la police s'inscrit dans une logique de réaction. Cette différenciation tend à s'effacer par le fait que la police est de plus en plus proactive en matière de terrorisme<sup>15</sup>.

---

<sup>11</sup> Coosemans, Thierry. « L'Union européenne et le renseignement : perspectives de coopération entre les États membres ». GRIP, Groupe de Recherche et d'Information sur la Paix et la Sécurité, 2004, pp. 10-11.

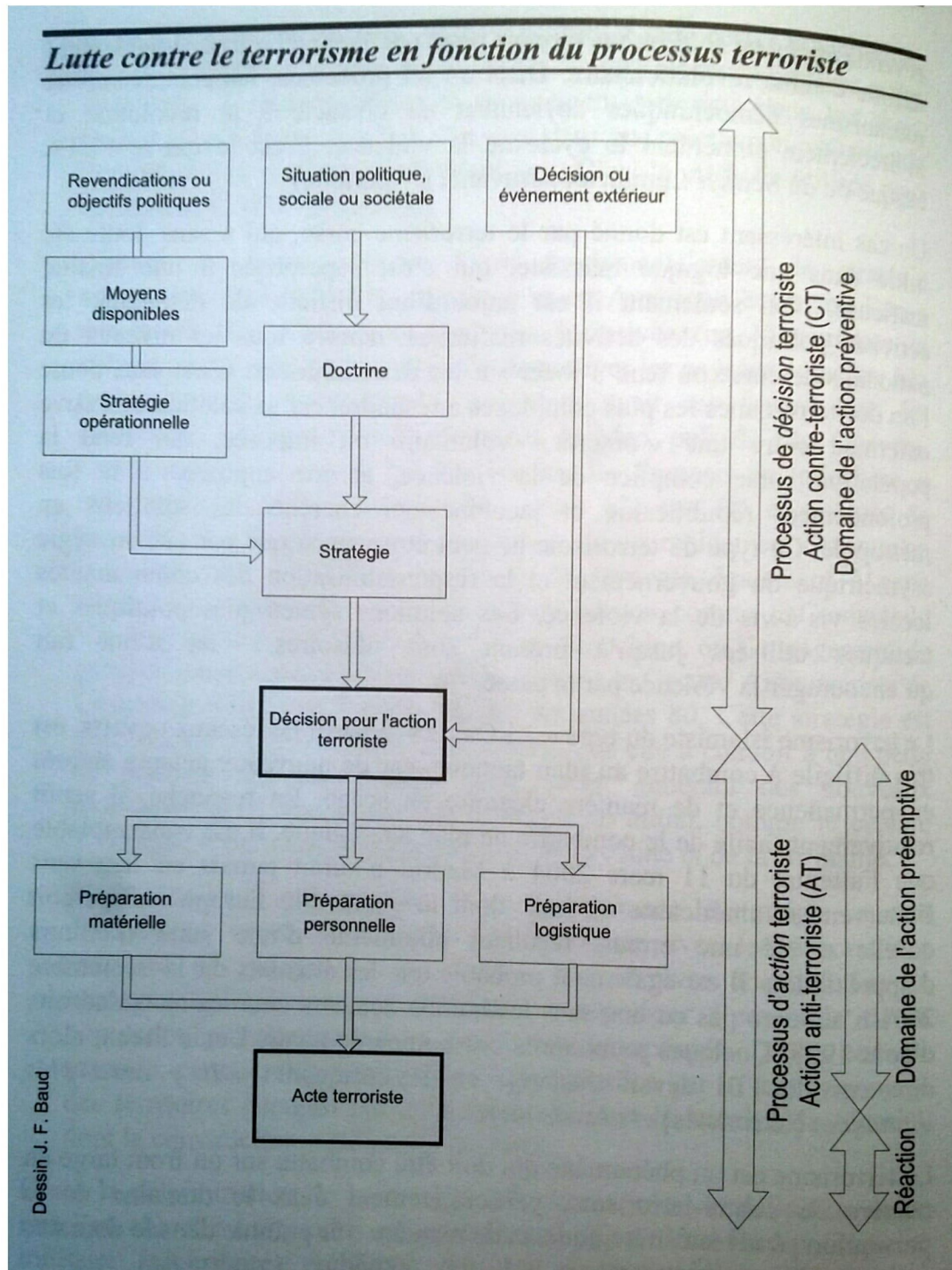
<sup>12</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». op. cit. p. 304.

<sup>13</sup> Ibidem. p. 298.

<sup>14</sup> Ibidem.

<sup>15</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. p. 298.

Figure I : l'action préventive et l'action préemptive<sup>16</sup>



<sup>16</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». op. cit. p. 304.

### *1.1.2. Les différents types et formes de renseignement*

Selon J. Baud, il y a, d'un côté, quatre types de renseignement, et de l'autre, quatre formes de renseignement<sup>17</sup>. Les types de renseignement se distinguent par leurs finalités : politique, judiciaire, militaire et opérationnelle. Les formes se différencient par le moment où l'action de renseignement va débiter : avant, pendant, après un événement ou en continu.

En ce qui concerne les quatre types de renseignement, l'auteur identifie le renseignement stratégique. L'objectif de ce type de renseignement est de reconstituer l'environnement d'un phénomène, ici, le terrorisme, avec les éléments politiques, économiques, sociaux ou encore militaire. Le renseignement stratégique est le résultat de la concertation des agences du renseignement et son client est le pouvoir exécutif pour lequel « *il contribue à la prise de décision visant à éviter le développement d'une situation [...]* »<sup>18</sup>. Dans le cadre du terrorisme, il s'agit de déterminer les « points de ruptures » qui représentent le point de basculement entre l'action politique et l'action violente, et les « centres de gravité » qui ont pour but de connaître la stratégie terroriste afin de mieux la contrer. Comme le souligne très bien J. Baud, l'intérêt de ces renseignements est d'être entendu par le politique afin qu'il puisse prendre des décisions à long terme. En d'autres termes, les renseignements stratégiques se raccrochent à l'action préventive qui est du domaine des services de renseignement.<sup>19</sup>

Il y a le renseignement de police. Celui-ci regroupe les activités qui ont pour objectif de récolter des indices, d'identifier des personnes, ou des réseaux, afin de les arrêter et de les juger, mais aussi de surveiller et de détecter des infrastructures, l'acquisition de matériel nécessaire à l'action criminelle. C'est le renseignement qui permet l'action préemptive. Comme l'analyse l'auteur, c'est entre ces deux types de renseignements que les services de police et de renseignement se rencontrent aux abords de la frontière très fine qui sépare les concepts de prévention et de préemption.<sup>20</sup>

Ensuite, l'auteur définit le renseignement de défense. Ces renseignements évaluent les menaces liées à la défense nationale et aident à définir les nécessités de la Défense pour y faire face.<sup>21</sup>

---

<sup>17</sup> Ibidem. pp. 128-131.

<sup>18</sup> Ibidem. p. 128

<sup>19</sup> Ibidem.

<sup>20</sup> Ibidem. p. 129.

<sup>21</sup> Ibidem.

Le dernier type est le renseignement opérationnel. C'est le renseignement le plus précis qui consiste au recueil des informations pertinentes à la planification et à la conduite des opérations de terrain<sup>22</sup>. Par exemple, ce renseignement peut porter sur le type de porte, blindée ou non, afin que l'équipe d'intervention sache quels outils employer pour franchir cet obstacle.

Concernant les quatre différentes formes du renseignement décrites par J. Baud, il y a, primo, le renseignement d'anticipation. L'objectif de ce renseignement est d'identifier les risques et d'évaluer la probabilité d'occurrence de ceux-ci. Ainsi, il peut permettre une action préventive, préemptive ou protectrice et sert à la prise de décision. L'auteur souligne les réticences qu'ont les services de renseignement à endosser ce rôle prédictif.<sup>23</sup>

Secundo, le renseignement situationnel a la spécificité d'étudier les événements en temps quasi-réel à travers un processus d'analyse et un cycle du renseignement rapide. Selon J. Baud, ce renseignement, qui étudie les événements présents et anticipe ceux à venir à très court terme, est souvent utilisé par le décideur lorsqu'il doit répondre devant les médias.<sup>24</sup>

Tertio, l'auteur décrit le renseignement d'investigation qui consiste à expliquer un événement passé<sup>25</sup>.

Quarto, il y a le renseignement de documentation qui est la constitution d'une connaissance de base. « *Cette documentation doit permettre d'appuyer les décisions routinières, mais doit aussi être suffisamment riche pour diminuer les besoins en renseignement complémentaires en cas de crise* »<sup>26</sup>. Selon J. Baud, cette démarche est commune à tous les types de renseignement, sert les organes d'analyse et nécessite une vision très large des problèmes.<sup>27</sup>

### *1.1.3. Les différentes structures du renseignement*

Après avoir défini le renseignement, analysé ses fonctions et étudié ses différentes formes, il est utile de s'attarder sur la typologie des systèmes nationaux de renseignement. Bien que chaque pays organise ses services de renseignement comme il l'entend, il est

---

<sup>22</sup> Ibidem. p. 129.

<sup>23</sup> Ibidem.

<sup>24</sup> Ibidem. pp. 130-131.

<sup>25</sup> Ibidem. 130.

<sup>26</sup> Ibidem.

<sup>27</sup> Ibidem.

possible de dégager quatre traits de caractères qui déterminent le type d'organisation de ces agences au sein de l'Etat<sup>28</sup>.

Il y a le modèle dit « intégré ». Ce modèle est caractérisé par une relation fusionnelle et de confiance entre les services de renseignement et le gouvernement<sup>29</sup>. Par exemple, en Grande-Bretagne, le renseignement extérieur est « *un instrument privilégié pour la prise de décision en matière de politique étrangère* »<sup>30</sup>.

Les services de renseignement peuvent suivre un modèle « unifié ». C'est le cas lorsque le pays ne dispose que d'une agence de renseignement principale, comme en Espagne, regroupant différentes disciplines, souvent réparties entre plusieurs services dans les autres pays.<sup>31</sup>

Certaines structures nationales de renseignement peuvent être considérées comme étant « communautaires ». Par exemple, les Etats-Unis disposent de plusieurs agences, chacune spécialisée dans une discipline du renseignement et celles-ci sont censées collaborer entre elles afin de produire un travail de renseignement complet<sup>32</sup>. Ainsi, une communauté du renseignement n'est pas seulement un regroupement d'agences, « *mais une machinerie complexe, qui fonctionne en symbiose, en exploitant les forces respectives de chaque service* »<sup>33</sup>.

Pour finir, la « dualité » peut caractériser une structure de renseignement. C'est le cas de la Belgique puisque celle-ci se base sur la différenciation entre le renseignement intérieur et extérieur afin de répartir les différentes tâches de renseignement entre les différents services.<sup>34</sup>

Selon J. Baud, la structure de renseignement basée sur la différenciation entre le renseignement intérieur et extérieur est issue de la Guerre Froide. A cette époque, la dualité du travail de renseignement était adaptée à la menace. Le renseignement militaire s'occupait de la menace venant de l'extérieur, c'est-à-dire de l'URSS, tandis que le

---

<sup>28</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ».op. cit. p. 46.

<sup>29</sup> Ibidem.

<sup>30</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». op. cit. p. 222.

<sup>31</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ».op. cit. p. 46.

<sup>32</sup> Ibidem.

<sup>33</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». op. cit. p. 222.

<sup>34</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ».op. cit. p. 46.

renseignement intérieur traitait la menace subversive sur le sol national<sup>35</sup>. Aujourd'hui, les trafics, la criminalité organisée ou le terrorisme, ont un caractère transnational<sup>36</sup>. Autrement dit, ces menaces tombent un jour sous la responsabilité du renseignement extérieur, et le lendemain, elles doivent être traitées par le renseignement intérieur. Cette dualité parfaite entre le renseignement intérieur et extérieur perd tout son sens lorsque les menaces ne sont plus structurées selon les frontières<sup>37</sup>. A la suite de ces changements, les services organisés par cette dualité ont tenté « *d'instaurer un continuum dans l'espace et assurer une continuité des responsabilités, et d'éviter que les menaces trans- ou internationales puissent trouver un espace de croissance* »<sup>38</sup>. En d'autres termes, les services de renseignement ont tenté de développer une coopération afin de contrer les différentes menaces. Néanmoins cette coopération a dû se confronter à « *des cadres juridiques, des formes et des cultures de renseignement différentes* »<sup>39</sup>. Il est intéressant de noter que J. Baud souligne qu'il est important d'éviter le partage de responsabilité entre les services<sup>40</sup>. Cela aurait pour effet que les différents services se renvoient la balle sur les tâches à effectuer. Enfin, certains pays ont décidé de fusionner leurs services de renseignement intérieur et extérieur. Selon l'auteur, ces fusions n'ont que peu souvent porté leurs fruits car ces différentes disciplines sont caractérisées par du personnel, des méthodes, des procédures et des cultures d'entreprises différentes. En guise de résultat, l'une des deux disciplines a souvent pris le pas sur l'autre qui a eu tendance à disparaître<sup>41</sup>.

Bien que certains auteurs décrivent les mêmes typologies, aucun ne se prononce sur l'efficacité d'une structure par rapport à une autre. Toutes possèdent de nombreux avantages et des inconvénients qui dépendent aussi du système politique dans lequel elles s'inscrivent, ce qui rend la comparaison difficilement qualifiable.

---

<sup>35</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». op. cit. p. 221.

<sup>36</sup> Ibidem. p. 137.

<sup>37</sup> Ibidem.

<sup>38</sup> Ibidem. p. 222.

<sup>39</sup> Ibidem.

<sup>40</sup> Ibidem.

<sup>41</sup> Ibidem. pp. 137-139.

## I.2. Le cycle du renseignement

Le cycle du renseignement est essentiel pour comprendre le processus des machines de renseignement étatiques. En d'autres termes, ce cycle est une définition fonctionnaliste pour rendre compte de la globalité des actions entreprises par les services de renseignement. Bien qu'il existe d'innombrables variantes de ce cycle du renseignement, ici, ne sera présenté que le cycle dit « classique » élaboré en 1949 par Sherman Kent<sup>42</sup> et encore utilisé aujourd'hui par la CIA<sup>43</sup> pour présenter ses activités au grand public. Celui-ci se compose de cinq étapes (*voir infra, figure II*). Cependant, il sera fait état des nombreuses critiques et améliorations portées à la première ébauche de ce concept.

### *I.2.1. Le cycle « classique » du renseignement*

La première phase du cycle du renseignement est celle de la « planification et de l'orientation ». Le cycle commence lorsque le décideur exprime un besoin de connaissance. Théoriquement, ce sont ces décideurs qui doivent désigner les objectifs stratégiques afin que les services de renseignement orientent leurs activités en accord avec ces mêmes objectifs. Comme tout cycle, l'arrivée est le point de départ. Dès lors, les décideurs endossent aussi le rôle de « consommateur ».<sup>44</sup>

La deuxième phase est celle de la « collecte » ou du « recueil » des informations. Il s'agit d'informations venant de sources « ouvertes » et de sources « couvertes ». En ce sens, les services de renseignement utilisent tout autant les journaux, les radios, et internet que leurs propres dispositifs, tels que les écoutes téléphoniques. Bref, la collecte d'informations n'a pas de limite, tout est bon à prendre.<sup>45</sup>

La troisième phase est celle du « traitement ». Cette phase est essentielle puisqu'il s'agit de recouper les différentes informations afin de les vérifier et de les considérer comme crédibles ou non<sup>46</sup>. De plus, c'est à ce moment que l'information va être classée, selon sa thématique et sa chronologie, par exemple<sup>47</sup>.

---

<sup>42</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». op. cit. p. 31.

<sup>43</sup> Central Intelligence Agency. (2007). « The Intelligence Cycle ». [En ligne] <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html> Consulté le 1er juin 2018.

<sup>44</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». op. cit. p. 47.

<sup>45</sup> Central Intelligence Agency. (2007). « The Intelligence Cycle ». [En ligne] <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html> Consulté le 1er juin 2018.

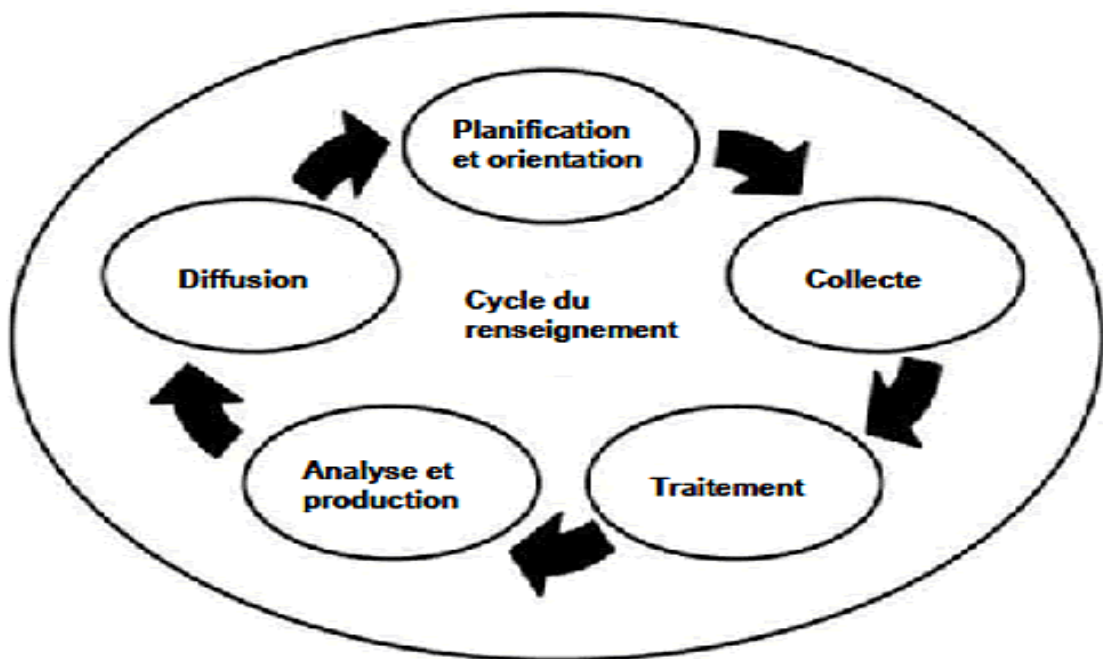
<sup>46</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». op. cit. p. 47.

<sup>47</sup> Bulinge, Franck. « Le cycle du renseignement : analyse critique d'un modèle empirique », Market Management 2006/3 (Vol. 6), p. 38.

La quatrième phase se compose de l'« analyse et de la production ». C'est l'étape de la synthèse de l'information qui va se muer en véritable renseignement<sup>48</sup>. Selon la CIA, c'est lors de cette étape qu'ils déterminent comment les différentes informations sont liées les unes aux autres. Une fois l'analyse réalisée, le service de renseignement doit être capable d'expliquer ce qu'il se passe, pourquoi cela se déroule, ce qu'il peut survenir par après et comment cela affecte les intérêts étatiques<sup>49</sup>. C'est aussi lors de cette étape que l'analyste va attribuer certains caractères au renseignement, comme les qualités de confidentialité et d'urgence, par exemple<sup>50</sup>.

La cinquième et dernière étape est celle de la « dissémination ». Lorsque les informations ont bel et bien mué en de véritables renseignements, ils sont remis au « consommateurs », c'est-à-dire les décideurs<sup>51</sup>. Afin que le renseignement soit utile, il est essentiel qu'il arrive à temps et à celui qui en aura l'utilité<sup>52</sup>.

Figure II<sup>53</sup> : Le cycle du renseignement



<sup>48</sup> Ibidem.

<sup>49</sup> Central Intelligence Agency. (2007). « The Intelligence Cycle ». [En ligne] <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html> Consulté le 1er juin 2018.

<sup>50</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». op. cit. p. 47.

<sup>51</sup> Ibidem.

<sup>52</sup> Ibidem. p. 49.

<sup>53</sup> Division de l'évaluation Secteur des politiques du Canada, « Rapport d'évaluation : sécurité en établissement ». Dossier n° 394-2-95. Février 2015. [En ligne] <http://www.csc-scc.gc.ca/publications/005007-2015-fra.shtml> Consulté le 6 mars 2018.

### 1.2.2. Les critiques du cycle du renseignement

De nombreux auteurs ont essayé d'apporter des améliorations au cycle dit « classique ». Malheureusement, il ne semble pas y avoir de consensus général sur un cycle du renseignement. Dès lors, il apparaît plus utile d'exposer les critiques faites à propos du cycle « classique ». Les critiques principales peuvent se regrouper en trois thématiques : la relation décideurs-services de renseignement, les activités des services de renseignement et le principe de rétroaction.

Tout d'abord, il y a un désaccord entre la théorie et la pratique à propos de la relation qu'entretiennent les décideurs avec les services de renseignement. Selon la théorie, les décideurs orientent les services afin que ceux-ci réduisent les zones d'ombres qui bordent leur prise de décision. En réalité, il semblerait que *« les autorités n'orientent pas les services mais attendent de leur part des alertes, les analystes cherchent à combler leurs propres gaps de connaissance, [...] [et que] les autorités n'hésitent pas à utiliser des renseignements bruts »*<sup>54</sup>. D'autres ajoutent même que *« les responsables politiques semblent attendre du renseignement plus un soutien et une légitimation que des informations »*<sup>55</sup>.

Ensuite, la critique porte sur l'absence de certains domaines d'activités ou de certaines relations qui sont parfois essentiels dans l'activité quotidienne d'un service de renseignement. En effet, le cycle du renseignement ne rend pas compte du contre-espionnage et pourtant, c'est cette activité qui rend le renseignement unique. Un service de renseignement doit composer avec des adversaires, que sont les autres services de renseignement, qui tentent d'induire en erreur le premier. En d'autres termes, les services de renseignement doivent développer un caractère paranoïde afin de remettre toujours en question la véracité d'une information et se poser la question si celle-ci n'est pas apparue dans le cycle du renseignement dans le seul but de nuire au service<sup>56</sup>. De plus, le cycle du renseignement « classique » n'aborde pas le domaine de l'action clandestine<sup>57</sup>. Cette action est l'œuvre d'un service de renseignement qui entreprend une mission en dehors du cadre légal sous la houlette de son gouvernement et qui nie en être l'auteur pour des raisons politiques. Bien qu'elle soit souvent la cause de nombreux fantasmes, l'action

---

<sup>54</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». op. cit. p. 32.

<sup>55</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». op. cit. p. 53.

<sup>56</sup> Ibidem. p. 41.

<sup>57</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». op. cit. p. 32.

clandestine semble une activité bien réelle de certaines puissances étatiques<sup>58</sup>. Néanmoins, il faut noter que ce genre d'action n'est pas une activité indispensable à l'existence d'un service de renseignement, puisque les services de renseignement belges existent tout en se passant d'un tel service<sup>59</sup>. Enfin, il est important de noter que le cycle inscrit les services de renseignement dans une relation unique avec le décideur et ne situe pas ces services dans un ensemble relationnel, marqué entre autres par la coopération internationale<sup>60</sup>. Il se pourrait qu'un service de renseignement oriente certaines de ses recherches à la demande d'un service étranger, par exemple.

La dernière critique cible l'absence de rétroaction dans le cycle du renseignement « classique ». En effet, le cycle rétroagit avec lui-même<sup>61</sup>. Comme l'écrivent Olivier Chopin et Benjamin Oudet : « [ce qu'il] *manque surtout dans la notion de cycle, c'est l'idée simple que chaque étape doit pouvoir rétroagir sur les étapes antérieures pour que le système fonctionne. La représentation circulaire induit réellement en erreur sur la façon dont l'activité de renseignement fonctionne au quotidien. Il faudrait représenter le cycle a minima comme un cycle de « boucles »* »<sup>62</sup>.

Il est important de souligner que ce cycle « classique » induit l'idée que l'activité de renseignement est un travail d'équipe. A l'inverse de ce qui est transmis par les différents films de fiction où un seul homme réalise pratiquement à lui tout seul un cycle complet du renseignement, ce cycle « classique » démontre l'importance de l'excellente réalisation de la phase antérieure afin que la phase suivante soit, elle aussi, parfaitement menée. Toutes ces phases sont des maillons d'une chaîne qui ne valent rien s'il n'y a pas d'étape précédente et suivante<sup>63</sup>.

---

<sup>58</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ».op. cit. p. 57.

<sup>59</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». p. 267.

<sup>60</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». op. cit. p. 32.

<sup>61</sup> Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». op. cit. p. 53.

<sup>62</sup> Ibidem.

<sup>63</sup> Ibidem. p. 51.

### I.3. Les niveaux et les obstacles à la coopération

Avant d'analyser les échanges de renseignements entre les services de renseignement belges, il est essentiel de faire le tour d'horizon des obstacles à la coopération intra- et internationale en matière de renseignement, reconnus dans la littérature et de présenter, en seconde partie, une typologie des niveaux de coopération possibles entre ces mêmes services.

#### *I.3.1. Les niveaux de la coopération*

J-C. Cousseran et P. Hayez formulent quatre modes de coopération internationale entre les services de renseignement, allant du plus basique au plus développé.

Le premier concerne la coopération « ad hoc ». Il s'agit d'échanges ponctuels, d'analyses ou de renseignement bruts, néanmoins encadrés par des accords bilatéraux.<sup>64</sup>

Le deuxième niveau de coopération est celui comprenant un « cadre permanent ». Il s'agit de plateformes multilatérales sur lesquelles il est possible d'échanger des informations de manière volontaire et régulière.<sup>65</sup>

Le troisième niveau est la « coopération opérationnelle ». Il peut s'agir d'entreprendre des opérations ou des formations communes, de partager des infrastructures permanentes à des fins opérationnelles, ou encore de se prêter assistance.<sup>66</sup>

Le quatrième niveau est non-seulement le plus développé en matière de coopération, mais aussi le moins abouti. Il s'agirait de « la division internationale du travail des services ». Ce mode de coopération implique la participation active de divers services de renseignement au sein d'un même cycle de renseignement, de la collecte à la dissémination, en passant par l'analyse. Il va sans dire que ce mode de coopération nécessite une totale transparence et une confiance à toutes épreuves. Comme exemple, les deux auteurs citent l'« EU INTCEN », à savoir l'« European Union Intelligence and Situation Centre ». Ce service, basé à Bruxelles, appartient au service de l'action extérieure de la Commission européenne et l'appuie afin de constituer sa connaissance en matière de politique étrangère. Bien que ce service soit précurseur, les auteurs soulignent qu'il ne s'agit que d'une esquisse.<sup>67</sup>

---

<sup>64</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». op. cit. p. 156.

<sup>65</sup> Ibidem. pp. 156-157.

<sup>66</sup> Ibidem. p. 157.

<sup>67</sup> Ibidem.

### *1.3.2. Les obstacles à la coopération*

Dans son ouvrage, Jacques Baud distingue cinq obstacles à l'échange d'informations entre les services de renseignement. Ceux-ci sont d'ordre sécuritaire, technique, opérationnel, juridique, et institutionnel.<sup>68</sup>

Tout d'abord, J. Baud met en exergue trois raisons de sécurité qui retiennent les services de renseignement d'échanger des informations de manière anodine. La première est la protection des intentions du décideur. En effet, autant la direction donnée par le décideur à ses services de renseignement que la production de ces derniers sont des indicateurs des ambitions stratégiques et politiques de l'Etat. Par conséquent, il est impératif que celles-ci soient couvertes par le secret afin que le décideur garde une marge de manœuvre lors du processus de décision. La deuxième est la protection des méthodes utilisées par le service de renseignement. Si celles-ci sont connues d'un adversaire, il n'aura aucun mal à s'en défendre et à rendre le service de renseignement non-opérationnel. La troisième protection est celle des sources. Il est impensable pour un service de renseignement de transmettre un élément qui donnerait des informations quant à l'origine de sa source au risque de la mettre en danger.<sup>69</sup>

Les obstacles peuvent être de nature technique. Les informations collectées par les services de renseignement sont cryptées et stockées dans des systèmes informatiques utilisant différents formats. Bien qu'il y ait des procédures d'uniformisation, le problème semble encore présent et entrave la fluidité de l'échange d'informations entre les services de renseignement.<sup>70</sup>

Ensuite, J. Baud décrit les contraintes juridiques existant et empêchant la transmission d'information entre les services de renseignement. Dans les démocraties, le recueil d'informations est soumis à un contrôle et certaines lois protègent la vie privée des citoyens afin de prévenir tout abus de ces services. Dans cette même logique de protection des données personnelles, il n'est pas légal pour les services de renseignement de transmettre n'importe quelle information à propos d'un citoyen, à n'importe qui, pour en faire n'importe quoi. En outre, il n'est pas acceptable pour un service de renseignement d'accepter une information venant d'un pays tiers alors que celle-ci a été acquise de

---

<sup>68</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales », op. cit. pp. 286-291.

<sup>69</sup> Ibidem. pp. 289-291.

<sup>70</sup> Ibidem. pp. 283-284.

manière illégale, sous la torture par exemple, par rapport à la législation de son pays et ce pour des raisons éthiques.<sup>71</sup>

D'un côté, J-C. Cousseran et P. Hayez indiquent que l'homogénéisation des pratiques de renseignement, nécessaire à une coopération élargie, implique souvent le contournement des dispositions légales nationales et, de ce fait, ralentit l'échange d'informations<sup>72</sup>. D'un autre côté, ces auteurs dénoncent aussi qu'il est arrivé que certains pays démocratiques n'aient pas refusé et aient même participé à l'acquisition d'informations en étant totalement hors du cadre juridique et éthique<sup>73</sup>.

Par la suite, J. Baud met en exergue l'obstacle opérationnel que pose l'échange d'informations. Afin que les échanges puissent se dérouler, il faut trois éléments qui ne sont que rarement présents simultanément. Il faut qu'il y ait un avantage comparatif. Les services de renseignement n'ont aucun intérêt à échanger de l'information s'ils n'acquièrent pas d'autres informations utiles à leurs yeux. En effet, le renseignement s'inscrit dans une logique de donnant-donnant, il faut donc avoir une certaine monnaie d'échange afin d'acquérir des informations venues d'ailleurs. La confiance est aussi un élément central à une bonne coopération. Si l'information n'est pas d'une qualité et d'une fiabilité exemplaires, un service de renseignement ne voudra pas obtenir cette information et encore moins offrir une contrepartie. Le dernier élément est la transparence. Un service de renseignement sera enclin à livrer une information s'il sait quel objectif elle va servir. Néanmoins, la nécessité du secret autour des intérêts de l'Etat entrave cette transparence et, de ce fait, l'échange d'informations.<sup>74</sup>

De la même manière, J-C. Cousseran et P. Hayez énoncent la théorie des jeux et le « dilemme du prisonnier » afin d'expliquer pourquoi les services de renseignement coopèrent ou non. Ainsi, ils insistent sur le fait que s'il existe une solidarité entre les services de renseignement ce n'est d'aucune façon un réflex altruiste, mais simplement parce qu'il existe une menace commune. Bien qu'un pays soit allié, il sera toujours bon de l'observer ne fût-ce que pour vérifier ses propres informations. Bref, la coopération entre les services de renseignement n'est jamais désintéressée. Cela explique aussi

---

<sup>71</sup> Ibidem. pp. 286-287.

<sup>72</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». op. cit. p. 160.

<sup>73</sup> Ibidem. pp. 166-167.

<sup>74</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales. op. cit. pp. 285-286.

pourquoi la coopération entre deux services de renseignement ne suit pas toujours la logique diplomatique<sup>75</sup>.

Enfin, J. Baud dénonce les obstacles institutionnels. Pour lui, les services de renseignement s'inscrivent dans une structure hiérarchique stricte qui paralyse l'échange d'informations. Bien que les informations vitales remontent facilement la pyramide hiérarchique, celles-ci ne sont pas transmises de manière transversale entre les services. Une raison à cet achoppement institutionnel est le corporatisme qui marque les services de renseignement.<sup>76</sup>

## Chapitre II – Les acteurs du renseignement belge

Patrick Leroy, un ancien professionnel du renseignement belge, différencie le concept de communauté d'agence de renseignement à celui de communauté de renseignement. D'un côté, il y aurait la communauté d'agence de renseignement qui regrouperait en un système fermé toutes les institutions proactives dans l'élaboration de renseignements. D'un autre côté, il y aurait la communauté du renseignement qui serait un système ouvert et intégrant n'importe quel acteur servant les intérêts de la culture du renseignement. En d'autres termes, il s'agirait d'une « *communauté d'idées, de connaissance* » qui inclurait, par exemple, le *Belgian Intelligence Studies Center* (BISC) et la *Belgian Intelligence Academy* (BIA). Ces agences n'ont pas pour objectif de nourrir le renseignement belge, mais plutôt de le développer et de le perfectionner en créant des liens avec le monde académique et d'autres horizons professionnels.<sup>77</sup>

Il peut y avoir une définition très minimaliste de la communauté d'agence du renseignement belge. Ce serait celle comprenant seulement les deux services de renseignement contrôlés par le Comité R<sup>78</sup>. A cela, il est possible d'ajouter l'OCAM, qui est aussi surveillée, entre autres, par le Comité R. Ce mémoire a pour objectif de comprendre les différents échanges et utilisations, qu'elles soient politiques, judiciaires

---

<sup>75</sup> Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement », op. cit. pp. 162-163.

<sup>76</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales. Op. cit. pp. 288-289.

<sup>77</sup> Leroy, Patrick. « La communauté du renseignement belge : essai de définition ». *Revue militaire Belge* 12, 2016. pp. 91-92.

<sup>78</sup> Idem.

ou administratives, des informations collectées par les services de renseignement belges. Dès lors, ce mémoire tente de dessiner le noyau central d'une communauté d'agences utilisant et échangeant des informations récoltées par les services de renseignement. Pour ce faire, ce mémoire présente la Sûreté de l'Etat, le SGRS, l'OCAM, le Comité R, le CNS et les comités de renseignement et de sécurité. Si ces agences sont décrites avec précision, c'est parce qu'elles jouent toutes un rôle central dans la production, l'échange, ou l'utilisation des informations récoltées par les services de renseignement ou parce que leur existence et leurs capacités sont généralement moins connues. Quant au Comité R, il est le garant d'un échange et d'une utilisation aussi efficace que démocratique de ces mêmes informations. Néanmoins, cette communauté d'agence ne s'arrête pas à ces quelques acteurs. C'est pour cette raison que le dernier point de ce chapitre citera brièvement les autres acteurs.

Aujourd'hui, comme le formule l'article 2 de la loi des services de renseignement, les deux services de renseignements doivent « *[respecter] et [contribuer] à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société* »<sup>79</sup>. Dès lors, les deux services de renseignement du pays ont pour objectif de protéger les individus et l'Etat de droit. Afin de connaître précisément ces deux acteurs principaux du renseignement belge, les deux sections suivantes présenteront ces deux services en analysant pour chacun leur organisation, compétences et missions.

## II.1. La Sûreté de l'Etat

La loi organique des services de renseignement et de sécurité du 30 novembre 1998 indique qu'il n'existe que deux services de renseignement en Belgique. La Sûreté de l'Etat (VSSE, *Veiligheid van de Staat* – Sûreté de l'Etat) est le service de renseignement civil. Ce service n'a pas attendu de la loi de 1998 pour exister. La Sûreté voit le jour le 15 octobre 1830. Sa première tâche était de protéger la Belgique, nouvellement indépendante, des tentatives de déstabilisations néerlandaises. Bien que la menace ait changé de visage, l'objectif semble être resté le même pour la Sûreté de l'Etat. Aux yeux

---

<sup>79</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 2 §1<sup>er</sup> alinéa 2.

de la loi, ses compétences et ses missions sont tournées vers l'intérieur du pays. C'est pour cette raison qu'elle est désignée comme le service de « renseignement intérieur ».<sup>80</sup>

### *II.1.1 L'organisation*

La Sûreté de l'Etat exécute ses missions sous l'autorité du ministre de la Justice dans le cadre des directives prescrites par le Conseil national de sécurité (*voir infra*)<sup>81</sup>. Néanmoins, le ministre de l'Intérieur possède une capacité de réquisition lorsque les missions de la Sûreté de l'Etat sont relatives au « *maintien de l'ordre public et à la protection des personnes* ». Ensuite, le ministre de l'Intérieur peut émettre des recommandations et des indications sur les moyens et sur les ressources, dans le cadre d'une réquisition. De plus, ce ministre est directement impliqué dans l'organisation et l'administration de la Sûreté de l'Etat. Ainsi, sa signature est nécessaire pour tout projet « de loi relatif à la Sûreté de l'Etat » et « d'arrêté réglementaire relatif à l'organisation générale de la Sûreté de l'Etat ». Enfin, ce dernier doit donner son avis conforme pour toute décision relative à la nomination, l'affectation des fonctionnaires généraux et aux attributions spécifiques confiées au directeur de la Sûreté de l'Etat.<sup>82</sup>

A travers ces différents articles, il apparaît que la Sûreté est sous la tutelle du ministre de la Justice et que le ministre de l'Intérieur possède toutefois un grand droit de regard en ce qui concerne l'élaboration de certaines missions et l'organisation générale du service.

Concrètement, 600 personnes travaillent pour la Sûreté de l'Etat et elle dispose d'un budget d'environ 45 millions d'euros en 2017. Elle est dirigée au jour le jour par un administrateur général et son adjoint. Ces 600 personnes travaillent soit pour les services extérieurs, soit les services intérieurs. Les premiers sont des unités de collecte. Ils sont sur le terrain et vont chercher les informations. Les seconds appartiennent aux services d'analyse. Ils reçoivent les informations récoltées par leurs collègues des services extérieurs et recoupent les différentes informations pour les muer en renseignement. Outre cette division, la Sûreté de l'Etat est basée à Bruxelles, mais elle possède sept postes provinciaux.<sup>83</sup>

---

<sup>80</sup> Rousseaux, Xavier, and David Somer. « Pour une histoire de la Sûreté de l'Etat en Belgique. Essai autour de 175 années de pénombre ». M. Cools, K. Dassen, R. Libert, and P. Ponsaers, *De Staatsveiligheid: Essays over 175*. p. 52

<sup>81</sup> Ibidem. Article 4.

<sup>82</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 4, 5 & 6.

<sup>83</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la

### II.1.2. Les missions

Aujourd'hui, la Sûreté de l'Etat est chargée de quatre missions, et d'une compétence qui dénote une anomalie.

La première mission est de « *rechercher, analyser et traiter les renseignements relatifs à toute activité qui menace ou pourrait menacer* :

- *la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel,*
- *la sûreté extérieure de l'État et les relations internationales,*
- *le potentiel scientifique ou économique défini par le Conseil national de sécurité,*
- *ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité »<sup>84</sup>.*

La loi énumère les activités qui pourraient menacer la sécurité intérieure du pays. Ainsi, « *l'espionnage, l'ingérence, le terrorisme, l'extrémisme, la prolifération, les organisations sectaires nuisibles, les organisations criminelles ; en ce compris la diffusion de propagande, l'encouragement ou le soutien direct ou indirect, notamment par la fourniture de moyens financiers, techniques ou logistiques, la livraison d'informations sur des objectifs potentiels, le développement des structures et du potentiel d'action et la réalisation des buts poursuivis* »<sup>85</sup> représentent les menaces que la Sûreté se doit de surveiller.

La deuxième mission est similaire à la première puisqu'il s'agit aussi de rechercher, d'analyser et de traiter des renseignements concernant les activités des services de renseignement étrangers sur le sol belge<sup>86</sup>. Il est intéressant de remarquer que l'idée de menace est absente de cette nouvelle mission confiée à la Sûreté de l'Etat en 2016<sup>87</sup>.

---

station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. pp. 272-273.

<sup>84</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 7, premier alinéa.

<sup>85</sup> Ibidem. Article 8, premier alinéa.

<sup>86</sup> Ibidem. Article 7, troisième alinéa.

<sup>87</sup> Loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique du 29 janvier 2016. Article 2.

La troisième mission concerne les enquêtes de sécurité. En effet, c'est la Sûreté de l'Etat qui est en charge de vérifier si un individu peut acquérir ou non une habilitation de sécurité<sup>88</sup>.

La quatrième mission stipule seulement que la Sûreté devra exécuter toutes autres missions que la loi lui indiquera. Cela démontre qu'une loi est nécessaire afin d'orienter la Sûreté de l'Etat sur une nouvelle mission<sup>89</sup>.

Enfin, comme cité au début de ce chapitre, le ministre de l'Intérieur a le droit de requérir la Sûreté de l'Etat afin de maintenir l'ordre public et la protection des personnes, comme par exemple lors de visites diplomatiques en Belgique<sup>90</sup>. Néanmoins, il est possible de se demander pourquoi cet article n'a pas été abrogé puisque la mission de protection des personnes qui incombait à la Sûreté de l'Etat a été transférée à la Police fédérale<sup>91</sup>. Cet arrêté n'a pas abrogé les compétences qu'a le Ministre de l'Intérieur par rapport à la Sûreté de l'Etat. Une hypothèse serait que la Sûreté dispose toujours d'une équipe d'intervention<sup>92</sup> réquisitionnable par le Ministre de l'Intérieur. Une autre serait qu'il y ait un attachement à l'implication et à la capacité d'action du ministre de l'Intérieur au sein de la Sûreté de l'Etat. En effet, suite aux lois de 1998 sur la réforme de la police et sur les services de renseignement, certains se sont posé la question de savoir s'il n'aurait pas mieux valu intégrer le service de renseignement civil directement au sein de la Police fédérale<sup>93</sup>. Cela aurait eu pour conséquence que la Sûreté de l'Etat aurait eu pour seul ministre de tutelle celui de l'Intérieur, alors qu'aujourd'hui elle est sous la responsabilité du ministre de la Justice, avec une implication non négligeable du ministre de l'Intérieur. Bref, il se peut que cette double tutelle soit le fruit d'un compromis belge entre service de police et service de renseignement et entre ministère de l'Intérieur et Ministère de la Justice.

---

<sup>88</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 7, second alinéa.

<sup>89</sup> Goossens, Franky, « Les missions et compétences des services de renseignement et de sécurité belges », *Journal des tribunaux* 6066, 2002. p. 620.

<sup>90</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 5, §2, premier alinéa.

<sup>91</sup> Loi portant des dispositions diverses Intérieur. - Police intégré du 21 avril 2016, article 92.

<sup>92</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 22.

<sup>93</sup> Goossens, Franky, « Les missions et compétences des services de renseignement et de sécurité belges » *op. cit.* p. 628.

## II.2. Le Service général de renseignement et de sécurité (SGRS)

Le SGRS voit le jour en 1915 afin de développer un service militaire de contre-espionnage et de planification d'opérations derrière les lignes allemandes<sup>94</sup>. Depuis lors, c'est le pendant militaire de la Sureté et, à l'inverse de celle-ci, il assure le renseignement extérieur.

### *II.2.1. L'organisation*

L'organisation du SGRS est plus claire car seul le ministre de la Défense interfère dans son organisation et dans son administration<sup>95</sup>. De plus, le SGRS réalise ses missions sous l'autorité du ministre de la Défense selon les directives du Conseil national de sécurité (*voir infra*)<sup>96</sup>. Il est important de comprendre que le SGRS fait partie intégrante de la Défense belge. Il y est dirigé par un lieutenant-général qui est directement sous l'autorité du ministre de la Défense, et non pas sous l'autorité du chef de la Défense (CHOD) comme les autres lieutenant-généraux de l'armée<sup>97</sup>.

En 2016, le SGRS disposait d'un budget avoisinant les 50 millions d'euros et employait 592 collaborateurs. La particularité de ce service militaire est qu'il est composé à la fois de militaires, près de 80% et de civils, 20%. Ce service est constitué, au minimum, de deux divisions : la Division du renseignement et la Division du renseignement de sécurité. La première se focalise sur les menaces extérieures alors que l'autre prend en charge les menaces intérieures. En 2012, le SGRS a dû mettre en place une cellule interne, appelée *Joint Cell Counter Terror*, réunissant ces deux divisions afin de mieux combattre le terrorisme. Il n'est pas possible d'en savoir plus sur l'organisation interne du SGRS qui est confidentielle.<sup>98</sup>

### *II.2.2. Les missions*

La loi organique du 30 novembre 1998 charge le SGRS de cinq missions.

La première mission concerne la recherche, l'analyse et le traitement de renseignements qui pourraient impacter la sécurité nationale ou internationale dans le cas où la Défense

---

<sup>94</sup> Ibidem. p. 103

<sup>95</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 10, §3.

<sup>96</sup> Ibidem. Article 10 §1 et 2.

<sup>97</sup> Cools, Marc, et al., eds. « 1915-2015 : Het verhaal van de Belgische militaire inlichtingen-en veiligheidsdienst. Maklu », 2015. p. 497.

<sup>98</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. pp. 279-282.

pourrait s'impliquer suite à cette déstabilisation<sup>99</sup>. En d'autres termes, le SGRS doit fournir une connaissance globale sur les phénomènes et les lieux où la Défense est susceptible d'opérer. Ceci est extrêmement large puisque la Belgique peut aussi bien se retrouver en Haïti afin d'assurer la protection de l'aide humanitaire ou en Syrie dans le cadre d'un conflit armé. De plus, il doit traiter de la même manière les renseignements qui pourraient menacer six cibles énumérées par la loi :

- « *l'intégrité du territoire national ou la population,*
- *les plans de défense militaires,*
- *le potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économiques et industriels liés à la défense et qui figurent sur une liste approuvée par le Conseil national de sécurité, sur proposition du ministre de la Justice et du ministre de la Défense,*
- *l'accomplissement des missions des Forces armées,*
- *la sécurité des ressortissants belges à l'étranger,*
- *tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité »*<sup>100</sup>

La loi stipule formellement que ces menaces doivent être de nature militaire pour que cela intéresse le SGRS<sup>101</sup>. D'ailleurs, il est un service militaire de renseignement et non un service de renseignement militaire<sup>102</sup>. Cette différence qui peut paraître anodine ne l'est pas. En effet, le fait que ce soit un service militaire de renseignement rend ce dernier compétent non seulement pour la récolte de renseignement tactiques, opérationnels, mais aussi stratégiques puisque celui-ci appuie le gouvernement dans la tenue de sa politique étrangère. C'est l'objectif de l'article 11 de la loi organique des services de renseignement et de sécurité qui stipule que le SGRS doit « *informer sans délai les ministres compétents ainsi que [de] donner des avis au gouvernement, à la demande de celui-ci, concernant la définition de sa politique intérieure et étrangère de sécurité et de défense* »<sup>103</sup>. Etrangement, il n'existe pas d'article similaire pour la Sûreté de l'Etat.

---

<sup>99</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 11, §1, premier alinéa.

<sup>100</sup> Ibidem.

<sup>101</sup> Ibidem. Article 11, §2.

<sup>102</sup> Ibidem. Article 2, §1.

<sup>103</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 11, §1, 1°.

La loi confère au SGRS la responsabilité des équipements, installations, documents et du personnel qui dépendent du ministre de la Défense<sup>104</sup>. Ainsi, toute menace dirigée vers la sécurité de tout élément touchant au domaine militaire intéresse le SGRS. Cette mission lui offre aussi la possibilité de répondre à une cyberattaque, ce qui a tendance à s'assimiler de plus à un acte de guerre dans le monde moderne<sup>105</sup>.

Ensuite, le SGRS est chargé de maintenir et d'assurer le secret de tout élément relatif à la Défense, tels les plans militaires, les bâtiments sensibles, les installations, les systèmes et moyens de communication informatiques<sup>106</sup>.

La quatrième mission du SGRS est d'effectuer les enquêtes de sécurité conformément aux directives du Conseil national de sécurité<sup>107</sup>.

La dernière mission du SGRS est exactement similaire à celle de la Sûreté de l'Etat puisqu'il s'agit de « *rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge* »<sup>108</sup>.

\*\*\*

La présentation de ces deux services et de leurs missions respectives fait apparaître la caractéristique « dual »<sup>109</sup> du renseignement belge puisque l'un, la Sûreté de l'Etat, s'occupe du renseignement intérieur, alors que l'autre, le SGRS, se concentre sur le renseignement extérieur.

Bien que la loi du 30 novembre 1998 semble nettement et clairement différencier les compétences de chaque service, la réalité est plus complexe. La menace terroriste, par exemple, semble intéresser les deux services. S'il paraît évident que la Sûreté de l'Etat s'y intéresse puisque la loi le lui indique, cela le semble moins pour le SGRS. Le terrorisme n'est pas une menace de nature purement militaire. Pourtant, le SGRS s'intéresse à la menace que le terrorisme fait peser sur le monde civil et non plus seulement sur le monde militaire depuis 2013, lorsqu'il crée un service dédié à l'étude du

---

<sup>104</sup> Ibidem. Article 11, §1, second alinéa.

<sup>105</sup> OTAN : communiqué de presse, « Communiqué sur le sommet de Varsovie » (2016) 100, §70, publié le 9 juillet 2016. [En ligne] [https://www.nato.int/cps/fr/natohq/official\\_texts\\_133169.htm](https://www.nato.int/cps/fr/natohq/official_texts_133169.htm)

<sup>106</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 11, §1, troisième alinéa.

<sup>107</sup> Ibidem. Article 11, §1, quatrième alinéa.

<sup>108</sup> Ibidem. Article 11, §1, cinquième alinéa.

<sup>109</sup> Cousseran, Jean-Claude, et Hayez Philippe. « Renseigner les démocraties, renseigner en démocratie ». Odile Jacob, 2015. p. 43

phénomène<sup>110</sup>. Cela s'explique par le fait que le phénomène implanté en Syrie et en Irak déstabilise la région et pourrait toucher la Belgique<sup>111</sup>. En d'autres termes, c'est le caractère international qui pousse le SGRS à s'y intéresser. De plus, vu l'intervention militaire belge contre l'Etat islamique, le terrorisme tombe pleinement dans les compétences du SGRS.

Enfin, il est intéressant de noter que le SGRS et la Sûreté de l'Etat ont une mission partagée, puisque les deux services sont compétents pour récolter et traiter les informations concernant les activités des services de renseignement étrangers opérant en Belgique<sup>112</sup>. Le législateur explique que s'il offre la même compétence aux deux services c'est parce que dans les faits la Sûreté et le SGRS se préoccupaient déjà de cette menace<sup>113</sup>. Le législateur a instruit les deux services de renseignement d'une compétence concurrente en connaissance de cause, mais il a préféré s'en remettre au Conseil national de sécurité qu'il charge de la répartition des tâches<sup>114</sup>. En tout état de cause, cette nouvelle mission entraîne, un peu plus, l'ambiguïté du partage des compétences entre les deux services de renseignement.

### II.3. L'Organe de coordination pour l'analyse de la menace (OCAM)

L'OCAM est institué par la loi organique du 10 juillet 2006. Cette institution remplace le Groupe Interforces Antiterroriste (GIA) dans le but de « *donner aux autorités politiques, administratives et judiciaires une image aussi précise que possible de la menace terroriste et extrémiste en Belgique ou visant la Belgique afin de leur permettre de réagir de manière adéquate* »<sup>115</sup>. En d'autres termes, l'OCAM est le carrefour de l'information du monde du renseignement en Belgique. Bien qu'il ne soit pas un service de

---

<sup>110</sup> Comité R, « Rapport d'activité du Comité R 2016 », pp. 32-33. [En ligne] [http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag\\_2016\\_FR.pdf](http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2016_FR.pdf)

<sup>111</sup> Idem.

<sup>112</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 7, troisième alinéa & article 11, §1, cinquième alinéa.

<sup>113</sup> Chambre des représentants de Belgique, « Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique ». Doc 54 0553/001, le 3 novembre 2014. p. 4

<sup>114</sup> Chambre des représentants de Belgique, « Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique ». Doc 54 0553/005, le 14 janvier 2016. p. 4

<sup>115</sup> Van Laethem, Wauter. « L'organe de coordination pour l'analyse de la menace : une analyse ponctuelle ». Virgiles. Revue du droit de police, 2007/4. p. 109.

renseignement, il est la charnière entre ces derniers et la police en matière de terrorisme et d'extrémisme. Dès lors, il est essentiel pour un mémoire portant sur l'échange et l'utilisation de l'information de s'intéresser à son organisation et à ses missions.

### *II.3.1. L'organisation*

L'OCAM est placé sous l'autorité conjointe des ministres de la Justice et de l'Intérieur qui sont responsables de son organisation et de son administration. Les membres de l'OCAM sont désignés et démis de leurs fonctions, en cas de faute grave, par le Roi et sur la proposition du ministre de l'Intérieur et/ou de la Justice. La loi distingue quatre sortes d'employés à l'OCAM.

- Il y a le directeur et le directeur-adjoint qui assurent la gestion quotidienne de l'OCAM. Ceux-ci doivent avoir la qualité de magistrat et effectuer leur fonction de manière indépendante. Ils sont nommés pour cinq ans et ce mandat est renouvelable deux fois.
- L'OCAM possède ses propres analystes.
- L'OCAM dispose d'un personnel administratif.
- L'OCAM accueille des experts détachés, à temps plein, venant des différents services d'appuis. La désignation de ces employés se fait par le Roi, mais la proposition revient au ministre compétent pour le service duquel l'intéressé est détaché. Ces services d'appuis sont au nombre de six :
  - les deux services de renseignement ;
  - les services de police locale et fédérale ;
  - le service public fédéral Finances, en particulier l'Administration des Douanes et Accises;
  - le service public fédéral Mobilité et Transports;
  - le service public fédéral Intérieur, en particulier l'Office des Etrangers;
  - le service public fédéral Affaires étrangères;

Il est intéressant de savoir que cette liste peut être aisément étendue par le Roi sur proposition du Comité ministériel du renseignement et de la sécurité (*voir infra*).<sup>116</sup>

### *II.3.2. Les missions*

La raison d'être de l'Organe de coordination de l'analyse de la menace est d'évaluer la menace<sup>117</sup>. Dès lors, il apparaît essentiel de définir quelle menace l'OCAM doit évaluer

---

<sup>116</sup> Loi relative à l'analyse de la menace du 10 juillet 2006, article 2, 5 & 7.

<sup>117</sup> Ibidem. Article 5, §1<sup>er</sup>, deuxième alinéa.

afin de connaître son domaine de compétence. Selon l'article trois de la loi OCAM, les menaces visées sont celles énumérées par l'article 8, 1<sup>o</sup>, B) et C) de la loi organique des services de renseignement et de sécurité du 30 novembre 1998. En d'autres termes, il s'agit de la menace terroriste et extrémiste qui « [porterait] *atteinte à la sûreté intérieure et extérieure de l'Etat, aux intérêts belges et à la sécurité des ressortissants belges à l'étranger ou à tout autre intérêt fondamental du pays tel que défini par le Roi sur la proposition du Comité ministériel* »<sup>118</sup>. Il est intéressant de noter que cette liste de menaces peut être étendue par le Roi sur proposition du comité ministériel du renseignement et de la sécurité, pourvu que la menace entre préalablement dans le cadre de l'article huit de la loi organique des services de renseignement.

Afin que l'OCAM atteigne son objectif, la loi l'instituant lui assigne trois missions spécifiques. L'une demande à l'OCAM d'évaluer stratégiquement et périodiquement si une menace terroriste ou extrémiste peut se manifester, ou, si elle est déjà présente, comment elle évolue, et quelles mesures sont nécessaires pour la combattre. Dès lors, le fait que la loi permette à l'OCAM de proposer des mesures afin de combattre la menace démontre l'objectif du législateur de faire de l'institution la véritable coordinatrice de la lutte contre le terrorisme et l'extrémisme. Il est important de noter que ces analyses stratégiques sont soit effectuées d'office, soit à la demande de n'importe quel membre du gouvernement. Néanmoins, cette évaluation est transmise au Comité ministériel, aux services d'appui, au membre du gouvernement qui a demandé l'évaluation, au Centre de crise, au Parquet fédéral et au procureur général qui est responsable de la matière du terrorisme et de l'extrémisme.<sup>119</sup>

La deuxième mission a le même objectif que la première mais ici, l'évaluation sera ponctuelle. Il évalue d'initiative le niveau de la menace qui pèse sur un événement, un lieu ou une infrastructure, ou qui émane d'un individu ou d'un groupe d'individu. Ces évaluations sont transmises au Comité ministériel, aux services d'appui, au Centre de crise, au Parquet fédéral et au procureur général qui est responsable de la matière du terrorisme et de l'extrémisme et à tout membre du gouvernement que le directeur de l'OCAM juge nécessaire d'informer. Seuls les services d'appui peuvent demander une analyse ponctuelle à l'OCAM. Dans ce cas, l'évaluation est transmise au service d'appui

---

<sup>118</sup> Ibidem. Article 3, §1<sup>er</sup>.

<sup>119</sup> Ibidem. Article 8 & 10.

et au ministre dont il dépend, ainsi qu'au Comité ministériel, au Centre de crise et au procureur général responsable de la matière du terrorisme et de l'extrémisme.<sup>120</sup>

Enfin, la dernière mission de l'OCAM est de nouer des liens avec les services étrangers et internationaux homologues<sup>121</sup>. Il est possible de comprendre qu'à travers cette dernière mission, l'OCAM est voué à devenir le carrefour entre tous les services nationaux et internationaux qui pourraient apporter une information pertinente afin d'évaluer la menace. Néanmoins, la loi rend le Roi compétent, sur proposition du Comité ministériel du renseignement et de la sécurité, pour déterminer les axes prioritaires des missions de l'OCAM. Ces axes prioritaires viennent apporter une précision sur ce qui doit être exactement considéré comme une menace terroriste ou extrémiste et faire l'objet d'une évaluation par l'OCAM. Il y a quatre axes prioritaires, définis par l'arrêté royal du 28 novembre 2006.

- Le premier axe considère que la menace terroriste ou extrémiste doit faire l'objet d'une évaluation par l'OCAM lorsque cette menace est dirigée vers l'intégrité d'une personne physique en Belgique ou d'un ressortissant belge à l'étranger.
- Le deuxième axe requiert une analyse de l'OCAM si la menace vise « *une infrastructure critique nationale* »<sup>122</sup>. En d'autres termes, si la menace terroriste ou extrémiste vise un bâtiment ayant une importance sociale ou économique, qu'il s'agisse d'un bâtiment essentiel à l'ordre public ou à l'Etat, ou d'un bâtiment qui abrite des substances dont la destruction pourrait avoir des conséquences graves, l'OCAM se doit de l'évaluer.
- Le troisième axe porte sur l'évaluation de la menace potentielle envers un événement ou un groupement d'individus.
- Le quatrième et dernier axe demande à l'OCAM d'évaluer la menace qui pèse sur les institutions et les intérêts belges à l'étranger.<sup>123</sup>

En parallèle, l'OCAM dispose de sa propre base de données. Celle-ci regroupe les informations sur une menace extrémiste ou terroriste pouvant émaner d'une personne,

---

<sup>120</sup> Ibidem. Article 8 & 10.

<sup>121</sup> Ibidem Article 8, 3°.

<sup>122</sup> Arrêté royal portant sur l'exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace du 28 novembre 2006, article 2, 2°.

<sup>123</sup> Ibidem. Article 2.

d'un groupe, ou d'un objet. Son accès est exclusivement réservé aux membres de l'OCAM.<sup>124</sup>

En conclusion, l'OCAM produit deux sortes d'évaluations de la menace terroriste et extrémiste. La première est stratégique et régulière. Il s'agit du niveau de la menace présent sur le territoire national, qui est relayé par les médias. L'objectif de cette évaluation est d'informer le monde politique d'un phénomène, à moyen ou long terme, pouvant affecter la sécurité afin qu'il puisse prendre des décisions politiques justes et appropriées à temps<sup>125</sup>. La seconde est d'ordre ponctuel et analyse une menace pesant sur ou émanant d'un lieu, d'une infrastructure ou d'un groupe d'individus. Cette évaluation a pour vocation d'être utilisée par les services judiciaires et opérationnels afin de contrer la menace.

## II.4. Le Comité permanent R

La mise en place en 1991 du Comité R, en charge du contrôle des services de renseignement apparaît avant même la loi organique de 1998 instituant ces services, leurs missions et leurs méthodes. Certains y verront un paradoxe en se demandant ce que le Comité R vérifiait, puisqu'il n'y avait aucun cadre légal imposé aux services de renseignement, d'autres diront qu'il avait d'autant plus son utilité afin de s'assurer de l'intérêt démocratique de ces services. Heureusement, cette ambiguïté est dissoute depuis lors. Néanmoins, il est intéressant de s'intéresser aux motivations qui ont mené le législateur à instaurer ce comité permanent. Dans son article, David Stans propose cinq raisons à cette démarche. Une raison est la possible implication des services de renseignement dans des « affaires », comme l'affaire *Westland Nieuw post*, qui a donné lieu à différentes enquêtes parlementaires. Une autre raison est la concomitance chronologique avec l'apparition du comité de contrôle des services de police, le Comité P, qui est institué par la même loi. En d'autres termes, le législateur aurait saisi l'occasion de faire d'une pierre deux coup afin de s'approprier un droit de regard sur des institutions de la force publique, dirigées par le pouvoir exécutif. Une troisième raison porte sur la nécessité de stabilité et de continuité dans le contrôle de ces organes. En effet, les

---

<sup>124</sup> Ibidem. Article 4 & 6.

<sup>125</sup> Van Laethem, Wauter. « L'organe de coordination pour l'analyse de la menace : une analyse ponctuelle ». op. cit. p. 114.

commissions d'enquêtes parlementaires variant au gré des élections ne permettaient pas un suivi s'inscrivant dans la durée, ce qui en réduisait l'efficacité. La dernière hypothèse serait que l'inauguration du Comité R traduit une réelle volonté du pouvoir législatif de surveiller les agissements du pouvoir exécutif. Enfin, la cinquième raison est de réduire l'opacité qu'entretenaient les services de renseignement à l'égard des assemblées législatives. Ces raisons informent sur la nature du Comité R et aident à décrypter le raisonnement de son organisation et de ses missions.<sup>126</sup>

#### *II.4.1. L'organisation*

En accord avec la loi, le Comité permanent R est constitué de trois membres, dont un président, ayant chacun deux suppléants. Tout d'abord, tous sont nommés par la Chambre des Représentants et tous peuvent être révoqués par celle-ci. Ensuite, la loi insiste sur le fait que les membres du Comité R « *ne peuvent exercer d'emploi ou d'activité public ou privé qui pourrait mettre en péril l'indépendance ou la dignité de la fonction* »<sup>127</sup>, c'est-à-dire que les membres ne peuvent pas exercer un mandat politique, par exemple. Enfin, il est intéressant de noter que la loi exige que le président du Comité R ait la qualité de magistrat. Les membres et leurs suppléants sont nommés pour un mandat de six ans renouvelables.<sup>128</sup>

A ces trois membres principaux, et leurs suppléants, il faut ajouter un greffier, lui aussi nommé par la Chambre et un service d'enquête, appelé Service d'enquêtes R. Ce dernier est dirigé par un chef qui doit avoir été magistrat, membre d'un service de renseignement ou de police, ou avoir une expérience d'au moins cinq ans en rapport avec les services de renseignements ou de police. Il est nommé pour cinq ans et révoqué, si besoin, par le Comité R, tout comme les autres membres du Service d'enquêtes R, puisque celui-ci est placé sous l'autorité du Comité R. Néanmoins, si les membres du Service d'enquêtes du Comité R (*voir infra*) remplissent une mission de police judiciaire, ils sont placés sous l'autorité d'un procureur. Il est intéressant de noter que la loi requiert que la moitié du Service d'enquêtes R, au minimum, soit composé de personnes détachées des services de renseignement, de police, ou d'une administration en lien avec ces services. Enfin, le

---

<sup>126</sup> Stans, David. « Le contrôle des services de renseignements belges : émergence d'une légitimité ». Revue de la Faculté de Droit de l'Université de Liège, 2010. pp. 373-384.

<sup>127</sup> Loi organique du contrôle des services de Police et de renseignement et de l'Organe de coordination de la menace du 18 juillet 1991, article 28, §2, 6°.

<sup>128</sup> Ibidem. Article 28.

personnel de ce Service d'enquête revêt la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi, et d'auditeur militaire.<sup>129</sup>

#### *II.4.2. Les missions*

Le premier article de la loi du 18 juillet 1991 indique trois objectifs centraux au Comité P et au Comité R. Le premier objectif est de s'assurer de la « *la protection des droits que la Constitution et la loi confèrent aux personnes* »<sup>130</sup> et de l'efficacité et de la coordination entre les services de renseignement. Le deuxième est de contrôler l'efficacité et la coordination de l'OCAM. Le troisième objectif est de contrôler les procédures de coordination qui existent entre l'OCAM et les autres services publics, appelés les « services d'appuis » dans la loi OCAM de 2006. D'ailleurs, le contrôle de l'OCAM est assuré par les Comités R et P, alors que le contrôle des services de renseignement relève uniquement de la compétence du Comité R.<sup>131</sup>

Plus précisément, le Comité R contrôle les activités et les méthodes employées par les services de renseignement de l'OCAM et des autres services d'appuis, ainsi que les règlements et directives internes propres à ces services. L'action du Comité R peut être entreprise à sa propre initiative, à la demande de la Chambre des représentants, des ministres de la Justice et de la Défense, par le dirigeant de l'OCAM, (qui, pour rappel, revêt la qualité de magistrat) ou encore, à la suite d'une plainte ou d'une dénonciation.<sup>132</sup>

Le Comité R joue aussi un rôle de relais entre les services de renseignement et le monde politique. En effet, après chaque enquête, le Comité R doit rédiger un rapport dont les « *conclusions [...] portent sur les textes, les activités ou les méthodes qui seraient de nature à mettre en péril les objectifs visés à l'article 1<sup>er</sup>* »<sup>133</sup>. Ensuite, ce rapport est transmis à la Chambre et aux ministres de la Justice et de la Défense. En outre, il existe deux autres cas où le Comité R rédige un rapport à destination de la Chambre. Le premier cas consiste en l'obligation du Comité R de rédiger un rapport d'activités annuel qui doit porter un regard particulier sur les utilisations des méthodes spécifiques et exceptionnelles de recueil de données. Le second cas permet au Comité R de transmettre un nouveau rapport s'il observe qu'aucune suite n'a été donnée à ses conclusions ou que les mesures prises à la suite de celles-ci sont inadéquates. Enfin, le Comité R peut rendre

---

<sup>129</sup> Ibidem. Article 35, 39, 41, 44 & 45.

<sup>130</sup> Ibidem. Article 1, 1<sup>o</sup>.

<sup>131</sup> Ibidem. Article 1 & 33, §3.

<sup>132</sup> Ibidem. Article 32, 33 & 34.

<sup>133</sup> Ibidem. Article 34, §3, premier alinéa.

un avis sur un texte législatif à la suite d'une demande de la Chambre, du ministre de la Justice ou de la Défense.<sup>134</sup>

\*\*\*

La doctrine apporte un éclairage intéressant à l'analyse de la loi organique du Comité R. Elle insiste sur le fait que si le législateur a confié au Comité R la mission de s'assurer de l'efficacité et de la coordination entre les services de renseignement, c'est pour lui permettre d'endosser le rôle de relais entre les services et le pouvoir législatif<sup>135</sup>. Ainsi, le Comité R est le porte-parole des services de renseignement auprès des assemblées législatives, afin que ceux-ci puissent acquérir des capacités utiles à la réalisation de leurs missions de façon démocratique et surveillée.

Le Comité R est aussi l'organe de contrôle législatif, mais le législateur s'est gardé de cloisonner ce contrôle<sup>136</sup>. Par exemple, le service d'enquête du Comité R tombe sous l'autorité du pouvoir judiciaire en cas d'intervention de celui-ci<sup>137</sup>, tandis que le pouvoir exécutif a la capacité d'ordonner une enquête par ce même comité<sup>138</sup>. Dès lors, le pouvoir législatif n'a pas le strict monopole de l'utilisation du Comité R, bien qu'il soit nettement plus impliqué que les deux autres pouvoirs traditionnels dans son organisation et en raison de l'automaticité des comptes-rendus que doit lui fournir le Comité R lors d'une enquête<sup>139</sup>.

Finalement, si le Comité R est un outil du contrôle législatif inscrit dans la durée, il n'empêche pas l'intervention immédiate du pouvoir législatif à l'égard des services de renseignement à l'aide d'une commission d'enquête<sup>140</sup>.

---

<sup>134</sup> Ibidem. Article 33 & 35.

<sup>135</sup> Stans, David. « Le contrôle des services de renseignements belges : émergence d'une légitimité ». op. cit. p. 377.

<sup>136</sup> Ibidem. p. 381.

<sup>137</sup> Ibidem. p. 380.

<sup>138</sup> Loi organique du contrôle des services de Police et de renseignement et de l'Organe de coordination de la menace du 18 juillet 1991, article 32, §1<sup>er</sup>.

<sup>139</sup> Ibidem. Article 32, §2.

<sup>140</sup> Stans, David. « Le contrôle des services de renseignements belges : émergence d'une légitimité ». op. cit. p. 383.

## II.5. Les différents conseils et comité liés au renseignement

Ici, sera présenté le Conseil national de sécurité, le Comité stratégique et le Comité de coordination. Ceux-ci représentent les liens qui unissent le monde du renseignement opérationnel au monde politique. Dès lors, il est essentiel de connaître leurs rôles et leurs compositions.

### *II.5.1. Le Conseil national de Sécurité (CNS)*

Le Conseil national de sécurité a été créé par l'Arrêté royal du 28 janvier 2015. Il s'agit d'un Conseil gouvernemental réunissant les ministres de la Justice, de la Défense nationale, de l'Intérieur et des Affaires étrangères ainsi que les Vice-Premiers Ministres qui n'ont pas ces matières dans leurs compétences et il est présidé par le Premier ministre. S'il le faut, d'autres membres du gouvernement peuvent y être invités, tout comme le dirigeant de la Sûreté, du SGRS, de l'OCAM, le commissaire général de la Police fédérale, le président du Comité de direction du Service public fédéral Intérieur, un représentant du Collège des procureurs généraux et le procureur fédéral si l'ordre du jour le requiert.<sup>141</sup>

L'objectif du Conseil national de Sécurité est triple<sup>142</sup>. Tout d'abord, il doit « [établir] *la politique générale du renseignement et de la sécurité, en [assurer] la coordination, et [déterminer] les priorités des services de renseignement et de la sécurité* »<sup>143</sup>. Ensuite, le CNS assure aussi la coordination de la lutte contre le financement du terrorisme et la prolifération des armes de destruction massive. Enfin, c'est à lui que revient d'établir la politique de protection des informations sensibles. Le CNS se réunit sur la convocation du Premier ministre et c'est lui qui fixe l'ordre du jour de la réunion<sup>144</sup>. La place prépondérante du Premier ministre traduit qu'il s'agit de l'échelon le plus élevé en matière de coordination entre le monde politique et celui du renseignement et de l'élaboration des politiques de sécurité.

### *II.5.2. Le Comité stratégique de renseignement et de la sécurité*

Le Comité stratégique est dirigé par un représentant du Premier ministre. Il est le deuxième échelon de la rencontre entre le renseignement et le monde politique. Il est

---

<sup>141</sup> Arrêté royal portant création du Conseil national de sécurité du 28 janvier 2015, article 1 & 2.

<sup>142</sup> Ibidem. Article 3.

<sup>143</sup> Idem.

<sup>144</sup> Ibidem. Article 4.

constitué des représentants des ministres membres du CNS et du président du Comité de coordination du renseignement et de la sécurité (*voir infra*).<sup>145</sup>

Ce comité est chargé de deux missions. La première consiste en l'examen des propositions que le CNS rédige et de celles soumises par le Comité de coordination du renseignement et de la sécurité au CNS. La seconde mission de ce Comité stratégique est de contrôler l'exécution des décisions du CNS. En d'autres termes, le Comité stratégique est réellement le point de contact entre le monde du renseignement belge, représenté par le Comité de coordination, et le monde politique de la sécurité qu'est le CNS.<sup>146</sup>

#### *II.5.3. Le Comité de coordination du renseignement et de la sécurité*

Le Comité de coordination est composé de manière permanente par les dirigeants du SGRS, de la Sûreté, de l'OCAM, du Centre de crise, du commissaire général de la Police fédérale, du procureur fédéral et d'un membre du Collège des procureurs généraux. Le président est désigné par le Conseil des ministres et est un des membres permanents. Il est aussi composé de membres non-permanents qui sont : « *l'administrateur général de l'Administration générale des Douanes et Accises du Service public fédéral Finances, le directeur du Centre pour la Cybersécurité Belgique, le président de la Cellule de traitement des informations financières, le directeur général de la Direction générale Transport aérien du Service public fédéral Mobilité et Transports, le directeur général de la Direction générale Transport maritime du Service public fédéral Mobilité et Transports, le président de l'Autorité nationale de Sécurité* »<sup>147</sup>. Ces derniers ne participent à la réunion que si un dossier les concerne particulièrement.<sup>148</sup>

Le Comité de coordination est chargé de quatre missions :

- « *soumettre au Conseil national de sécurité, via le Comité stratégique, des propositions coordonnées concernant la politique générale du renseignement et de la sécurité, sa coordination et les priorités des services de renseignement et de la sécurité, la coordination de la lutte contre le financement du terrorisme et de la prolifération des armes de destruction massive et la politique en matière de protection des informations sensibles;*

---

<sup>145</sup> Arrêté royal portant création du Comité stratégique et du Comité de coordination du renseignement et de la sécurité du 2 juin 2015, article 2.

<sup>146</sup> Ibidem. Article 3.

<sup>147</sup> Ibidem. Article 8, §2.

<sup>148</sup> Ibidem. Article 8.

- *développer les plans d'action pour chaque priorité établie par le Conseil national de sécurité et les suivre ou proposer de nouvelles priorités;*
- *promouvoir la collaboration efficace et l'échange d'information entre les services de renseignement et de la sécurité;*
- *garantir l'exécution coordonnée des décisions du Conseil national de sécurité »<sup>149</sup>.*

En définitive, ce Comité rassemble tous les dirigeants des services qui sont de près ou de loin impliqués dans le renseignement et la sécurité.

## II.6. Le monde du renseignement belge

En reprenant les compositions, permanentes et non-permanentes du Comité de coordination du renseignement et de la sécurité, il est possible d'ajouter quelques acteurs, et d'apprécier leur importance au sein de ce cercle fermé qu'est la communauté d'agences définie par ce mémoire. De plus, une typologie très intéressante est faite entre des « services de base » et des « services partenaires » dans l'arrêté royal relatif à la banque de données commune « *foreign terrorist fighters* » (FTF)<sup>150</sup>. Cette différenciation se rapporte à l'article 44/11/3ter de la loi sur la fonction de police de 1992. En effet, cet article différencie, d'une part, les services ayant un accès direct aux « *banques de données communes* », sous-entendu celles de la police, et d'autres part, les services qui peuvent les interroger de manière indirecte<sup>151</sup>. L'accès privilégié de certains services par rapport à d'autres et les dénominations du législateur telles que « services de base » et « services partenaires » traduisent aussi l'intensité du rôle joué par ces services dans la communauté du renseignement.

Le tableau suivant démontre combien il est complexe d'établir la communauté d'agence du renseignement (voir *figure III*). Tout d'abord, il apparaît que le renseignement belge ne s'arrête pas aux frontières des deux services de renseignement, le SGRS et la Sûreté de l'Etat. Ensuite, ce tableau met en évidence certains acteurs qui se démarquent nettement. Ainsi, les deux services de renseignement, la police, et encore plus la police fédérale, et l'OCAM semblent jouer un rôle prédominant à l'égard du renseignement belge. En effet, ces acteurs sont considérés comme des « services de bases », ils

---

<sup>149</sup> Ibidem. Article 9.

<sup>150</sup> Arrêté royal relatif à la banque de données commune « *foreign terrorist fighters* » du 21 juillet 2016. Article 1<sup>er</sup>, §1<sup>er</sup>, 7<sup>o</sup> & 8<sup>o</sup>.

<sup>151</sup> Loi sur la fonction de police du 5 août 1992. Article 44/11/3ter, §1<sup>er</sup>, 2§.

constituent les sièges permanents du Comité de coordination du renseignement et de la sécurité et peuvent aussi participer aux décisions politiques auprès des plus hautes strates de l'Etat lors des Conseils nationaux de sécurité. Enfin, relevons la présence répétée de certains acteurs qui semblent proches du monde du renseignement. C'est le cas du Centre de crise, du SPF Affaires étrangères, du procureur fédéral, du service des douanes, de la Cellule de traitement des informations financières (CTIF). Pour terminer, il est aussi intéressant de noter la présence de l'Office des étrangers, des établissements pénitentiaires, du Centre pour la Cybersécurité et des directions générales du SPF « Mobilités et transports ».

*Figure III : Entités représentées, de manière permanente ou non permanente, au Comité de coordination du renseignement et de la sécurité ou ayant un accès, direct ou indirect, à la base de données « FTF »*

|                                              | <b>Loi sur la fonction de police<sup>152</sup> / Arrêté royal relatif à la banque de données « FTF »<sup>153</sup></b>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                               | <b>Composition du Comité de coordination du renseignement et de la sécurité<sup>154</sup></b>                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Services de base – accès direct</b>       | <ul style="list-style-type: none"> <li>- Sûreté de l'Etat</li> <li>- SGRS</li> <li>- OCAM</li> <li>- la police intégrée</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>Membres permanents</b>     | <ul style="list-style-type: none"> <li>- Sûreté de l'Etat</li> <li>- SGRS</li> <li>- OCAM</li> <li>- Police fédérale</li> <li>- Centre de crise</li> <li>- SPF Affaires étrangères</li> <li>- Collège des procureurs généraux</li> <li>- le procureur fédéral</li> </ul>                                                                                                                                                                       |
| <b>Services partenaires – accès indirect</b> | <ul style="list-style-type: none"> <li>- la Cellule de traitement des informations financières</li> <li>- l'Administration générale des Douanes et Accises du SPF Finances</li> <li>- la Commission permanente de la police locale</li> <li>- le Centre de crise</li> <li>- la Direction générale Sécurité et Prévention du SPF Intérieur</li> <li>- la Direction générale des Etablissements pénitentiaires</li> <li>- le SPF Affaires étrangères, Direction générale Affaires consulaires</li> <li>- le Ministère public</li> <li>- l'Office des Etrangers</li> </ul> | <b>Membres non-permanents</b> | <ul style="list-style-type: none"> <li>- la Cellule de traitement des informations financières</li> <li>- l'Administration générale des Douanes et Accises du SPF Finances</li> <li>- le Centre pour la Cybersécurité</li> <li>- la Direction générale Transport aérien du SPF Mobilité et Transports</li> <li>- la Direction générale Transport maritime du SPF Mobilité et Transports</li> <li>- l'Autorité nationale de Sécurité</li> </ul> |

<sup>152</sup> Loi sur la fonction de police du 5 août 1992. Article 44/11/3ter, §1<sup>er</sup>, 2§.

<sup>153</sup> Arrêté royal relatif à la banque de données commune « *foreign terrorist fighters* » du 21 juillet 2016. Article 1<sup>er</sup>, §1<sup>er</sup>, 7° & 8°.

<sup>154</sup> Arrêté royal portant création du Comité stratégique et du Comité de coordination du renseignement et de la sécurité du 2 juin 2015, article 8, §2.

## Chapitre III – Le cadre politico-juridique du recueil, de l'échange et de l'utilisation des données

### III.1. Les méthodes de recueil de données (MRD ou BIM)

Cette sous-section n'a pas pour ambition d'analyser et de commenter les méthodes de recueil de données et leur contrôle. Ce sujet ne rentre pas dans le cadre de l'échange et de l'utilisation de ces données. Il semble essentiel de connaître les procédés de récolte des services de renseignement belges avant d'étudier les procédés de dissémination de ces données. Ici, il sera donné un aperçu général des méthodes de recueil de données en omettant les exceptions concernant les procédures d'urgence et celles spécifiques lorsqu'il s'agit d'un médecin, d'un avocat ou d'un journaliste.

Les services de renseignement utilisent des méthodes afin de récolter des informations pour ensuite les traiter. Ces méthodes sont appelées « méthodes de recueil de données » et généralement abrégées MRD ou BIM (*Bijzondere inlichtingenmethoden*) dans les différentes publications. La loi organique des services de renseignement définit ces méthodes en trois catégories : ordinaire, spécifique et exceptionnelle. Attention, ces méthodes ne sont pas les seuls moyens qu'ont les services de renseignement pour acquérir des informations. Outre les échanges internationaux, les articles 44 et suivants de la loi organique des services de renseignement offre le droit au SGRS de mettre en place des capacités étendues de récolte d'informations à l'étranger. Alors que les MRD doivent se dérouler sur ou à partir du Royaume, les articles 44 et suivants sont des procédures qui ne peuvent être mises en place qu'à l'extérieur du pays. C'est pour cette raison que les capacités du SGRS à l'étranger ne seront pas développées dans ce mémoire.

#### *III.1.1. Les méthodes ordinaires de recueil de données*

Il existe sept différentes méthodes ordinaires. La condition sine qua non commune à toutes ces méthodes ordinaires est qu'elles doivent toutes se réaliser dans le cadre des missions assignées par la loi aux services de renseignement.<sup>155</sup>

Une technique permet aux services de renseignement belges de requérir une information détenue par un services public tiers, en ce compris les services de police. Les différents

---

<sup>155</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 14 à 18.

services publics peuvent s'y opposer, s'ils pensent que la transmission de l'information peut compromettre une affaire judiciaire ou l'intégrité physique d'une personne. De plus, les services de renseignement ont accès aux bases de données du secteur public.<sup>156</sup>

En deuxième lieu, la loi autorise les services de renseignement à collecter des données à caractère personnel avec le concours de personnes ou d'organisations du secteur privé.<sup>157</sup>

Une autre méthode ordinaire concerne l'observation et l'inspection des lieux publics et des objets qui s'y trouvent, si ces derniers ne sont ni verrouillés ni surveillés par le possesseur. L'observation des personnes dans les lieux publics est autorisée, mais pas leur inspection.<sup>158</sup>

Les services de renseignement peuvent pénétrer dans les lieux accessibles aux publics et visiter les établissements hôteliers dans le respect de l'inviolabilité du domicile. Ils sont autorisés à consulter les données d'inscriptions des voyageurs avec le concours du tenancier de l'établissement.<sup>159</sup>

Une cinquième méthode autorise les deux services à récolter des informations à l'aide de sources humaines, appelées communément « informateurs »<sup>160</sup>.

L'identification d'un utilisateur d'un service de communication électronique ou l'identification d'un service de communication électronique employé par une personne déterminée constitue la sixième méthode ordinaire. De plus, les services de renseignement peuvent requérir le concours d'une institution financière pour identifier l'acheteur d'une carte prépayée.<sup>161</sup>

La dernière méthode ordinaire concerne l'accès « *aux données des passagers visées à l'article 27 de la loi du 25 décembre 2016 relative au traitement des données des passagers* »<sup>162</sup>.

---

<sup>156</sup> Ibidem. Article 14.

<sup>157</sup> Ibidem. Article 15.

<sup>158</sup> Ibidem. Article 16/1.

<sup>159</sup> Ibidem. Article 17.

<sup>160</sup> Ibidem. Article 18.

<sup>161</sup> Ibidem. Article 16/2.

<sup>162</sup> Ibidem. Article 16/3, §1.

### *III.1.2. Les méthodes spécifiques de recueil de données*

La loi présente cinq méthodes spécifiques de recueil de données.

La première méthode concerne l'observation. Dans ce cadre, il est possible pour un service de renseignement d'observer à l'aide d'un moyen technique un lieu public, les personnes s'y trouvant et les événements s'y déroulant. De plus, cette méthode permet d'observer, à l'aide d'un moyen technique ou non, un lieu non accessible au public qui n'est pas soustrait à la vue, sans y pénétrer. Cela contraste avec les méthodes ordinaires puisque l'utilisation d'un moyen technique y est proscrite.<sup>163</sup>

Une des méthodes spécifiques est l'inspection des lieux publics et des objets verrouillés s'y trouvant, à l'aide d'un moyen technique<sup>164</sup>.

L'identification et la prise de connaissance des données d'un utilisateur d'une boîte postale, d'un destinataire ou de l'expéditeur d'un courrier constitue la troisième méthode. Cette compétence est étendue aux données concernant les utilisateurs d'un service postal privé<sup>165</sup>.

Les services de renseignement peuvent identifier ou localiser l'utilisateur d'un moyen de communication électronique à l'aide d'un moyen technique. De plus, l'article 18/7 permet aux services de renseignement de requérir les informations concernant le moyen de paiement d'un utilisateur auprès d'un fournisseur d'un service de communication.<sup>166</sup>

Il est intrigant de remarquer qu'ici, l'information récoltée par les services de renseignement peut être totalement la même qu'en utilisant une méthode ordinaire. En effet, la septième méthode ordinaire, présentée précédemment, permet aux services de renseignement de requérir l'identification d'un utilisateur d'un service de communication avec le concours du fournisseur. Ici, bien que l'information finale soit la même, le moyen technique utilisé pour l'obtenir implique sa catégorisation parmi les méthodes spécifiques qui sont soumises à un contrôle plus important. Cette comparaison démontre que la loi sur les MRD restreint la capacité des services de renseignement selon leurs moyens et non par rapport à la nature, plus ou moins, personnelle de la donnée acquise par le service de renseignement.

---

<sup>163</sup> Ibidem. Article 18/4.

<sup>164</sup> Ibidem. Article 18/5.

<sup>165</sup> Ibidem. Article 18/6 & 18/6/1.

<sup>166</sup> Ibidem. Article 18/7.

La dernière méthode spécifique concerne la possibilité des services de renseignement de « [repérer] *des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées* »<sup>167</sup> et de « [localiser] *l'origine ou la destination de communications électroniques* »<sup>168</sup> et ce, avec ou sans l'aide du fournisseur du service de communication. Un dernier élément de l'article 18/8 est qu'il émet des restrictions par rapport à la période de temps sur laquelle les informations peuvent être récoltées selon le type de menace. Ainsi, si la menace concerne une organisation criminelle, les données concernant le trafic des moyens de communication électronique ne pourront être récoltées que sur une période de six mois précédant la date de réquisition, alors qu'il s'agira d'une période de 12 mois en cas de menace terroriste, par exemple. Cet élément met à jour que la loi différencie la capacité d'action des services de renseignement selon le type menace.<sup>169</sup>

### *III.1.3. Les méthodes exceptionnelles de recueil de données*

La loi comporte sept méthodes exceptionnelles de recueil de données.

La première concerne l'observation. Les services de renseignements sont habilités à pouvoir observer, à l'aide de moyens techniques ou non, des lieux non accessibles au public qui sont soustraits à la vue sans l'accord du propriétaire. Pour ce faire, ils peuvent y pénétrer afin d'y installer un moyen technique.<sup>170</sup>

La deuxième méthode exceptionnelle est celle de l'inspection. Dans ce cas, ils peuvent inspecter, à l'aide de moyens techniques ou non, des lieux non accessibles au public et les objets verrouillés s'y trouvant, sans l'accord du propriétaire.<sup>171</sup>

Les services de renseignements peuvent avoir recours à une personne morale fictive afin de recueillir des informations. Cette méthode n'est pas limitée dans le temps, néanmoins, un contrôle bimensuel de son utilité est effectué.<sup>172</sup>

La prise de connaissance du contenu d'un courrier postal par les services de renseignement constitue la quatrième méthode exceptionnelle<sup>173</sup>.

---

<sup>167</sup> Ibidem. Article 18/8, §1, premier alinéa.

<sup>168</sup> Ibidem. Article 18/8, §1, second alinéa.

<sup>169</sup> Ibidem. Article 18/8

<sup>170</sup> Ibidem. Article 18/11.

<sup>171</sup> Ibidem. Article 18/12.

<sup>172</sup> Ibidem. Article 18/13.

<sup>173</sup> Ibidem. Article 18/14, §1.

Les services de renseignement ont le droit de récolter des informations bancaires d'une personne déterminée<sup>174</sup>.

La loi permet aux services de renseignement d'infiltrer un système informatique afin d'y récolter des informations pertinentes. Il est intéressant de noter que le service de renseignement ne peut pas altérer ces informations et doit veiller à la non-dissémination de celles-ci. Ils peuvent aussi pénétrer dans des lieux non accessibles au public afin de mettre en place cette méthode exceptionnelle. Néanmoins, le SGRS possède des compétences élargies concernant l'intrusion des systèmes informatiques, puisqu'il peut, par exemple, le perturber.<sup>175</sup>

La septième méthode exceptionnelle autorise l'écoute et l'enregistrement de communications téléphoniques. Pour ce faire, les services de renseignement peuvent s'introduire dans des lieux non accessibles au public afin de placer un moyen technique. La loi prévoit que seuls les enregistrements utiles à la mission seront conservés.<sup>176</sup>

## III.2. Le contrôle des MRD

Il est utile de comprendre les organes et les principes que régissent le contrôle des méthodes de recueil de données. Il existe deux organes externes aux services de renseignement qui endossent la responsabilité du contrôle de ces méthodes : la Commission BIM et le Comité R. Après l'analyse de l'interaction entre la Commission BIM et le Comité R, les principes intrinsèques à ces contrôles seront présentés.

### *III.2.1. Le contrôle des méthodes de recueil de données par la Commission BIM*

La commission qui contrôle les méthodes de recueil de données est appelée la commission BIM (*Bijzondere inlichtingenmethoden*). Elle est indépendante et composée de trois magistrats qui ont chacun un suppléant. Plus précisément, elle est composée de trois personnes ayant la qualité de magistrat du ministère public, de juge ou de juge d'instruction. Les suppléants ont la même qualité de magistrat que la personne qu'ils remplacent. Lorsqu'ils doivent prendre une décision, ils statuent à la majorité et la présidence de cette commission revient au magistrat ayant la qualité de juge d'instruction. Ces magistrats ne peuvent pas avoir été membre du Comité P, du Comité R, d'un service

---

<sup>174</sup> Ibidem. Article 18/15.

<sup>175</sup> Ibidem. Articles 18/16 & 44/1.

<sup>176</sup> Ibidem. Article 18/17.

de police ou de renseignement au cours des cinq années précédant leur nomination. Ils sont nommés pour cinq ans et ce mandat est renouvelable deux fois. Les six magistrats de la Commission BIM sont nommés, ou démis en cas de faute grave, par arrêté décidé en conseil des ministres sur la proposition du ministre de la Défense ou de la Justice. Cette commission est assistée par un secrétariat composé de membres des services de renseignement. Celle-ci ne vérifie que les méthodes spécifiques et exceptionnelles au préalable ou en cours.<sup>177</sup>

Dans le cas des méthodes spécifiques, la commission BIM assure un contrôle « *à tout moment* »<sup>178</sup>. En d'autres termes, le chef du service de renseignement n'a pas besoin de l'accord de la commission BIM pour démarrer une méthode spécifique, mais il doit l'en avertir de sa mise en place par écrit. Celle-ci peut en vérifier la légalité, quand bon lui semble, et mettre fin à cette méthode, si elle ne l'estime pas légale.<sup>179</sup>

En ce qui concerne les méthodes exceptionnelles, la commission BIM exerce un contrôle *a priori* en délivrant une autorisation pour leurs mises en place au service, qui en a fait la demande.<sup>180</sup>

Si la commission BIM constate une irrégularité ou que la menace, qui justifiait l'élaboration d'une méthode, ne répond plus aux principes de subsidiarité et de proportionnalité, elle suspend et interdit l'exploitation des données recueillies et notifie sa décision au Comité R<sup>181</sup>.

### *III.2.2. Le contrôle des MRD par le Comité R*

Le Comité R est compétent pour le contrôle de toutes les méthodes, qu'elles soient en cours ou clôturées<sup>182</sup>. Il peut démarrer une procédure de contrôle de sa propre initiative, après une plainte ou de plein droit, si une telle méthode a été autorisée par un ministre compétent ou suspendue par la commission BIM<sup>183</sup>. Si une méthode est suspendue par la Commission BIM, c'est le Comité R qui statuera sur la légalité ou l'irrégularité de la méthode en définitive<sup>184</sup>. De cette façon, il assure un contrôle permanent et aucun recours

---

<sup>177</sup> Ibidem. Article 43/1.

<sup>178</sup> Ibidem. Article 18/3, §6.

<sup>179</sup> Ibidem. Article 18/3.

<sup>180</sup> Ibidem. Article 18/10.

<sup>181</sup> Ibidem. Article 18/3, §6.

<sup>182</sup> Rapaille, Guy, Van Laethem Wauter. « La nouvelle loi sur les méthodes particulières de renseignement : une révolution pour les services de renseignement belges ». *Revue de droit pénal et de criminologie* 91, no. 9, 2011. p. 827.

<sup>183</sup> Ibidem. p. 827.

<sup>184</sup> Ibidem. p. 826.

n'est possible à la suite de sa décision<sup>185</sup>. Il peut mettre fin à ces méthodes, interdire l'exploitation des données recueillies irrégulièrement et ordonner leur destruction<sup>186</sup>. En d'autres termes, la Commission BIM opère un premier filtre et le Comité R un second tout en assumant un rôle hiérarchiquement plus élevé puisqu'il statue définitivement par rapport à la Commission BIM.

### *III.2.3. Les principes régissant l'autorisation et le contrôle des MRD*

La mise en œuvre et le contrôle des différentes méthodes sont marqués par plusieurs principes et par certaines limites.

#### *Principes de légalité, de finalité, de proportionnalité et de subsidiarité*

La loi impose le respect des principes de finalité, de légalité<sup>187</sup>, de proportionnalité et de subsidiarité. Ainsi, la loi met l'accent sur la légalité puisque l'article 12 ne permet aux services de renseignement d'agir que par des procédés inscrits dans cette loi : « *Pour accomplir leurs missions, les services de renseignement et de sécurité ne peuvent utiliser des moyens de contrainte que dans les conditions prévues par la loi* »<sup>188</sup>. Ensuite, la loi ne cesse de répéter que les méthodes de recueil de données doivent se limiter à recueillir des données « *dans l'intérêt de l'exercice de leurs missions* » qui sont clairement décrites par cette même loi. Par ailleurs, elle insiste sur le fait que « *les méthodes de recueil des données des services de renseignement et de sécurité visées à la présente loi ne peuvent être utilisées dans le but de réduire ou d'entraver les droits et libertés individuels* »<sup>189</sup>. Ces deux obligations constituent le principe de finalité. Enfin, les principes de subsidiarité et de proportionnalité doivent être respectés en cas d'utilisation d'une méthode spécifique ou exceptionnelle de recueil de données. Le principe de subsidiarité permet l'utilisation des méthodes spécifiques que si les méthodes ordinaires se révèlent inefficaces pour l'objectif poursuivi. Si les moyens spécifiques ne suffisent toujours pas, alors les méthodes exceptionnelles pourront être mises en œuvre. Le principe de proportionnalité induit que le degré d'intrusion de la méthode utilisée doit être justifié par la nature ou la certitude de la menace. L'appréciation de ces principes revient à la Commission BIM.<sup>190</sup>

---

<sup>185</sup> Ibidem. p. 826.

<sup>186</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 43/6, §6..

<sup>187</sup> Rapaille, Guy, Van Laethem Wauter. op. cit. p. 816.

<sup>188</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 12.

<sup>189</sup> Ibidem. Article 2, §1<sup>er</sup>.

<sup>190</sup> Ibidem. Articles 18/3, §1<sup>er</sup> & 18/9.

### Les limites de temps et de lieu.

Il est important de noter que la loi ne pose pas de limite de temps et lieu dans le cadre des méthodes ordinaires<sup>191</sup>. En ce qui concerne les méthodes spécifiques et exceptionnelles, la Sûreté ne peut qu'employer ces méthodes « *sur ou à partir du territoire du Royaume* »<sup>192</sup>, tandis qu'il n'y a pas de limites territoriales pour le SGRS. Auparavant, les méthodes spécifiques et exceptionnelles devaient être appliquées par les deux services uniquement sur le territoire du royaume. Ce changement est opéré par la loi du 30 mars 2017<sup>193</sup> qui répond aux considérations du Comité R<sup>194</sup>. D'un côté, ce changement autorise le SGRS à mettre en œuvre des méthodes à l'étranger. D'ailleurs, la loi sur les méthodes spécifiques et exceptionnelles de recueil de données ne s'applique pas à « *l'interception de communication émises ou reçues à l'étranger et de l'intrusion d'un système informatique situé à l'étranger et de la prise d'images fixes ou animées effectuée à l'étranger* »<sup>195</sup>. Cette exemption semble confirmer l'apport de Jacques Baud selon lequel les services de renseignement disposent d'une plus grande marge de manœuvre et de moins d'obligations lorsqu'il s'agit de récolter des données personnelles hors du territoire national<sup>196</sup>. D'un autre côté, il autorise aussi la Sûreté à acquérir des données situées à « l'étranger », tel qu'un mail appartenant à une personne établie dans un autre pays. En effet, la Sûreté est compétente pour s'introduire dans un système informatique. Dès lors, il est imaginable que cette action se fasse à partir de la Belgique tout en récoltant des informations se situant dans un système informatique situé dans un autre pays. Bien que la durée des méthodes spécifiques ne soit pas déterminée par la loi, il apparaît que le Comité R limite leur utilisation à 12 mois<sup>197</sup>. Quant à elles, les méthodes exceptionnelles sont clairement limitées à deux mois<sup>198</sup>.

---

<sup>191</sup> Rapaille, Guy, Wauter Van Laethem. op. Cit. p. 818.

<sup>192</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 18/1, premier alinéa.

<sup>193</sup> Loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité du 29 janvier 2016 et l'article 259bis du Code pénal, article 27.

<sup>194</sup> Comité R, « Rapport d'activité du Comité R 2016 ». op. cit. p. 172.

<sup>195</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 18/1, deuxième alinéa.

<sup>196</sup> Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». op. cit. p. 286.

<sup>197</sup> Rapaille, Guy, Wauter Van Laethem. op. cit. pp. 825-826.

<sup>198</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 18/10, §1<sup>er</sup>, deuxième alinéa.

### Un contrôle corrélé au degré d'intrusion

Chaque méthode est soumise à des contrôles corrélés à leur caractère intrusif : moins stricts pour les méthodes ordinaires, plus stricts pour les méthodes exceptionnelles. Les méthodes ordinaires sont soumises au seul contrôle du Comité R<sup>199</sup>. Pour les deux méthodes les plus intrusives, à savoir la spécifique et l'exceptionnelle, les contrôles sont triples : le contrôle du chef de service, le contrôle de la Commission BIM, et le contrôle du Comité R<sup>200</sup>. Ainsi, pour les méthodes spécifiques, le dirigeant du service de renseignement est responsable du contrôle interne. Celui-ci doit mettre fin à de telles méthodes quand il constate la fin de la menace potentielle qui justifiait ces méthodes ou lorsqu'il constate une irrégularité<sup>201</sup>. L'un des contrôles externes est assuré par la commission BIM qui peut contrôler la légalité de telles mesures, lorsqu'elles sont en cours. En plus d'être soumis à ces mêmes contrôles, les méthodes exceptionnelles doivent être préalablement autorisés par la Commission BIM<sup>202</sup>. L'autre contrôle externe est opéré par le Comité R qui vérifie toutes les méthodes qu'elles soient en cours ou clôturées.

Ces méthodes permettent aux services de renseignement belges d'acquérir des informations sensibles. Pour accomplir leurs missions, protéger leurs sources et leurs techniques il est important de développer une culture du secret.

### III.3. La protection du secret

Le secret, la confidentialité et la discrétion sont des caractères intrinsèques aux services de renseignement. En effet, ces services qui protègent la stabilité de l'Etat ont entre leurs mains des informations parfois vitales. Dès lors, tout doit être mis en œuvre pour que ces informations ne tombent pas dans de mauvaises mains. La classification, le besoin d'en connaître (need-to-know) et la règle du tiers service sont trois principes élémentaires qui marquent le fonctionnement des services de renseignement. Ces principes ont pour objectif de restreindre au maximum les détenteurs des informations sensibles, de protéger les sources et les méthodes des services, et d'éviter qu'une information soit divulguée à un mauvais client<sup>203</sup>. Néanmoins, ces protections sont aussi la cause de certains

---

<sup>199</sup> Rapaille, Guy, Wauter Van Laethem. op. cit. p. 818.

<sup>200</sup> Ibidem. p. 826.

<sup>201</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 18/3, §8.

<sup>202</sup> Ibidem. Article 18/10, §1.

<sup>203</sup> Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». Perrin, 2018. p. 565

dysfonctionnements des services de renseignement et ceux-ci ouvrent la voie à de nouveaux concepts, comme celui du « need-to-share ».<sup>204</sup>

### *III.3.1. La classification et l'habilitation*

Pour protéger ses secrets et désigner ceux qui peuvent les détenir, les Etats mettent en place un système de classification des documents<sup>205</sup> et d'habilitation des personnes. En Belgique, la loi du 11 décembre 1998, relative à la classification et aux habilitations, attestations et avis de sécurité, institue ce système de protection des documents sensibles de l'Etat<sup>206</sup>.

D'un côté, les documents qui ne peuvent pas être rendus public se voient apposer le qualificatif « confidentiel », « secret » ou « très secret »<sup>207</sup>. Il s'agit d'un degré de protection<sup>208</sup> qui peut non seulement s'appliquer à un document, mais aussi à toutes informations, données ou tout autre élément matériel *« dont l'utilisation inappropriée peut porter atteinte à l'un des intérêts suivants :*

- *la défense de l'intégrité du territoire national et des plans de défense militaire ;*
- *l'accomplissement des missions des forces armées ;*
- *la sûreté intérieure de l'Etat, y compris dans le domaine de l'énergie nucléaire, et la pérennité de l'ordre démocratique et constitutionnel ;*
- *la sûreté extérieure de l'Etat et les relations internationales de la Belgique ;*
- *le potentiel scientifique et économique du pays ;*
- *tout autre intérêt fondamental de l'Etat ;*
- *la sécurité des ressortissants belges à l'étranger ;*
- *le fonctionnement des organes décisionnels de l'Etat.*
- *la sécurité des personnes auxquelles en vertu de l'article 104, § 2 du Code d'instruction criminelle, des mesures de protection spéciales sont octroyées »*<sup>209</sup>.

---

<sup>204</sup> Ibidem.

<sup>205</sup> Ibidem. p. 151.

<sup>206</sup> Loi relative à la classification et aux habilitations, attestations et avis de sécurité du 11 décembre 1998.

<sup>207</sup> Ibidem. Article 4.

<sup>208</sup> Ibidem. Article 2

<sup>209</sup> Ibidem. Article 3, §1<sup>er</sup>.

Le degré de classification dépend de son contenu<sup>210</sup> et c'est le Roi qui détermine qui est habilité à attribuer un degré de classification<sup>211</sup>. De plus, il est intéressant de noter que dans le cadre d'échanges bilatéraux et multilatéraux, les Etats ont développé un système d'équivalence des classifications afin d'assurer la protection de l'information échangée<sup>212</sup>.

D'un autre côté, il existe les habilitations de sécurité qui sont, elles, destinées aux personnes. Cette habilitation détermine le degré de classification auquel une personne peut avoir accès<sup>213</sup>.

Ce système de classification des documents et d'habilitations a pour objectif de restreindre l'accès aux informations sensibles de l'Etat à des personnes dont la loyauté a été vérifiée.

### *III.3.2. Le besoin d'en connaître (need-to-know)*

Le besoin d'en connaître se base sur le principe que « *nul ne prend connaissance d'une information dont il n'a pas l'utilité* »<sup>214</sup>. De cette façon, les services de renseignement cloisonnent leurs opérations en différents domaines d'activités afin que si l'un d'entre eux est contaminé par de fausses informations, ou si des informations venaient à fuiter, seul un de ces domaines serait impacté et le reste de l'opération « sauvé ». En termes pratiques, cela veut dire qu'une personne détenant une habilitation de sécurité peut se voir refuser l'accès à une information si elle n'en a pas besoin afin d'accomplir sa mission.<sup>215</sup>

En Belgique, la loi relative à la classification et aux habilitations fait référence très clairement au besoin d'en connaître puisque l'article huit stipule que « *Nul n'est admis à avoir accès aux informations, documents ou données, au matériel, aux matériaux ou matières classifiés s'il n'est pas titulaire d'une habilitation de sécurité correspondante et s'il n'a pas besoin d'en connaître et d'y avoir accès pour l'exercice de sa fonction ou de*

---

<sup>210</sup> Ibidem. Article 5.

<sup>211</sup> Ibidem. Article 7.

<sup>212</sup> Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». Perrin, 2018. p. 103.

<sup>213</sup> Loi relative à la classification et aux habilitations, attestations et avis de sécurité du 11 décembre 1998. Article 9.

<sup>214</sup> Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». op. cit. p. 100.

<sup>215</sup> Ibidem.

*sa mission* [...] »<sup>216</sup>. Dès lors, ces deux exigences doivent être remplies pour qu'une personne ait accès à un secret d'Etat<sup>217</sup>.

Si le besoin d'en connaître est une nécessité afin de protéger les informations sensibles, certains n'hésitent pas à dire que c'est un principe qui permet de couvrir certaines activités illégales, d'empêcher un contrôle démocratique efficace et un prétexte pour ne pas partager certaines informations<sup>218</sup>. Cette excuse n'est pas valable en Belgique puisque le Comité R a accès à tous les dossiers constitués par les services de renseignement et il peut demander à ceux-ci de fournir toute information utile à son contrôle<sup>219</sup>. Quant à la Commission d'enquête parlementaire, constituée suite aux attentats du 22 mars 2016, il a fallu établir un protocole encadrant l'accès aux données classifiées entre cette dernière, le Comité R et les services de renseignement puisque les membres de la Commission n'avaient pas d'habilitations de sécurité<sup>220</sup>.

### *III.3.3. La règle du tiers service (originator control)*

La règle du tiers service interdit à un service de renseignement de divulguer une information reçue par un autre service sans son autorisation. Tout comme le principe du besoin d'en connaître, la règle du tiers service restreint l'accès à l'information et, de ce fait, rend plus difficile l'échange d'information et le contrôle démocratique.<sup>221</sup>

Selon Bertrand Warusfel, la règle du tiers service implique le principe de la « propriété du renseignement ». En d'autres termes, l'information récoltée ou le renseignement élaboré par un service de renseignement lui appartient et c'est lui qui décide de sa dissémination même après un ou plusieurs partages avec d'autres services. Si un service ou un pays venait à enfreindre cette règle, la confiance que lui accorde le service ou le pays émetteur du renseignement ou de l'information, et les autres services, se verrait amoindrie. La confiance est un élément central de l'échange d'information entre les services. Si celle-ci est amoindrie ou rompue, cela impacte systématiquement la relation entre les deux services et entrave leur coopération. Enfin, l'établissement de cette règle implique deux éléments. Le premier est la préférence qu'ont les services de renseignement à échanger leurs informations dans des relations bilatérales plutôt que

---

<sup>216</sup> Loi relative à la classification et aux habilitations, attestations et avis de sécurité du 11 décembre 1998, article 8.

<sup>217</sup> Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». op. cit. p. 100

<sup>218</sup> Ibidem. p. 101.

<sup>219</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 43/5, §1.

<sup>220</sup> Comité R, « Rapport d'activité du Comité R 2016 ». op. cit. p. 123.

<sup>221</sup> Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». op. cit. p. 103

multilatérales car l'échange entre deux services facilite la traçabilité de l'information et le maintien du secret. Le second est la prédilection qu'ont les services de renseignement à transmettre des synthèses d'informations, plutôt que des données brutes qui pourraient donner des indications quant à la source et aux méthodes utilisées par le service émetteur.<sup>222</sup>

#### *III.3.4. Le need-to-share*

Richard A. Best Jr. démontre que l'application trop rigide du besoin d'en connaître empêche un partage efficace des informations entre les services de renseignement. C'est la menace terroriste et les événements du 11 septembre 2001 qui ont mis à jour le manque de partage des informations au nom du principe du besoin d'en connaître. Pour l'auteur, le principe du besoin d'en connaître répond à une logique de cloisonnement des activités de renseignement. Dès lors, ce principe est incompatible avec l'organisation en réseau de la menace terroriste.<sup>223</sup>

Richard A. Best Jr. met à jour un paradoxe propre au monde du renseignement. En effet, le renseignement n'est utile que s'il est porté à la connaissance de celui qui est capable de l'utiliser, mais, au plus il est partagé, au plus il risque d'être compromis. De plus, la logique de cloisonnement rend impossible le fait de savoir ce dont l'autre a besoin. Par conséquent, il faut trouver, pour chaque renseignement, le point d'équilibre entre un partage efficace du renseignement et la protection de celui-ci.<sup>224</sup>

Bien que partager des informations représente toujours un risque pour les services de renseignement, certains pensent qu'un échange trop large, au risque d'être dommageable, reste préférable à un cloisonnement qui rendrait le travail des services de renseignement inutile.<sup>225</sup> Ces observations ont poussé les services américains à se défaire de la logique du cloisonnement et du principe du besoin d'en connaître pour le « need-to-share » qui

---

<sup>222</sup> Warusfel, Bertrand. « Contraintes juridiques et culture du secret, comme freins à l'échange de données de sécurité en Europe ». Intervention au colloque sur l'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne. CESICE, Université Grenoble-Alpes, 18 novembre 2016. [En ligne] [http://www2.droit.parisdescartes.fr/warusfel/articles/SecretEchangeDonnees\\_resumWarusfel1116.pdf](http://www2.droit.parisdescartes.fr/warusfel/articles/SecretEchangeDonnees_resumWarusfel1116.pdf) Consulté le 5 juin 2016.

<sup>223</sup> Best, Richard A. Jr. « Intelligence Information : Need-to-Know vs. Need-to-Share ». Congressional Research Service, 6 juin 2011. [En ligne] <https://fas.org/sgp/crs/intel/R41848.pdf> Consulté le 5 juin 2011. pp. 2-3.

<sup>224</sup> Ibidem. p. 1.

<sup>225</sup> Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». op. cit. p. 565.

consiste en une coopération forte en multipliant les échanges d'informations en matière de lutte contre le terrorisme.<sup>226</sup>

L'utilité du « need-to-share » est essentiel face à la menace terroriste. Cette menace terroriste bouscule le monde du renseignement car elle n'est pas organisée comme les autres. Elle est tellement différente qu'elle oblige les services de renseignement à sortir de leur logique de cloisonnement et à entrer dans une coopération pleine et entière.

### III.4. Le cadre juridique de l'échange des informations

L'objectif de cette sous-section est de recenser toutes les normes légales qui s'imposent lors d'un échange d'informations entre un service de renseignement et un service public, avec son homologue national ou un de ses homologues étrangers.

#### *III.4.1. L'échange entre les services de renseignement*

La loi organique des services de renseignement et de sécurité n'offre pas une description complète de la coopération qui devrait exister entre les deux services de renseignement du Royaume. Seul l'article 20 indique que les services de renseignement et de sécurité doivent assurer une coopération « *mutuelle aussi efficace que possible* »<sup>227</sup>, au même titre qu'avec les services de police et les autorités administratives et judiciaires. Néanmoins, la loi stipule que le Conseil national de sécurité définit les conditions de la coopération entre ces services et autorités publics. De plus, il est utile de mettre en exergue que la loi force la Sûreté de l'Etat et le SGRS à conclure un accord de coopération, selon les directives du Conseil national de la sécurité, précisément sur la cogestion de la recherche et l'analyse des activités des services de renseignement étrangers sur le territoire national.<sup>228</sup>

#### *III.4.2. L'échange entre les services de renseignement et les autres services publics*

Il est très complexe de trier toutes les notions de l'échange d'informations entre les services de renseignement et les autres services publics qui sont disséminées dans de nombreuses lois et arrêtés royaux. Cette partie présentera les éléments se trouvant essentiellement dans les deux lois règlementant la majeure partie de l'échange d'informations : la loi organique des services de renseignement et la loi OCAM. Ces

---

<sup>226</sup> Ibidem.

<sup>227</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 20, §1<sup>er</sup>.

<sup>228</sup> Ibidem. Article 20, §1, 3 & 4.

éléments seront complétés par la présentation de l'échange d'informations à l'aide de banques de données et de l'échange lors de plateformes de concertation.

#### L'échange d'informations vu par la loi organique des services de renseignement

Comme vu précédemment, la loi sur les méthodes ordinaires de recueil de données stipule que « *les autorités judiciaires, les fonctionnaires et les agents des services publics, y compris des services de police, peuvent communiquer d'initiative* »<sup>229</sup> aux services de renseignement et de sécurité les informations utiles à leurs missions. Si la demande provient des services de renseignement, ces mêmes autorités et services publics doivent communiquer les informations demandées<sup>230</sup>. Les deux seules exceptions qui exemptent les services publics de communiquer des informations à la suite d'une requête des services de renseignement sont :

- si la communication de ces données peut porter atteinte à une information ou une instruction judiciaire ou ;
- si la communication de ces données peut porter atteinte à l'intégrité physique d'une personne<sup>231</sup>.

Ensuite, la loi organique des services de renseignement et de sécurité cite les destinataires éventuels des informations détenues par les services de renseignement. Ainsi les services de renseignement peuvent transmettre seulement leurs informations « *aux ministres et aux autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leur missions ainsi qu'aux instances et personnes qui font l'objet d'une menace [...]* »<sup>232</sup>. De plus, dans le respect de la vie privée et si l'information ou l'intérêt général l'exige les dirigeants des services de renseignement et de sécurité peuvent communiquer des informations à la presse<sup>233</sup>.

S'il semble que les services de renseignement peuvent communiquer les informations qu'ils veulent à toutes les personnes concernées par une menace, il ne faut pas oublier que cela ne peut pas se faire sans une habilitation de sécurité équivalente au degré de

---

<sup>229</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 14, §1<sup>er</sup>.

<sup>230</sup> Ibidem. Deuxième alinéa.

<sup>231</sup> Ibidem. Troisième alinéa.

<sup>232</sup> Ibidem. Article 19, premier alinéa.

<sup>233</sup> Ibidem. Article 19, deuxième alinéa.

protection de l'information. Dès lors, la transmission d'informations n'est pas aussi simple qu'il n'y paraît.

Enfin, l'article 19/1 de la loi organique des services de renseignement indique une procédure particulière afin d'appliquer à ces services l'article 29 du code d'instruction criminelle. « *Les services de renseignement possèdent des indices sérieux relatifs à la commission d'un crime ou d'un délit ou indiquent, sur base d'une suspicion raisonnable que des faits punissables vont être commis ou ont été commis mais ne sont pas encore connus [...]* »<sup>234</sup>. Si tel est le cas, alors le service de renseignement doit porter ces informations à la commission BIM, qui, il faut le rappeler, est composée de personnes ayant la qualité de magistrat. Si la commission BIM est d'avis qu'un crime a été commis ou va être commis, alors elle doit immédiatement dresser un procès-verbal au parquet. Néanmoins, le dirigeant du service doit être préalablement entendu par la commission BIM sur les conditions de cette transmission d'informations.<sup>235</sup>

#### L'échange d'informations vu par la loi OCAM

Si les services publics coopèrent d'initiative ou à la demande des services de renseignement, les services d'appui de l'OCAM, en ce compris les services de renseignement, ont l'obligation de transmettre leurs informations liées à la menace terroriste et à la radicalisation. La seule exception vise les obligations internationales qui les en empêcheraient, puisque la loi OCAM institue la règle du tiers service<sup>236</sup>. De ce fait, la loi exempte spécialement les services de renseignement, le service des douanes et l'administration des affaires étrangères de transmettre des informations à l'OCAM, si ces informations proviennent d'un services homologue étranger qui a demandé de ne pas transmettre l'information à un autre service ou si ces informations mettent en péril une source humaine<sup>237</sup>. La seule obligation est d'intégrer le directeur de l'OCAM dans la confiance, mais sans l'accord du service émetteur, l'information ne sera intégrée dans aucune évaluation<sup>238</sup>. Si le pays émetteur donne son accord, le directeur ayant livré ces informations à l'OCAM a son mot à dire concernant l'intégration, ou non, de ces informations dans les évaluations de l'OCAM et sur la transmission de ces évaluations<sup>239</sup>.

---

<sup>234</sup> Ibidem. Article 19/1, premier alinéa.

<sup>235</sup> Ibidem. Article 19/1, premier et deuxième alinéa.

<sup>236</sup> Loi relative à l'analyse de la menace du 10 juillet 2006, article 6.

<sup>237</sup> Ibidem. Article 12.

<sup>238</sup> Arrêté royal portant sur l'exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace du 28 novembre 2006, article 15, §1<sup>er</sup>, troisième alinéa.

<sup>239</sup> Loi relative à l'analyse de la menace du 10 juillet 2006, article 12.

En temps normal, les évaluations de l'OCAM, comprenant des informations originaires des services de renseignement, sont transmises aux membres du Comité ministériel, aux services d'appui, au Centre de crise, au parquet fédéral et au membre du Collège des procureurs généraux ayant la matière du terrorisme et de l'extrémisme dans ses attributions. De plus, ces évaluations peuvent être transmises à un membre du gouvernement, s'il en fait la demande ou si cela est jugé utile par le directeur de l'OCAM<sup>240</sup>. Bien qu'il ne s'agisse pas d'un échange direct d'une information d'un service de renseignement à un autre service public, il est intéressant de comprendre le cheminement indirect des données récoltées par les services de renseignement, transmises à l'OCAM et, ensuite, disséminées à différents acteurs. De plus, il ne faut pas perdre de vue que ces procédés ne concernent que les échanges d'informations liés à la menace extrémiste et terroriste, puisque l'OCAM n'a, dans ses compétences, que cette matière.

Pratiquement, il existe une personne de contact au sein de chaque service d'appui de l'OCAM, afin d'assurer l'échange des données vers l'OCAM et la bonne dissémination des renseignements obtenus par l'OCAM. Ces informations transitent à travers un système de communication informatisé, sécurisé et crypté afin d'optimiser la vitesse et l'échange des données. Chaque information ou demande est qualifiée d'une mention « FLASH », « URGENT », « ROUTINE » ou « NON URGENT ». Ce qualificatif détermine la vitesse à laquelle ces informations ou ces demandes devront être traitées. Respectivement 24 heures, trois jours, 10 jours et 30 jours.<sup>241</sup>

#### L'échange d'informations à l'aide des bases de données

Les banques de données sont des outils qui permettent de fluidifier l'échange d'information. Ainsi, plusieurs services, ou plusieurs composantes d'une même entité, peuvent regrouper et partager leurs informations sur une même plateforme informatique. Puisqu'il n'est pas possible de recenser toutes les bases de données de tous les services publics belges, il sera fait état de la Banque de données nationale générale (BNG), qui appartient à la police, et de la possibilité d'instaurer des banques de données communes. Quant aux services de renseignement, leurs banques de données sont gardées secrètes même si la Commission Attentat fait apparaître qu'il en existe<sup>242</sup>.

---

<sup>240</sup> Ibidem. Article 10, §1 & 2.

<sup>241</sup> Arrêté royal portant sur l'exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace du 28 novembre 2006, article 11, §1, 3, 5, & 7.

<sup>242</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la

La BNG permet la coordination, le croisement et la vérification des données à caractère personnel et des antécédents de police administrative et judiciaire<sup>243</sup>. C'est un outil à la disposition de chaque policier afin qu'il puisse réaliser son travail avec efficacité. Elle n'est pas accessible aux services de renseignement, bien qu'ils se soient manifestés pour obtenir l'accès à cette base de données<sup>244</sup>. La situation de l'OCAM est un peu plus complexe car elle détient du personnel appartenant entre autres aux services de renseignement, mais aussi à la police. Comme tous policiers ceux-ci peuvent utiliser la BNG, alors que leurs collègues venus des autres services d'appui ne disposent d'aucun accès, sauf exception dans le cadre de leurs missions<sup>245</sup>.

Pour rappel, les services de renseignement peuvent avoir un accès aux banques de données des services publics, dont les services de police et c'est au Roi qu'il revient de fixer les modalités générales de cet accès direct<sup>246</sup>. Si la loi oblige les services publics, dont les services de police, de coopérer avec les services de renseignement, dans le cas où ceux-ci ont une demande particulière, rien n'oblige ces mêmes services à offrir un accès direct à ses banques de données, que ce soit à la Sûreté ou au SGRS.

D'un autre côté, la loi sur la fonction de police institue la possibilité d'établir des banques de données communes entre l'OCAM, les services de police et les services de renseignement dans le cadre de missions de prévention et de suivi de la menace terroriste et extrémiste<sup>247</sup>. Ces bases de données sont créées conjointement par les ministres de l'Intérieur et de la Justice dont ils sont les responsables.

Si ces banques de données doivent s'inscrire dans le cadre des missions de lutte contre le terrorisme et l'extrémisme, il faut aussi que leur mise en place soit motivée par :

- la nécessité de traiter en commun des informations appartenant aux différents services prenant part à la banque de données,

---

station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. pp. 281-282.

<sup>243</sup> Loi sur la fonction de police du 5 août 1992, article 44/7, 3° & 4°.

<sup>244</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. p. 207.

<sup>245</sup> Arrêté royal portant sur l'exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace du 28 novembre 2006, article 12., §1.

<sup>246</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 14, quatrième alinéa.

<sup>247</sup> Loi sur la fonction de la police du 5 août 1992, article 44/2, §2.

- l'aide à la prise de décisions par les autorités administratives, de police administrative ou judiciaire<sup>248</sup>.

Si de telles banques de données sont mises en place afin de lutter contre le terrorisme, elles doivent être directement accessibles à l'OCAM, à la police intégrée et aux services de renseignement. De plus, les informations contenues dans ces bases de données communes peuvent être directement accessibles, transmises ou faire l'objet d'une interrogation directe par :

- la Commission permanente de la police locale ;
- la Direction générale Centre de crise ;
- la Direction générale Sécurité et Prévention du service Public Fédéral Intérieur ;
- la Direction générale des Etablissements pénitentiaires et les établissements pénitentiaires ;
- le Service Public Fédéral Affaires étrangères, Direction générale Affaires consulaires ;
- le Ministère public ;
- la Cellule de traitement des informations financières ;
- l'Office des Etrangers ;
- les services d'enquête et recherche de l'Administration générale des douanes et accises.

Il est nécessaire de souligner que la loi stipule précisément que ces accès, transmissions et interrogations doivent se faire dans le respect du principe du « besoin d'en connaître ». <sup>249</sup>

Pour le moment, il existe deux bases de données communes. L'une a pour objectif de suivre les « terrorist fighters »<sup>250</sup>, l'autre tente de recenser les « propagandistes de haine »<sup>251</sup>.

---

<sup>248</sup> Ibidem. Article 44/11/3bis, §1 et 2.

<sup>249</sup> Ibidem. Article 44/11/3ter, §1 et 2.

<sup>250</sup> Arrêté royal relatif à la banque de données Terrorist Fighters du 21 juillet 2016.

<sup>251</sup> Arrêté royal relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1erbis « de la gestion des informations » du chapitre IV de la loi sur la fonction de police du 23 avril 2018.

### L'échange d'informations à l'aide des plateformes de concertations

La menace de l'extrémisme et du terrorisme a forcé les pouvoirs publics à mettre en place une approche globale de la sécurité en créant le Plan radicalisme, souvent appelé le « Plan R ». Pour ce faire, ils ont créé différentes plateformes aux niveaux national et local.

Tout d'abord, il y a la « *Task Force nationale* » (TFN). Elle est créée en 2006, mais son fonctionnement est précisé par la circulaire FTF du 21 août 2015. Sous la direction de l'OCAM, la TFN rassemble la Sûreté de l'Etat, le SGRS, les représentants de la police fédérale et locale, des Affaires étrangères, de la Justice, de l'Intérieur, de la CTIF, de l'Office des étrangers, du Centre de crise, du ministère public, des communautés et des régions. Ses objectifs sont la prévention de la radicalisation, assurer le suivi et évaluer les mesures existantes afin de restreindre l'impact des groupes radicalisés. Pratiquement, la TFN est subdivisée en groupes de travail selon des problématiques (radicalisation sur internet, en milieu carcéral, à la télévision) et des thématiques (salafisme, extrême droite et gauche, tendances en Asie mineure et dans le Caucase du Nord). En résumé, la TFN doit englober tous les acteurs fédéraux utiles afin de mener à bien la politique de sécurité contre l'extrémisme et le radicalisme.<sup>252</sup>

Ensuite, il y a les Taskforces locales, qui ont pour objectif de transposer les efforts de la TFN en assurant un suivi supra-local. « [...] *une TFL est une plateforme de concertation décentralisée où s'échangent des informations relatives à la radicalisation violente et où se concluent des accords de coordination portant sur l'obtention de telles informations* »<sup>253</sup>. Elles sont guidées par les consignes et les priorités de la TFN. « *Les objectifs de la TFL sont :*

- *d'échanger et de discuter d'informations, de renseignements et d'analyses;*
- *de faire concorder les projets de recueil d'information avec les activités d'information des différents services et veiller à l'exécution de ces procédures, et de faire des propositions d'insertion et de suppression d'entités dans la Joint Information Box (JIB);*
- *de déterminer les entités décrites comme "à suivre de façon prioritaire";*

---

<sup>252</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste », op. cit. pp. 160-162.

<sup>253</sup> Ibidem. pp. 162-163.

- *d'offrir un appui aux fonctionnaires de police de premier plan, qui ne sont pas spécialisés en la matière mais qui sont susceptibles d'être confrontés aux signes d'une éventuelle radicalisation;*
- *de proposer et de faire appliquer des mesures préventives ainsi que des mesures destinées à contrecarrer;*
- *d'entretenir des contacts structurels et/ou ponctuels avec les autorités locales et leurs services »*<sup>254</sup>
- d'assurer le suivi des « Foreign Terrorist Fighters ».

Les TFL regroupent au niveau supra-local les services de sécurité fédéraux, Police fédérale, Sûreté de l'Etat, SGRS, OCAM, la police locale ainsi que les parquets locaux et fédéraux.<sup>255</sup>

Enfin, il existe les Cellules de sécurité intégrale locale (CSIL). Celles-ci rassemblent tous les acteurs pouvant jouer un rôle dans la détection et le suivi de personnes ou de groupes radicalisés. Elles sont composées du bourgmestre, d'un officier de la police locale, et des services socio-préventifs de la commune, de la région ou de la communauté d'où réside la personne ou le groupe suivi. De nombreuses communes n'ont pas créées de CSIL puisqu'elles n'habitaient pas de groupes ou personnes radicalisées<sup>256</sup>. Néanmoins, les CSIL vont devenir obligatoire puisque le Parlement a adopté le projet de loi allant dans ce sens le 19 juillet 2018<sup>257</sup>.

Il y a une réelle interaction entre la TFL et la CSIL. La TFL regroupe les professionnels issus des métiers du renseignement et de la sécurité. Sous cette casquette, il assume le rôle répressif du radicalisme à un niveau supra-local, tandis que la CSIL regroupe les acteurs issus du milieu préventif. Le lien entre ces deux plateformes se fait à travers l'officier de la police locale qui rapporte les éléments transmis par la CSIL à la TFL. Par conséquent, il y a une jonction qui est faite entre les secteurs préventif et répressif.

Face à la menace terroriste et extrémiste, des outils ont été mis en place afin de forcer la concertation et la coordination. Rien de tel n'existe pour contrer les autres menaces. L'analyse des textes législatifs n'a pas démontré qu'il existait des plateformes de

---

<sup>254</sup> Ibidem. p. 163.

<sup>255</sup> Ibidem. pp. 162-166.

<sup>256</sup> Ibidem. pp. 166-167.

<sup>257</sup> La Chambre des représentants de Belgique, « Projet de loi portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme ». 19 juillet 2018. Article 2.

concertation qui s'échangent de l'information à propos des organisations sectaires, de l'espionnage, de l'ingérence, ou encore de la défense du potentiel économique et scientifique. Il faut rappeler que le terrorisme et l'extrémisme ne sont qu'une seule des différentes menaces qui préoccupent les services de renseignement. Néanmoins, le fait que ces différents acteurs de la sécurité se rassemblent, tant au niveau fédéral que local, rend certainement service à l'échange d'informations en général.

#### *III.4.3. L'échange entre les services de renseignement et les services étrangers*

A l'instar de la coopération entre les services nationaux, la loi organique des services de renseignement et de sécurité ne précise pas les modalités de la coopération entre les services nationaux et leurs homologues étrangers. Celle-ci indique seulement que les services de renseignement doivent veiller à assurer une collaboration avec les services étrangers.<sup>258</sup>

En parallèle, il est utile de rappeler qu'une des trois missions de l'OCAM, qui n'est pas un service de renseignement, est d'assurer des relations internationales avec des services homologues et de transmettre les informations, obtenues dans le cadre de ces relations, aux services d'appui<sup>259</sup>. Dès lors, il s'agit, ici, d'un échange indirect d'informations entre les services de renseignement nationaux et internationaux passant par l'entremise de l'OCAM et de ses homologues étrangers.

### III.5. Le cadre juridique de l'utilisation des informations

Cette sous-section présente les dispositions légales qui s'appliquent à l'utilisation des informations collectées par les services de renseignement. Ici, il est fait état des utilisations politiques, judiciaires, et administratives.

Avant d'aborder les différentes exploitations possibles des informations récoltées par les services de renseignement, il est utile de savoir que « *si le Comité permanent R constate que les décisions relatives à des méthodes spécifiques ou exceptionnelles de recueil de données sont illégales, il ordonne la cessation de la méthode concernée [...] et ordonne l'interdiction d'exploiter les données recueillies grâce à cette méthode et leur destruction*

---

<sup>258</sup> Ibidem. Article 20, §1<sup>er</sup>.

<sup>259</sup> Loi relative à l'analyse de la menace du 10 juillet 2006, article 8, 3°.

[...] »<sup>260</sup>. Néanmoins aucune loi n'interdit l'exploitation des données reçues par un service étrangers dont la récolte a suivi un processus contraire au droit belge.

### *III.5.1. L'utilisation politique des informations*

Dans la loi organique des services de renseignement, seul un article aborde la relation entre le SGRS et le monde politique. Ainsi, le SGRS doit rechercher, analyser et traiter les informations menaçant l'Etat, mais, contrairement à la Sûreté, il doit aussi informer les ministres compétents et il peut donner son avis en ce qui concerne la politique intérieure et étrangère de sécurité et de défense<sup>261</sup>. Quant à la Sûreté, aucune disposition de cette loi ne traite de sa relation avec le monde politique.

De son côté, le Conseil national de sécurité, avec l'appui du comité stratégique et du Comité de coordination du renseignement et de la sécurité, établit les priorités de la politique de renseignement et de sécurité, sur la base des recommandations fournies par les services de sécurité du pays. Ensuite, c'est aux comités d'appui d'élaborer les plans stratégiques afin d'appliquer cette politique.<sup>262</sup> Cela peut se faire par le renforcement de la législation pénale, par des plans d'action (plan Radicalisme, plan Canal), ou encore par l'interdiction des cartes prépayées anonymes, par exemple.

Enfin, le CNS est compétent pour désigner un territoire « *zone de conflit djihadiste* »<sup>263</sup> et les personnes ou entités ciblées par des mesures financièrement restrictives afin de lutter contre le terrorisme<sup>264</sup>.

### *III.5.2. L'utilisation judiciaire des informations*

Cette sous-partie présente la priorité qui est faite aux missions judiciaires par rapport aux missions de renseignement. De cette relation découle de nombreux débats menant tous au difficile équilibre entre la sécurité et le droit des individus à un procès équitable. Si les agents du renseignement ont l'obligation de dénoncer les crimes et les délits qui sont portés à leur connaissance, il doit exister une procédure qui permet aux agents de se protéger, mais de protéger aussi leurs sources, leurs capacités et leurs méthodes. C'est pour cette raison que cette sous-partie abordera la question de l'utilisation du témoignage

---

<sup>260</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 43/6, §1<sup>er</sup>.

<sup>261</sup> Ibidem. Article 11, §1<sup>er</sup>, 1<sup>o</sup>.

<sup>262</sup> Arrêté royal portant création du Conseil national de sécurité du 28 janvier 2015, article 3 & Arrêté royal portant création du Comité stratégique et du Comité de coordination du renseignement et de la sécurité du 2 juin 2015, article 9, 1<sup>o</sup> & 2<sup>o</sup>.

<sup>263</sup> Arrêté royal relatif à la banque de données Terrorist Fighters du 21 juillet 2016, article 1<sup>er</sup>, §1<sup>er</sup>, 13<sup>o</sup>.

<sup>264</sup> Arrêté royal relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme du 28 décembre 2006.

anonyme par un agent du renseignement, de celle des informations classifiées lors d'un procès pénal et de l'utilisation du blanchiment de l'information lors d'une procédure pénale afin de protéger une source ou une technique d'enquête.

#### La primauté du judiciaire sur le renseignement

Il a été vu précédemment (*voir supra*, 3.1.) que les services de renseignement ont l'obligation de porter à la connaissance des autorités judiciaires leurs informations indiquant qu'un délit ou un crime a été ou sera commis. Cependant, les informations récoltées par les services de renseignement ne peuvent pas « *constituer le motif exclusif ni la mesure prédominante conduisant à la condamnation d'une personne* »<sup>265</sup>. En d'autres termes, les autorités judiciaires doivent étayer l'affaire avec d'autres éléments de preuves qui devront représenter une partie prédominante du dossier.<sup>266</sup>

Cette obligation démontre que les agents du renseignement ne détiennent pas de passe-droit et doivent appliquer, comme tous les autres fonctionnaires et officiers publics, l'article 29 du code d'instruction criminelle. Cette prévalence de l'autorité judiciaire se manifeste aussi par l'interdiction de gêner une information ou une instruction par une mission de renseignement. Si les services de renseignement entreprennent des méthodes de recueil de données qui viennent concourir une information ou une instruction judiciaire, le magistrat compétent peut en demander l'arrêt<sup>267</sup>.

#### Le témoignage anonyme d'un agent du renseignement dans un procès

L'article 75 du code d'instruction criminelle indique que les témoins doivent se faire connaître en prêtant serment. Cependant, il existe trois formes d'anonymat possible afin de protéger une personne lors d'un procès pénal.

Tout d'abord, il y a l'anonymat partiel. Celui-ci permet au juge d'instruction, au juge du fond, ou au ministère public d'omettre certaines informations personnelles des témoins dans les procès-verbaux et au procès afin de les protéger eux et leurs proches. Evidemment, il faut que cette décision soit motivée.<sup>268</sup>

---

<sup>265</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 19/1, §1<sup>er</sup>, cinquième alinéa.

<sup>266</sup> Ibidem.

<sup>267</sup> Ibidem. Article 13/5.

<sup>268</sup> Code d'instruction criminelle, article 75bis & 155bis.

Ensuite, il est possible pour les personnes chargées de constater, d'instruire, d'examiner les circonstances d'une infraction de renseigner l'adresse à laquelle ils exercent leurs professions plutôt que celle de leur domicile.<sup>269</sup>

Enfin, il existe l'anonymat complet. Cet anonymat est possible pour les témoins menacés et pour les officiers de police judiciaire craignant pour leur sécurité physique. Cet anonymat est décidé par le juge d'instruction, du fond ou le ministère public. Néanmoins, il doit répondre à certaines conditions. En effet, il doit être subsidiaire aux autres formes d'anonymat, il est utilisé si les autres moyens d'instruction ne sont pas suffisants à la manifestation de la vérité et il n'est envisageable que pour certains crimes bien définis. Si une instruction peut s'ouvrir sur la base d'un témoignage anonyme, il est essentiel de souligner que la condamnation d'une personne ne peut pas reposer ni exclusivement, ni de manière déterminante, sur un témoignage anonyme.<sup>270</sup>

En dehors de ces trois modalités, le témoignage anonyme n'a pas de force probante, bien que la Cour de cassation ait admis que les témoignages anonymes « *peuvent être pris en considération pour ouvrir ou orienter une enquête et rassembler des preuves de manière autonome, ou pour en apprécier la cohérence* »<sup>271</sup>.

Dans son avis, le Comité R préconise qu'il soit créé la possibilité pour les agents du renseignement de témoigner sous le couvert de l'anonymat absolu<sup>272</sup>. Cette possibilité risque de pousser un peu plus les agents du renseignement dans les bras de l'autorité judiciaire. En effet, les autorités judiciaires pourraient être tentées d'utiliser les agents du renseignement comme élément de preuve de plus en plus fréquemment. Cependant, l'anonymat complet empêche une condamnation sans autre moyen de preuves. Dès lors, le travail judiciaire reste essentiel afin de condamner l'auteur d'un crime ou d'un délit.

#### L'utilisation de preuves illégales

Comme rappelé au début de cette sous-partie, le Comité R a comme devoir de détruire les informations illégalement obtenues et d'en interdire l'exploitation. Dans son avis, le Comité R demandait au législateur de clarifier si la preuve obtenue illégalement devait

---

<sup>269</sup> Ibidem. Article, 75ter & 155ter.

<sup>270</sup> Ibidem. Article 86bis & 189bis.

<sup>271</sup> Cour de cassation de Belgique, arrêt P.04.1528.F du 23 mars 2005.

<sup>272</sup> Le comité permanent R, « Avis du Comité permanent R relatif à l'avant-projet de loi relatif aux méthodes de recueil de données des services de renseignement et de sécurité ». 2006. p. 11. [En ligne] <http://www.comiteri.be/images/pdf/franstalig/Avis%20projet%20loi%20methodes%20recueil%20donnees%20services%20renseignement%20et%20securite.pdf>

être frappée de nullité, or, aujourd'hui, une telle preuve n'est pas sanctionnée de cette manière<sup>273</sup>. En effet, le Comité R doit détruire ces informations et interdire leur exploitation, mais il n'a autorité que sur les services de renseignement. L'autorité judiciaire n'est pas sous le contrôle du Comité R. Dès lors, il est imaginable que la preuve soit utilisée lors d'un procès pénal. L'avis du Comité R reprend l'arrêt de la Cour de cassation qui explique dans quelle mesure une preuve illégalement obtenue peut être utilisée<sup>274</sup>. Ainsi, il existe trois exceptions à l'exclusion d'une preuve obtenue illégalement : « *le cas de la violation d'une forme prescrite à peine de nullité, [que] lorsque son obtention est entachée d'un vice de nature à lui ôter sa fiabilité ou à compromettre le droit à un procès équitable* »<sup>275</sup>.

Afin d'éviter de compromettre la tenue d'un procès équitable, le juge peut tenir compte :

- du caractère purement formel de l'irrégularité;
- de l'absence d'incidence du manquement incriminé sur le droit ou sur la liberté protégée par la norme transgressée;
- de la circonstance que l'irrégularité imputée à la police ou au dénonciateur n'a pas été commise intentionnellement;
- du fait que la preuve illégalement obtenue ne constitue qu'une composante matérielle du délit;
- du fait que la gravité de l'atteinte constatée surpasse nettement celle de l'irrégularité du constat du délit.<sup>276</sup>

Selon le Comité R, ces critères peuvent être utiles à l'appréciation d'une preuve irrégulièrement obtenue par les services de renseignement lors d'un procès pénal<sup>277</sup>.

Ces exceptions rejoignent la jurisprudence « Antigone » puisque selon celle-ci seuls la peine de nullité, la fiabilité de la preuve, ou le droit à un procès équitables peuvent être les raisons de l'exclusion d'une preuve obtenue de manière irrégulière.

---

<sup>273</sup> Ibidem. pp. 10-11.

<sup>274</sup> Ibidem. p. 6.

<sup>275</sup> Cour de cassation de Belgique, arrêt P.05.0119.F du 12 octobre 2005.

<sup>276</sup> Ibidem.

<sup>277</sup> Le comité permanent R, « Avis du Comité permanent R relatif à l'avant-projet de loi relatif aux méthodes de recueil de données des services de renseignement et de sécurité », op. cit. p. 7.

## L'usage des données classifiées

D'un côté, l'article 38 de la loi organique des services de renseignement et de sécurité fait état de la possibilité de l'acquisition de données classifiées des services de renseignement par l'autorité judiciaire. En effet, le magistrat instructeur a la possibilité de saisir des données et du matériel classifiés qu'il doit remettre au dirigeant du service de renseignement à la fin de la procédure judiciaire. Dans le cas où la saisie de ces informations classifiées menacerait la conduite des missions de la Sûreté ou du SGRS, elles sont mises sous scellés en attendant la décision de la Chambre des mises en accusation. Lors de cette procédure, seuls les magistrats du siège et du ministère public siégeant en Chambre des mises en accusation, le magistrat instructeur et le dirigeant du service peuvent prendre connaissance des pièces classifiées saisies. Si la Chambre des mises en accusation répond par la négative à la contestation du dirigeant du service, la donnée ou le matériel classifié peut s'intégrer à une procédure judiciaire.<sup>278</sup>

De l'autre côté, les arrêts de la Cour constitutionnelle stipulent que le droit qu'a la partie défenderesse de prendre connaissance de tous les éléments de preuve de la partie poursuivante n'est pas absolu. Lorsqu'il en va de la sécurité nationale, d'une personne, d'une source, de la préservation de la capacité d'un service ou d'une méthode d'enquête, *« il peut être nécessaire de ne pas divulguer certains éléments de preuve à cette partie en vue de préserver les droits fondamentaux d'une autre personne ou de garantir un intérêt général important »*<sup>279</sup>. En d'autres termes, ces raisons contrebalancent le droit des prévenus à avoir un procès équitable qui se base sur *« le principe de l'égalité des armes entre l'accusation et la défense, ainsi que le caractère contradictoire du procès »*<sup>280</sup>. Effectivement, si la partie défenderesse n'a pas les preuves qui la mettent en cause, elle n'a pas la possibilité de se défendre. Cependant, les arrêts de la Cour constitutionnelle mettent un point d'orgue à ce que cette justification soit proportionnée aux objectifs poursuivis et que cette procédure intègre un juge indépendant et impartial afin de contrôler la légalité de la procédure.<sup>281</sup>

---

<sup>278</sup> Loi organique des services de renseignement et de sécurité du 30 novembre 1998, article 38.

<sup>279</sup> Cour constitutionnelle, arrêt n° 105/2007 du 19 juillet 2007, B.11.1.

<sup>280</sup> Ibidem.

<sup>281</sup> Cour constitutionnelle, arrêt n° 202/2004 du 21 décembre 2004, B.27.6, arrêt n° 105/2007 du 19 juillet 2007, B.11.1, et l'arrêt n°145/2011 du 22 septembre 2011, B.18.

Il faut ajouter que la Cour européenne des droits de l'Homme approuve cette justification.<sup>282</sup>

#### Le blanchiment d'informations

Lorsque la simple révélation d'une information permet d'identifier une source, une technique ou une méthode d'enquête, il se peut que l'autorité judiciaire procède à un blanchiment d'information. Dans le cas où l'indicateur est le seul à détenir une information permettant l'arrestation de l'auteur d'un fait, l'anonymat ne suffit pas et le blanchiment de l'information se révèle comme le seul moyen efficace afin de protéger la source. En d'autres termes, il s'agit d'utiliser l'information par un autre moyen d'enquête qui ne révélera pas la provenance de l'information.<sup>283</sup>

Deux types de blanchiments d'informations paraissent strictement interdits par la doctrine. Le premier est celui qui consiste à couvrir l'illégalité de l'obtention d'un élément de preuve ou l'introduction de faux éléments dans la procédure. Le second est celui qui dissimule « *l'existence d'une méthode d'enquête qui a permis d'administrer des renseignements susceptibles d'intéresser une autre information ou une autre instruction ou d'en ouvrir une nouvelle, de les faire entrer en procédure en indiquant qu'ils proviennent d'un informateur* »<sup>284</sup>. Ces deux formes de blanchiment sont exclues car, soit, elles ne représentent pas la réalité, soit, elles consistent en l'utilisation d'une méthode d'enquête qui n'est pas vérifiable.<sup>285</sup>

Bien que le blanchiment de l'information paraisse déloyal, il est accepté lorsque la réalité n'en est pas manipulée et qu'il n'y a qu'une occultation d'une partie de la vérité à des fins de protection. De plus, il ne réduit pas les droits de la défense pour deux raisons. Primo, si l'origine de l'information est occultée dans la procédure, cette origine ne peut pas être, non plus, le siège de la culpabilité de la défense. Dans le cas d'un blanchiment d'informations, la partie défenderesse se retrouve dans une position égale au ministère public puisqu'ils ont les mêmes éléments. Cette situation est plus confortable pour la défense que lorsque cette dernière n'a pas accès à tous les éléments puisqu'ils sont classifiés. Secundo, l'élément présent dans la procédure existe réellement et la défense a la possibilité d'en vérifier la légalité. Dans ce cas l'élément de preuve « *n'a aucun*

---

<sup>282</sup> CEDH, 22 juillet 2003 et 27 octobre 2004, Edwards et Lewis c. Royaume-Uni

<sup>283</sup> De Valkeneer, Christian-paul, « Manuel de l'enquête pénale ». Bruxelles, Editions Larcier, 2018. pp. 177-178.

<sup>284</sup> Ibidem. p. 178.

<sup>285</sup> Ibidem. pp. 178-179.

*caractère artificiel à l'instar de données créées de toutes pièces qui contrarient l'exercice des droits de la défense en raison de leur caractère frauduleux »<sup>286, 287</sup>.*

### *III.5.3. L'utilisation administrative des informations*

La recherche et l'analyse de différents textes législatifs n'ont pas permis de mettre à jour une utilisation administrative des informations récoltées par les services de renseignement. Cela paraît logique puisque ces services ne sont pas des services de répression. Cependant, bien que les services de renseignement ne prennent pas directement des mesures administratives envers des personnes, leurs renseignements peuvent être utilisés en ce sens.

Tout d'abord, une utilisation possible des informations collectées par les services de renseignement se fait par l'entremise de l'OCAM. En effet, l'OCAM utilise ces informations afin d'évaluer la menace et les mesures nécessaires pour contrer cette menace<sup>288</sup>. Plus précisément, les données centralisées au sein de l'OCAM doivent permettre d'évaluer la menace selon quatre niveaux : niveau 1 ou faible ; niveau 2 ou moyen ; niveau 3 ou grave ; niveau 4 ou très grave<sup>289</sup>. Par exemple, c'est à l'aide d'informations récoltées par les services de renseignement et de cette échelle que l'OCAM est capable de déterminer le niveau de menace qui pèse sur le territoire national.

Ensuite, il est envisageable qu'un citoyen belge se voie retirer ou invalider sa carte d'identité par le ministre de l'Intérieur sur base d'un avis de l'OCAM. Cette utilisation est réalisable si l'OCAM estime que le citoyen va se rendre dans une zone où des groupes terroristes sont actifs et que son retour peut poser une menace sérieuse d'infraction terroriste ou que ce citoyen projette de perpétrer un acte terroriste hors du territoire du royaume. Cette décision est prise en concertation avec les autorités judiciaires afin de ne pas impacter négativement la procédure pénale.<sup>290</sup>

Parallèlement, il existe une mesure similaire quant au retrait et au refus de délivrance d'un passeport, par le ministère des Affaires étrangères, à un citoyen représentant une menace pour l'ordre et la sécurité publics. Dans ce cas-ci, il faut noter que la loi autorise ce genre

---

<sup>286</sup> Ibidem. p. 179.

<sup>287</sup> Ibidem.

<sup>288</sup> Loi relative à l'analyse de la menace du 10 juillet 2006, article 8, 1° & 2°.

<sup>289</sup> Arrêté royal portant sur l'exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace du 28 novembre 2006, article 11, §6.

<sup>290</sup> Loi modifiant la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques du 10 août 2015, article 2, alinéa 1 & 2.

de refus sur l'avis motivé d'une autorité compétente, et qu'elle fait référence à l'ordre et la sécurité publics et non seulement au terrorisme. De plus, il est utile de signaler que l'invalidation du passeport est automatique, si le citoyen est la cible d'un refus d'octroi ou d'une invalidation de sa carte d'identité.<sup>291</sup>

Enfin, le Conseil national de sécurité peut geler les fonds d'une personne ou d'une organisation en lien avec le terrorisme après une évaluation de l'OCAM et avec la concertation des autorités judiciaires<sup>292</sup>.

En conclusion, aucune de ces mesures administratives ne sont prises directement par l'un des deux services de renseignement, mais ces derniers alimentent l'OCAM qui, lui, est compétent pour prendre de telles mesures. Ces nouvelles applications démontrent le fait que les services de sécurité disposent d'un arsenal de mesures plus important face à la menace de l'extrémisme et du terrorisme qu'à d'autres menaces, comme le crime organisé ou la protection du potentiel économique et scientifique, par exemple. Il va sans dire que ces possibilités sont offertes par l'existence de l'OCAM qui, elle, peut utiliser les informations qu'elle reçoit, contrairement aux services de renseignement qui doivent les distribuer aux bons destinataires afin que les bonnes décisions soient prises.

---

<sup>291</sup> Loi portant modification du Code consulaire du 10 août 2015, article 4 & 5.

<sup>292</sup> Arrêté royal relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme du 28 décembre 2006, article 3.

## Chapitre IV – L'état des lieux de l'échange d'informations des services de renseignement

Il existe plusieurs moyens permettant d'augmenter la collaboration entre les services. La loi aborde souvent les modalités d'échange d'informations à partir des banques de données et de certaines plateformes de concertation, comme les Task Forces locales (TFL). Parallèlement à cela, les services de renseignement élaborent des protocoles d'accord de coopération avec certaines administrations dans le but de forcer la communication entre ces entités. Ceux-ci réglementent les domaines dans lesquels les synergies doivent s'opérer et fixent la fréquence des rencontres entre ces services, mais surtout, ils permettent d'établir quelles connexions doivent être établies entre quelles personnes. En effet, un bon échange d'informations se base avant tout sur la connaissance du bon détenteur ou destinataire de l'information. Parfois, les services de renseignement ont la possibilité de placer un officier de liaison dans un service.

Ce chapitre a pour objectif de présenter sur base des entretiens réalisés les connexions qui existent en pratique entre les différents partenaires du monde du renseignement belge. Nous présenterons l'état des relations entre la Sûreté de l'Etat et le SGRS, puis entre ces deux services et, d'une part, les services publics nationaux, et, d'autre part, leurs homologues étrangers.

### IV.1. L'échange d'informations entre les services de renseignement en pratique

En 2004, un protocole d'accord de coopération, classé confidentiel, est signé entre le SGRS et la Sûreté. Il prévoyait un échange de personnel entre la Sûreté et le SGRS, mais cette modalité n'a encore jamais été appliquée. Ce protocole oblige les membres des services analyses de ces deux services à partager des informations dans certains domaines lors de réunions. Il prévoit que les deux services se rencontrent une fois tous les mois. Les domaines de coopération dépendent de l'actualité et il est probable que le terrorisme en fait partie aujourd'hui. Il semblerait que ce protocole ait réglementé la procédure de communication entre ces deux services, mais qu'il n'a pas enclenché la collaboration entre eux. En fait, les services de renseignement coopéraient déjà de manière informelle

par le biais de relations interpersonnelles. D'ailleurs, les premières réunions formelles n'ont été que peu fructueuses et ce sont les relations personnelles qui ont permis un échange efficace en dehors de toute structure formelle.<sup>293</sup>

Pour des raisons de sécurité, ce protocole est classifié « confidentiel » et il n'est dès lors pas possible d'en dire plus.

## IV.2. L'échange d'informations entre les services de renseignement et les services publics en pratique

Il est toujours délicat de mettre au grand jour les relations qu'entretiennent les services de renseignement avec leurs partenaires. Certains éléments étaient plus accessibles que d'autres, ce qui explique pourquoi certaines relations sont analysées en profondeur et d'autres de manière beaucoup plus superficielle.

Les points suivants aborderont les relations qu'entretiennent les services de police, l'administration pénitentiaire et le FOREM avec les services de renseignement et de manière sommaire, le lien qui existe entre les administrations du renseignement et les autres services publics. Enfin, l'interaction qu'il y a entre les plateformes de concertation, telles que les TFL et les CSIL, sera analysée.

### *IV.2.1. La relation entre les services de renseignement et les services de police*

De 1938 à 2004, des gendarmes étaient détachés dans les bâtiments du SGRS afin de mener des enquêtes de sécurité. Suite à la réforme de la Police de 1998, ils ont été réintégrés au corps de la police fédérale et ce détachement a été supprimé, malgré les demandes de maintien du dirigeant du SGRS.<sup>294</sup>

Bien que ce n'était pas l'objectif, la proximité de ces gendarmes avec le SGRS fluidifiait l'échange d'informations entre eux. Si le personnel du SGRS avait une demande à adresser à un service de gendarmerie, il pouvait demander au gendarme qui savait directement à qui s'adresser. De manière non officielle, le détachement de gendarme agissait comme un service de liaison entre les deux services. Aujourd'hui, un membre du SGRS travaille dans les bureaux de la police fédérale dans le domaine de l'anti-

---

<sup>293</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>294</sup> Comité R, « Rapport d'activité du Comité R 2004 ». pp. 66-68. [En ligne] <http://www.comiteri.be/images/pdf/Jaarverslagen/2004%20fr.pdf?phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb>

terrorisme. Bien que ce ne soit pas sa fonction, le simple fait de sa présence établit un canal de communication entre ces deux services.<sup>295</sup>

De son côté, la Sûreté de l'Etat ne dispose pas d'un représentant à la police fédérale et cette dernière n'a pas non plus d'officier de liaison à la Sûreté. En revanche, certains employés de la Sûreté sont d'anciens policiers. Ils n'ont plus aucun lien officiel avec les services de police, mais il est envisageable d'imaginer que leurs anciennes relations professionnelles soient bénéfiques à la transmission d'informations entre les deux services.<sup>296</sup>

A ce jour, aucun des deux services de renseignement nationaux n'a conclu d'accord de coopération avec les police fédérale et locale<sup>297</sup>. Tel que démontré, ils coopèrent à l'aide de banques de données, comme celle des « *terrorist fighters* », et la circulaire du 21 août 2015 structure officiellement l'échange d'informations à propos de ces derniers. De plus, les TFL reposent sur des accords tacites et elles sont jugées efficaces, en termes de communication, par les praticiens<sup>298</sup>.

Ces différentes relations démontrent qu'il existe une multitude de possibilités, comme la cohabitation des services, la présence d'un officier de liaison, ou encore les plateformes de concertation, visant à enclencher la collaboration entre les services de police et les services de renseignement. Bien qu'il y ait une coopération entre ces services, un protocole d'accord de coopération reste un des outils qui permet un échange plus fluide et durable. C'est pour cette raison qu'il serait judicieux d'entériner les règles de cette coopération dans un protocole officiel qui est, depuis longtemps, en négociation<sup>299</sup>.

#### *IV.2.2. La relation entre les services de renseignement et l'administration pénitentiaire*

En 2000, la Sûreté de l'Etat recommandait l'intensification des échanges avec l'administration pénitentiaire. L'accord sera signé six ans plus tard à la demande de la Sûreté de l'Etat qui jugeait que cette administration ne transmettait pas de manière spontanée les informations utiles. Le Comité R distingue une première période, entre 2006 et 2014, où l'échange entre les deux services est resté faible et une seconde période, après 2014, durant laquelle les échanges se sont intensifiés. Il y aurait plusieurs raisons à

---

<sup>295</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>296</sup> Ibidem.

<sup>297</sup> Comité R, « Rapport d'activité du Comité R 2016 », op. cit. p. 119.

<sup>298</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>299</sup> En 2004, la Sûreté de l'Etat assurait avoir entamer des discussions avec la police fédérale en vue d'un accord de coopération. Voir : Comité R, « Rapport d'activité du Comité R 2004 », op. cit. p. 18.

cela. D'un côté, la conjoncture a poussé les deux services à se rapprocher. A partir de 2012, le nombre de personnes détenues pour des raisons de terrorisme ou de radicalisme a nettement augmenté et, deux ans plus tard, la nouvelle direction a fait de l'échange d'informations, tant au niveau national qu'international, sa priorité. D'un autre côté, le protocole d'accord a permis de couvrir juridiquement et administrativement le personnel de l'administration pénitentiaire dans leurs échanges avec la Sûreté de l'Etat. Cela a permis aux directeurs de prisons de faire preuve de moins de réserves dans leurs relations avec la Sûreté. D'ailleurs, le Comité R remarque que ce protocole a paradoxalement facilité les échanges informels entre les deux services publics. Ces échanges informels ont inquiété le Comité R qui met en garde sur la perte des renseignements lors de tels échanges. Ce protocole d'accord prévoit d'échanger des informations à propos des personnes liées au terrorisme, au radicalisme, à l'ingérence, à l'anarchisme, à l'extrême droite ou gauche, et aux organisations sectaires nuisibles. L'échange se fait autant de la Sûreté vers les directeurs de prisons pour qu'ils puissent prendre des mesures de sécurité adéquates, que l'inverse. En outre, il offre à la Sûreté un accès direct à la base de données « SIDIS Suite » de l'administration pénitentiaire. Cette base de données contient, entre autres, l'identité des visiteurs de la prison et leurs numéros de téléphone. Enfin, il prévoit une formation, dispensée par la Sûreté, des agents pénitencier afin qu'ils soient capables de reconnaître les signes de radicalisation.<sup>300</sup>

Ce protocole aurait contraint les professionnels de la Sûreté et de l'administration pénitentiaire à se parler, malgré des réticences de la part de certains directeurs de prison. A cette occasion, la plupart des directeurs de prison ont reçu une habilitation de sujet afin de pouvoir acquérir des informations classifiées de la part de la Sûreté. Une fois ce processus enclenché, chacun y aurait trouvé son intérêt ce qui a entraîné un rapprochement entre les deux services. Un membre de la Sûreté insiste sur l'utilité et l'efficacité des réunions entre les services, les directeurs de prison, les polices locale et fédérale. Cet échange permet à la Sûreté de savoir si un individu est radicalisé ou s'il radicalise d'autres personnes et de connaître la date de sortie de tels individus. Le risque est de voir une personne détenue, peu importe la raison, se radicaliser lors de sa détention. Dans ce cas, la Sûreté n'a pas de moyen aussi efficace que les agents pénitentiaires pour

---

<sup>300</sup> Comité R, « Rapport d'activité du Comité R 2016 ». op. cit. p. 59-62.

détecter les individus radicalisés. Ainsi, le service de renseignement peut mettre en place une surveillance lors de leur libération.<sup>301</sup>

Concernant le SGRS, il n'a aucun lien particulier avec l'administration pénitentiaire. Ce n'est pas étonnant puisqu'il a pour mission la gestion des menaces liées à la Défense nationale.

L'accord entre la Sûreté de l'Etat et l'administration pénitentiaire est utile. La formation des agents pénitentiaires permettant de détecter un individu radicalisé est la première étape d'une bonne gestion du phénomène de radicalisation en prison. En effet, il est impossible de gérer une problématique si elle n'est pas reconnaissable. Ensuite, les agents pénitentiaires agissent comme des détecteurs pour la Sûreté de l'Etat. Alors que la Sûreté de l'Etat peine à remplir ses missions avec ses moyens limités, tant humains que financiers, ces détecteurs lui permettent de mieux adapter ses ressources afin de surveiller les individus dangereux. Auparavant, la Sûreté ne savait pas qui suivre ni qui laisser tranquille à sa sortie de prison. Ce protocole d'accord permet d'établir quels individus doivent être suivis en priorité. Enfin, la Sûreté de l'Etat pourrait empêcher un attentat prévu par un ancien détenu radicalisé fraîchement libéré. Cette hypothèse n'est pas une fiction au vu de l'affaire de l'attentat de Liège perpétré en mai 2018. En surveillant les anciens détenus présentant un risque, la Sûreté de l'Etat endosse un rôle préventif qui est celui pour lequel elle a été créée. Néanmoins, il serait judicieux de ne pas se reposer uniquement sur un service de renseignement pour éviter un drame, mais de coupler ces mesures avec un accompagnement plus adapté des individus radicalisés lors de leur libération en vue d'une réinsertion réussie.

#### *IV.2.3. La relation entre les services de renseignement et le FOREM*

Après leur sortie de prison, certains individus sont suivis afin qu'ils participent aux formations offertes par le FOREM et qu'ils trouvent un emploi. Il se peut que certains individus radicalisés soient détectés par ce biais. Il a été révélé qu'un ancien détenu radicalisé s'est vu renvoyé car il prêchait son idéologie au sein d'une entreprise qui l'avait embauché par l'entremise du FOREM. Cette information est remontée à un directeur régional du FOREM et elle a pu être transmise à la Sûreté de l'Etat, grâce à un protocole d'accord entre ces deux institutions. Si l'exemple expose le cas d'un ancien détenu, rien

---

<sup>301</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

n'empêche un employé du FOREM de transmettre une information sur une personne n'ayant jamais eu affaire à la justice.<sup>302</sup>

A l'instar du protocole de coopération avec l'administration pénitentiaire, celui entre le FOREM et la Sûreté de l'Etat permet d'enclencher de nouveaux « détecteurs » que sont les accompagnateurs du FOREM. L'exemple démontre que lors de certains accompagnements, les employés du FOREM peuvent acquérir des informations utiles au renseignement belge. Si aucune procédure n'existe pour remonter l'information, celle-ci risque de se perdre faute de trouver le bon destinataire, tandis que la coopération permet la récupération des informations par les services de renseignement.

#### *IV.2.4. La relation entre les services de renseignement et les autres services publics*

Sans autre information plus précise, il a été révélé que la Sûreté et le SGRS ont convenu un protocole d'accord avec, respectivement, la CTIF et le CGRA.

De son côté, la Sûreté de l'Etat a conclu des protocoles de coopération avec : l'Inspection sociale, la Direction générale de l'Exécution des peines et des mesures, l'Office des Etrangers, l'Ecole Royale Militaire, l'Administration flamande de l'Enseignement, les services patrimoniaux, et la Banque Nationale de Belgique. Elle collabore aussi avec les CPAS et le service des douanes, mais aucun protocole n'est signé.

Concernant les Services publics fédéraux, des employés de la Sûreté ont leurs bureaux au ministère des Affaires étrangères, et aux cabinets des ministres de la Justice et de l'Intérieur. Quant au SGRS, son dirigeant rencontre régulièrement le Ministre de la Défense nationale et il dispose d'un point de contact aux Affaires étrangères. Les deux services sont très satisfaits de la collaboration avec le ministère des Affaires étrangères. Celui-ci aurait mieux compris l'utilité et la manière dont les services de renseignement fonctionnent.

Dans le cadre des relations entre les services de renseignement et les services publics, la question des habilitations est centrale. Les protocoles d'accord de coopération sont essentiels afin de faciliter l'échange entre deux administrations, mais aucune information ne circule si le destinataire ne possède pas une habilitation de niveau égal à la classification de celle-ci. En d'autres termes, plus il y a d'habilitations, plus il est possible d'échanger de l'information.

---

<sup>302</sup> Ibidem.

Les habilitations sont soumises au préalable à une enquête de sécurité. Celles-ci permettent de s'assurer de la fiabilité d'une personne. Elles agissent comme un premier filtre et empêchent que des informations tombent entre les mains d'une personne mal intentionnée. Certaines personnes issues de l'OCAM et des services de renseignement sont plutôt favorables à l'augmentation des habilitations de sécurité afin que ces destinataires puissent utiliser de manière concrète l'information reçue. Néanmoins, elles pointent les problèmes de la surcharge de travail et du manque de culture sécuritaire en Belgique.

L'enquête de sécurité est un processus qui impose une charge importante de travail qui s'étend sur plusieurs mois. L'explosion de leur nombre vient s'ajouter aux missions de renseignement<sup>303</sup>. Cela a pour effet de réduire les capacités opérationnelles des services de renseignement qui se plaignent déjà des faibles moyens dont ils disposent.

Les personnes détenant une habilitation de sécurité doivent développer une culture de la protection du secret. En effet, une habilitation de sécurité, c'est aussi l'obligation de protéger l'information reçue. C'est pour cette raison qu'il est fondamental que les personnes habilitées soient les mêmes que celles qui vont utiliser l'information. Le risque est de voir des responsables sous-traiter des dossiers confidentiels à des personnes de leurs administrations dont la fiabilité n'aura pas été vérifiée.<sup>304</sup>

Au plus il y a de personnes habilitées à recevoir une information, au plus celle-ci risque de fuir. Certains services de police ont fait preuve de négligence à cet égard en divulguant des éléments d'enquêtes terroristes à la presse. Evidemment, ce genre de fuite met en péril toute une enquête judiciaire.<sup>305</sup>

Le principe du « need to know » permet de limiter une dissémination trop large des données confidentielles et ce principe doit être appliqué avec la plus grande rigueur afin d'éviter de mettre à mal une affaire judiciaire.<sup>306</sup>

Les habilitations et le principe du « need to know » servent la protection du secret, mais cela ne semble pas suffire. Ces deux modalités doivent être soutenues par une culture du

---

<sup>303</sup> Entretien avec un membre de l'OCAM, juillet 2018.

<sup>304</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>305</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme.

<sup>306</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

secret. Les personnes possédant de telles informations ne peuvent pas prendre à la légère la sécurité de celles-ci.

#### *IV.2.5. L'implication des services de renseignement dans les plateformes de concertation*

Les services de renseignement participent aux TFL, mais ne sont pas présents lors des rencontres des CSIL. Néanmoins, il existe un lien entre ces deux plateformes. De ce fait, il est difficile de présenter l'une sans l'autre, et il est même intéressant de peser les avantages et désavantages qui existent à faire collaborer les services répressifs avec les professionnels de la prévention.

#### *Les Task Force Locales (TFL)*

Les TFL sont vues d'un très bon œil par les praticiens du renseignement. La présence des services de renseignement, des polices fédérale et locales, ainsi que du parquet permettent aux professionnels de la sécurité de se rencontrer une fois par mois et d'apprendre à se connaître. D'après eux, ce rapprochement sur le terrain est bénéfique à la circulation des informations.<sup>307</sup>

Concrètement, chaque service va partager ce qu'il sait à propos d'une personne radicalisée afin de réaliser la « cartographie » de l'individu. Par exemple, si une personne sort de prison, la Sûreté va donner son avis sur son degré de radicalisation, le parquet et la police judiciaire présenteront les raisons de sa condamnation, et la police locale pourra éclairer ses partenaires sur son environnement social ou familial. Suite à cette concertation, les membres des TFL élaborent un suivi adapté. Ce suivi peut être pris en charge par la police locale qui aura un rôle plutôt préventif afin que la personne ne retombe pas dans la délinquance. Dans ce cas, la personne radicalisée doit accepter de faire l'objet d'un suivi. En effet, l'individu ayant purgé sa peine, il n'est pas tenu de rendre des comptes que ce soit à la police locale, fédérale ou aux services de renseignement. Les TFL se concertent aussi à propos des personnes repérées comme radicalisées par des comportements suspects ou par l'expression de propos excessifs. Il en est de même pour les personnes libérées sous conditions. Dans ce dernier cas, le suivi des TFL vient s'ajouter aux conditions imposées à leurs libérations. L'addition de ces mesures peut paraître excessive pour les personnes recouvrant leur liberté. Les TFL permettent de trouver un équilibre et de réduire l'impact invasif de ces différentes mesures.<sup>308</sup>

---

<sup>307</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>308</sup> Entretien avec P. Somers, substitue du procureur du Roi au parquet fédéral, juillet 2018.

### Les Cellules de sécurité intégrale locale (CSIL)

Si certains praticiens du renseignement ne sont pas convaincus de l'utilité des CSIL, ils ne le sont absolument pas quant à l'obligation des CSIL dans chaque commune. Les CSIL peuvent être utiles dans les grandes villes, mais elles perdent leurs sens dans les communes situées hors des agglomérations. De plus, ces mêmes personnes ont peur de créer un service qui ferait le même travail préventif que les polices locales<sup>309</sup>.

Outre la question de l'efficacité des CSIL, la réunion des travailleurs sociaux et d'un officier de police amène à se demander si c'est une si bonne idée de faire travailler les mondes préventif et répressif ensemble. Selon certains professionnels de la sécurité, il est nécessaire d'établir un lien entre la structure répressive et préventive. Il faut qu'il y ait un passage de flambeaux entre l'action socio-préventive et répressive lorsque la menace s'aggrave. Il doit exister car le risque est tel qu'il est important de sévir si besoin<sup>310</sup>. De plus, ce lien permet de créer une approche plus efficace.

Les services préventifs permettent aux proches d'une personne en cours de radicalisation de se tourner vers eux pour trouver de l'aide. Si ces proches se tournent vers les services préventifs, c'est justement parce que ces derniers offrent d'autres solutions que la répression. Dès lors, rapprocher les professionnels de la prévention et de la répression peut être contre-productif. Certains pourraient y voir une complicité entre la police et les travailleurs sociaux. Dans ce cas, se tourner vers les services préventifs ne représenterait plus une option pour les proches des personnes dans le besoin d'une aide sociale. Cela aurait pour conséquence que les travailleurs sociaux seraient moins sollicités pour aider des personnes en difficulté. Afin d'éviter ce scénario, il est préférable de distinguer très clairement le travail des services préventifs de ceux de la sécurité et de faire confiance aux professionnels de la prévention pour transmettre une information capitale si un danger se présente. En Belgique, la répression et la prévention ne forment pas qu'un, bien que les CSIL soient un premier pas allant dans ce sens, justifié par la menace terroriste.

A contrario, la réunion des acteurs sociaux et de l'officier de police de la TFL peut permettre aussi d'élaborer une meilleure approche des personnes dans le besoin. En effet, le rôle pivot de l'officier de police qui participe à la fois à la TFL et à la CSIL permet aussi d'informer les acteurs sociaux de l'environnement dangereux d'une personne

---

<sup>309</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>310</sup> Entretien avec un membre de l'OCAM, juillet 2018.

radicalisée. En effet, il arrive parfois que la CSIL demande à la Sureté de l'Etat une information ou un avis sur un individu<sup>311</sup>. Ces informations pourront aider les assistants sociaux à mieux comprendre et aider l'individu. En d'autres termes, si le risque de radicalisation est trop grand, la CSIL permet d'avertir les services de sécurité. Inversement, les TFL peuvent permettre aux services sociaux d'élaborer une meilleure approche envers une personne radicalisée.

Il est possible de créer une collaboration saine entre la structure répressive et la structure préventive. C'est le rôle de l'officier de police désigné comme l'« *information owner* ». Ce dernier doit entretenir une relation de confiance entre les services de la prévention et de la répression. Un exemple est de ne pas enclencher systématiquement une réaction répressive sur base d'une information provenant d'un service social. Si cette confiance existe, chacun pourra travailler, de son côté, en disposant de plus d'informations et, ainsi, mieux accomplir sa tâche.<sup>312</sup>

Le politique a tranché : les CSIL deviennent obligatoire. Certaines communes ont refusé de créer des CSIL alors qu'elles comprenaient des personnes fortement radicalisées sur leur territoire<sup>313</sup>. C'est sûrement pour cette raison que le politique a forcé le pas pour toutes les communes.

#### IV.3. L'échange d'informations au niveau international en pratique

Ce mémoire est centré sur les liens nationaux qui existent entre les différentes administrations et les services de renseignement. Cependant, un service de renseignement n'est efficace que s'il entretient des relations avec ses homologues étrangers. D'ailleurs, la loi belge oblige les services de renseignement à tisser des liens sur le plan international. Ces collaborations sont nécessaires à la Belgique et elles posent certaines interrogations. En effet, la règle du tiers service est inscrite dans la loi belge, mais le principe de tiers pays s'immisce dans les débats nationaux. Pour ces raisons, un premier point situera le renseignement belge sur l'échiquier international et un second point détaillera les implications du principe du tiers pays.

---

<sup>311</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>312</sup> Ibidem.

<sup>313</sup> Ibidem.

#### *IV.3.1. Les relations des services de renseignement belges avec leurs homologues étrangers*

A l'instar de la diplomatie, les relations entre les services de renseignement belges entretiennent des relations avec leurs homologues étrangers selon deux modalités : le multilatéralisme et le bilatéralisme.

De manière générale, les services de renseignement belges ont toujours été perçus comme des services collaborant. Néanmoins, La Belgique pourrait obtenir bien plus d'informations de partenaires étrangers, si elle produisait plus d'informations puisque le renseignement repose, entre autres, sur le principe du donnant-donnant<sup>314</sup>.

Concernant le multilatéralisme, la Belgique est présente entre autres au « Club de Berne », à l'Union Européenne et à l'Otan. Le « Club de Berne » est un forum d'échange entre les dirigeants des services de renseignement des pays de l'Union européenne, de la Norvège et de la Suisse<sup>315</sup>. Il ne s'agit pas d'échanges d'informations opérationnelles, mais plutôt d'un partage et d'une discussion autour des problématiques rencontrées par ces services. Quant à l'Union européenne et à l'OTAN, la Sûreté dispose d'un employé travaillant au sein de l'EU INTCEN et de l'Alliance Atlantique nord<sup>316</sup>.

Selon le Comité R, les relations bilatérales sont souvent plus efficaces que les réunions multilatérales. Bien qu'elles ne s'exposent pas au grand jour, même s'il est possible de dire que la Sûreté de l'Etat collabore avec des services venus d'une septantaine de pays différents<sup>317</sup>. Elle entretient de proches relations avec les pays limitrophes à la Belgique. Ainsi, une personne de la Sûreté est en place à la Direction générale de la sécurité intérieure (DGSI) à Paris, et elle mène régulièrement des discussions par écrans interposés avec les services de renseignement allemands et néerlandais<sup>318</sup>. En parallèle, il n'a pas été possible d'établir les relations qu'entretient le SGRS avec ses homologues étrangers.

#### *IV.3.2. Le principe du tiers pays*

Certains appellent à remplacer le principe du tiers service par celui du tiers pays. Ce principe induit que si un service de renseignement étranger communique une information

---

<sup>314</sup> Entretien avec G. Dallemagne, Député à la Chambre des représentants de Belgique et membre de la commission permanente de l'accompagnement du Comité permanent P et du Comité permanent R, juillet 2018.

<sup>315</sup> Lefebvre, Nicolas. « Les domaines de coopérations entre les services de renseignements et de sécurité européens en matière de lutte antiterroriste », (mémoire de master). Université catholique de Louvain, Louvain-la-Neuve, 2011. pp. 56-57.

<sup>316</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>317</sup> Comité R, « Rapport d'activité du Comité R 2016 ». op. cit. p. 30.

<sup>318</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

à un service de renseignement belge, ce dernier pourra la transmettre à n'importe quelle administration belge, sans devoir demander l'accord du service étranger.

Si le principe du tiers pays n'est pas encore la règle, cette conception est de plus en plus commune lors des échanges entre certains services, comme l'OCAM. Elle permet d'augmenter la rapidité des échanges, mais elle paraît mieux convenir à des services de police travaillant au plus proche de l'anti-terrorisme, alors que la règle du tiers pays se prête mieux à l'effort de contre-terrorisme déployé par les services de renseignement.<sup>319</sup>

Le principe du tiers pays permet d'échanger l'information de manière plus rapide que la règle du tiers service. C'est un fait, demander une autorisation à un autre pays et recevoir la réponse peut mettre du temps. Les partisans de la règle du tiers pays fondent leur raisonnement sur l'idée qu'aujourd'hui, les renseignements doivent être échangés rapidement afin d'entraîner des réactions opérationnelles rapides. Après tout, si un service de renseignement livre une information c'est qu'il attend que des mesures soient prises rapidement contre cette menace. Attention, il ne s'agit pas de la diffuser largement, mais bien de permettre à l'information d'opérer une réaction qu'elle soit politique, judiciaire, ou administrative.<sup>320</sup>

La règle du tiers pays ne convient pas aux relations de confiance nécessaire à la collaboration entre les services de renseignement. Les informations détenues par un service de renseignement sont une monnaie d'échange pour obtenir d'autres informations détenues par les services de renseignement étrangers. L'information est parfois très sensible et sa divulgation peut avoir des répercussions sur des vies humaines. Si elle est divulguée sans son accord, le service étranger sera moins enclin à fournir des renseignements. Le fait de demander au service détenteur de l'information si une partie, ou l'entièreté, de celle-ci peut être transmise et à qui, permet de conserver ce lien de confiance. En d'autres termes, les services de renseignement s'échangent plus d'informations qu'il n'en faudrait pour enclencher une réaction opérationnelle. Dès lors, la règle du tiers service protège cette confiance et intensifie le flux d'informations entre les services. En effet, les services de renseignement se gardent de partager une information, s'ils ne connaissent pas le destinataire final. De plus, le monde du

---

<sup>319</sup> Entretien avec un membre de l'OCAM, juillet 2018.

<sup>320</sup> Entretien avec G. Dallemagne, Député à la Chambre des représentants de Belgique et membre de la commission permanente de l'accompagnement du Comité permanent P et du Comité permanent R, juillet 2018.

renseignement est petit et si un service de renseignement venait à trahir la règle du tiers service, ses homologues étrangers en seront vite informés et les relations de confiance avec ces différents partenaires seraient impactées.<sup>321</sup>

La Belgique a la chance d'obtenir des informations primordiales de pays ayant plus de moyens qu'elle et produisant plus de renseignements. La quantité et la qualité des renseignements transmis par les services de renseignement sont telles que la Belgique ne peut pas risquer de limiter ce flux d'informations fondamental<sup>322</sup>. De plus, il est toujours possible de demander une déclassification d'une partie du renseignement afin de pouvoir l'utiliser de manière administrative ou judiciaire<sup>323</sup>.

#### IV.4. Conclusion sur l'échange d'informations

G. Dallemagne fait trois propositions afin d'améliorer la communication entre les services de renseignement et leurs partenaires proches. Tout d'abord, il faut moderniser et améliorer l'interopérabilité des banques de données. Ensuite, créer une banque de données entre plusieurs services pour permettre aux services de sécurité de disposer de plus d'informations. Enfin, assurer la présence d'officiers de liaison dans les différents services afin d'améliorer la communication entre les services<sup>324</sup>. Contrairement aux deux premières solutions, la dernière proposition permet d'établir un réel lien humain entre deux administrations. De cette manière, une relation de confiance peut s'établir entre les personnes et, plus largement, entre les services.

Les protocoles d'accord de coopération ne règlent pas tous les problèmes liés à l'échange d'informations. Il est impossible d'affirmer ou d'infirmer qu'une collaboration entre deux services est efficace sur la seule base de la signature d'un protocole. Les réunions obligatoires entre les services peuvent aussi être totalement infructueuses. Ce qui permet une véritable collaboration entre deux services, c'est la confiance qu'ils se font mutuellement, qu'ils soient des partenaires nationaux ou internationaux. Néanmoins, les protocoles, les plateformes de collaboration, les réunions, le transfert de personnel d'un

---

<sup>321</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>322</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme.

<sup>323</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

<sup>324</sup> Entretien avec G. Dallemagne, Député à la Chambre des représentants de Belgique et membre de la commission permanente de l'accompagnement du Comité permanent P et du Comité permanent R, juillet 2018.

service à l'autre, et toutes les autres modalités qui forcent les services à se rencontrer permettent de développer cette confiance. Si le politique veut instaurer un véritable échange d'informations, il doit amener les services publics, proches et moins proches des services de renseignement, à se rencontrer. Ainsi, ils pourront se connaître, comprendre le rôle de chacun et, enfin, se faire confiance.

Pour atteindre cet objectif, il est primordial de savoir qu'un service de renseignement fonctionne sur le principe du « nice to know »<sup>325</sup>. Le « nice to know » est ce réflexe qu'ont les membres des services de renseignement de récolter des informations aussi largement que possible, dans les limites de la loi. Souvent, ces informations n'ont pas d'utilité directe, mais parfois certains éléments se recoupent et leur rapprochement crée des renseignements. Il ne s'agit pas de faire de la rétention d'informations, mais de noter ce qui est entendu et dit, tout en sachant qu'il est possible que l'intérêt de cette information se révélera peut-être plus tard. Paradoxalement, lorsqu'un renseignement est créé, celui-ci est soumis à la protection du secret, qui comprend les principes d'habilitations, de classification et du « need to know ». Bien que les avis penchent de plus en plus pour une application du principe du « need to share », la culture du secret est intrinsèque aux services de renseignement qui ont besoin de rester dans l'ombre afin de protéger les intérêts supérieurs de l'Etat. C'est sûrement cette perception des services de renseignement, qui récoltent tout, mais qui se restreignent à partager leurs informations qui freinent les politiques et les administrations à se rapprocher de ces services.

---

<sup>325</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

## Chapitre V – L’utilisation des informations collectées par les services de renseignement

### V.1. L’utilisation politique des informations en pratique

L’utilisation des services de renseignement par le monde politique dépend de trois éléments. Le premier est la proximité qui lie ces deux acteurs. Si ceux-ci ne travaillent pas ensemble, il est peu probable que les services de renseignement aient leurs mots à dire en matière de sécurité. Le second élément est l’implication des services de renseignement dans les politiques sécuritaires. Au plus les services de renseignement s’impliquent dans l’élaboration des politiques de sécurité, au plus leur rôle dans l’Etat est important. Le troisième dépend du pilotage politique des services de renseignements qui doit les guider à atteindre des objectifs stratégiques.

#### *V.1.1. La proximité des politiques avec les services de renseignement*

Certains pensent qu’aujourd’hui les services de renseignement sont utilisés à bon escient par le politique<sup>326</sup>. Il y aurait eu une évolution positive dans les rapports entre les politiques et les services de renseignement ces dernières années. Elle peut être due à une meilleure connaissance des attentes des autorités politiques, dans la mesure où les dirigeants des services ont travaillé dans des cabinets ministériels, ou encore comme responsable d’un service public fédéral, ce qui n’a pas été toujours le cas<sup>327</sup>. L’évolution de la considération politique à l’égard des services de renseignement est illustrée par l’augmentation du budget de la Sûreté et du SGRS, bien que celle-ci ne soit pas jugée suffisante par tous.

Un autre avis estime que le renseignement sert suffisamment la politique belge aujourd’hui. Une association trop forte entre ces deux acteurs n’est pas souhaitable car le politique est guidé par une idéologie, alors que le renseignement doit rester neutre et défendre la démocratie. Cependant, il faut espérer que cette bonne utilisation des services de renseignement par le politique s’inscrive dans la durée, et ne soit pas juste un réflexe sécuritaire à la suite des attentats.<sup>328</sup>

---

<sup>326</sup> Entretien avec deux membres du SPF Affaires étrangères, août 2018.

<sup>327</sup> Entretien avec P. Pétry, Administrateur général adjoint de la Sûreté de l’Etat, août 2018.

<sup>328</sup> Entretien avec un membre de l’OCAM, juillet 2018.

D'autres dénoncent le manque de pilotage politique et de vision stratégique des services de renseignement belges<sup>329</sup>. Les disciples d'une collaboration plus étroite entre les services de renseignement et le politique doutent de la connaissance de ce dernier à-propos du fonctionnement des premiers. Selon eux, les politiques ne distinguent pas le sens des services de renseignement. Ils accusent l'appréhension avec laquelle les politiques abordent les services de renseignement d'être la cause de cette relation distante.<sup>330</sup>

Les avis divergent à propos de l'utilisation des services de renseignement par le politique. Cependant, tous s'accordent à dire qu'il y a un équilibre à trouver. Les services de renseignement doivent servir les intérêts sécuritaires de la nation, et non les intérêts politiques.

A partir de 2012, les services de renseignement belges ont transmis des notes à destination du politique pour les prévenir de la dangerosité des citoyens quittant le territoire national pour aller combattre en Syrie dans les rangs de l'Etat islamique<sup>331</sup>. Les « *returnees* » sont ces combattants qui ont acquis des capacités meurtrières et des convictions extrêmes revenus dans leur pays d'origine.

La proximité des services de renseignement avec le monde politique permet d'affronter un problème en temps et en heure avec l'expertise nécessaire pour en limiter les conséquences. Le phénomène des « *returnees* » est un exemple de l'importance de la proximité entre ces deux mondes.

Les attentats de 2014, 2015 et 2016 en France et en Belgique, ont particulièrement détérioré l'image de la Belgique sur la scène internationale car les terroristes avaient fomenté leurs projets dans ce pays<sup>332</sup>. Depuis, la Belgique a su redorer son image grâce à la gestion de la radicalisation. En effet, elle était un des premiers pays à identifier et à comprendre l'étendue de ce phénomène. Par la suite, d'autres pays qui ne se croyaient pas touchés ont eux aussi reconnu être impactés par le danger des « *returnees* » et, plus largement, de la radicalisation.<sup>333</sup>

---

<sup>329</sup> Entretien avec G. Dallemagne, Député à la Chambre des représentants de Belgique et membre de la commission permanente de l'accompagnement du Comité permanent P et du Comité permanent R, juillet 2018.

<sup>330</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>331</sup> Comité R, « Rapport d'activité du Comité R 2016 », op. cit. pp. 31-32.

<sup>332</sup> Entretien avec deux membres du SPF Affaires étrangères, août 2018.

<sup>333</sup> Ibidem.

Il y a fort à parier que le monde politique s'est tourné vers les services de renseignement, qui depuis quelques années avaient enrichi leur connaissance autour de cette problématique, afin de pouvoir faire face à cette situation. Cet exemple montre l'importance du rôle des services de renseignement auprès du politique. Ils sont là pour prévenir et conseiller, mais ils ne sont utiles que s'ils sont proches du gouvernement. C'est aussi ce qu'établit le cycle du renseignement. Le politique donne une direction aux services de renseignement qui vont leur livrer les informations récoltées sur les thèmes demandés.

La présence des officiers de liaisons de la Sûreté de l'Etat dans les cabinets des Ministres de l'Intérieur et de la Justice est un signe de proximité entre les services de renseignement et les autorités politiques.<sup>334</sup>

#### *V.1.2. L'implication des services de renseignement dans les politiques sécuritaires*

Au Ministère des Affaires étrangères, les contacts avec les deux services de renseignement sont quasi-quotidiens. Ce ministère est subdivisé en groupes de travail répartis selon des zones géographiques. Par exemple, il existe la cellule « Syrie-Irak », « Sahel » ou encore la « Black and white » qui s'occupe de l'Afrique centrale. Celles-ci se réunissent une fois par mois avec le SGRS et parfois avec la Sûreté de l'Etat. Un autre exemple est celui des « briefings » sur l'état d'une situation politique d'un pays que reçoivent les diplomates par la Sûreté et le SGRS. Ces deux exemples permettent au Ministère des Affaires étrangères et aux diplomates de connaître les revers d'une situation politique. De cette façon, les services de renseignement nourrissent le Ministère des Affaires étrangères qui élaborera sa politique en ayant le moins de zones d'ombres lors de sa prise de position politique.<sup>335</sup>

Outre cette implication, les services de renseignement sont parfois les entrepreneurs d'une politique en matière de sécurité grâce à la Task Force Nationale (TFN) et au Comité de coordination.

Le plan radicalisme institue les CSIL, les TFL et la TFN. Lorsque les acteurs de terrain des TFL remarquent un nouveau phénomène, un défaut dans le suivi des personnes radicalisées ou tout autre problème plus global se rapportant à la radicalisation, il le rapporte à la TFN. Cette dernière s'occupe de la problématique du radicalisme pour le

---

<sup>334</sup> Entretien avec Pascal Pétry, Administrateur général adjoint de la Sûreté de l'Etat, août 2018.

<sup>335</sup> Entretien avec deux membres du SPF Affaires étrangères, août 2018.

compte du Comité de coordination. Elle est divisée en groupes de travail qui ont pour objectif d'apporter des ajustements globaux par rapport aux soucis rapportés par les TFL. Ces groupes de travail sont singulièrement dirigés par un des services participant à la TFN, dont les services de renseignement, selon leurs expertises. Ainsi, ils peuvent proposer d'ajuster les circulaires ou les directives afin de mieux aborder le problème du radicalisme en Belgique. Les services de renseignement ne se contentent pas d'assister la TFN, mais ils ont participé à son élaboration et collaborent avec les autres services à son ajustement. De cette façon, les services de renseignement mettent leurs informations et leur expertise au profit d'une politique de sécurité ayant pour mission la lutte contre les vecteurs de la radicalisation en Belgique : le plan R.<sup>336</sup>

Le Comité de coordination, composé des différents acteurs de la sécurité et du renseignement belges, est un outil central qui permet aux services de renseignement de s'impliquer dans les politiques à mener en matière de sécurité. Il se réunit tous les mois. Contrairement à la TFN, cet organe ne s'occupe pas seulement de la radicalisation. Il est subdivisé en 11 groupes de travail qui sont tous dirigés par un service membre de ce comité. Par exemple, il y a le groupe de travail du « Potentiel économique et scientifique », ou encore « Plan national de renseignement ». Le groupe qui se penche sur la protection du potentiel économique et scientifique se doit d'élaborer des propositions politiques afin que le gouvernement puisse prendre des mesures pour protéger l'industrie nationale. Le « Plan national de renseignement » a pour mission de définir ce qu'est la sécurité nationale, ce qu'est le renseignement en Belgique et d'établir un état des lieux des relations qui existent entre les services de renseignement. Ce document permet aux acteurs politiques de comprendre le rôle des services de renseignement pour mieux les utiliser. Lorsqu'un dossier est assez mûr, le Comité de coordination le transmet au Comité stratégique qui aura un débat sur le projet. Ce dernier peut demander au Comité de coordination de revoir le projet ou de se concerter avec d'autres acteurs qui sont concernés par le plan politique, comme les entités fédérées, par exemple.<sup>337</sup>

La proximité des services de renseignement avec le ministère des Affaires étrangères, les cabinets des ministres de l'Intérieur et de la Justice et l'implication des services de renseignement dans l'élaboration des plans d'action en matière de sécurité démontrent qu'ils ont un rôle politique important. Il est probable que les attentats de 2014, 2015 et

---

<sup>336</sup> Entretien avec Pascal Pétry, Administrateur général adjoint de la Sûreté de l'Etat, août 2018.

<sup>337</sup> Ibidem.

2016 en France et en Belgique, aient poussé les politiques à prendre davantage en considération les services de renseignement. La structure politique à trois niveaux, (CNS, Comité Stratégique et Comité de coordination), couplée au Plan R, permet aux services de renseignement de proposer aux politiques des plans d'actions concrets visant à assurer la sécurité des intérêts de l'Etat. Dans le cadre du Plan radicalisme, les services de renseignement réagissent à un phénomène. Ils répondent à une nécessité.

### *V.1.3. Le pilotage politique des services de renseignement*

Les autorités politiques sont proches des services de renseignement et mettent à profit leurs informations pour élaborer leurs politiques de sécurité. Cependant, cela n'équivaut pas à un pilotage politique des services de renseignement. Ce pilotage passe par la définition des intérêts stratégiques. Ces services ont l'avantage d'apporter des informations susceptibles de protéger les intérêts à long-terme de l'Etat. Si la Belgique veut se protéger de l'ingérence d'un autre pays dans ses élections ou être un acteur incontournable sur l'échiquier internationale lors d'une problématique touchant l'Afrique centrale, il faut se donner les moyens aujourd'hui pour être prêt demain.

Après les attentats du 11 septembre 2001, l'attention politique s'est tournée vers l'extrémisme islamique. Le Plan Mosquée, ou Plan M, élaboré en 2002, était l'ainé du Plan R dont la première version est apparue en 2004. En 2015, ce dernier a été révisée suite à la neutralisation de la cellule terroriste de Verviers.<sup>338</sup>

L'élaboration du Plan R avant les attentats de 2001, ou, du moins, sa révision en 2012, lorsque la Sûreté de l'Etat envoyait les premières alertes de la dangerosité de la radicalisation, aurait été stratégique. Elle aurait été une politique de « prévision ». Le Plan R est une politique de prévention en réaction à certains événements pour éviter d'autres drames. Le pilotage politique des services de renseignement aurait été de prévoir la possibilité que ces drames arrivent et de mettre en œuvre une stratégie pour les éviter. La prévision et la planification de la stratégie pour atteindre un objectif se fait grâce aux informations des services de renseignement. C'est le principe du cycle du renseignement. D'abord, les informations servent les autorités politiques à prévoir les risques et les opportunités. Ensuite, les politiques définissent, à l'aide de ces informations, les objectifs stratégiques qui vont cadrer le travail des services de renseignement. Enfin, le cycle recommence.

---

<sup>338</sup> SPF Intérieur, « Plan R The action plan against radicalism », 2016. p. 6.

Il semble y avoir eu une évolution dans les rapports entre les autorités politiques et les services de renseignement. Ces derniers ont acquis une proximité nécessaire aux politiques et leurs informations sont utilisées par ceux-ci. Il faut que cette évolution s'incarne aussi dans le développement d'une vision à long-terme de ce que peuvent apporter ces services. Cette vision passe avant tout par la définition des objectifs stratégiques. Si la première version du « Plan national de renseignement » définit la sécurité nationale, il faut espérer que les prochaines versions définissent les intérêts stratégiques de la Belgique pour permettre le déploiement de véritable politique de « prévision », et non des politiques de prévention en réaction à des événements.

## V.2. L'utilisation judiciaire des informations en pratique

L'utilisation judiciaire des informations récoltées par les services de renseignement posent de nombreuses questions. Si la loi semble réglementer avec précision la relation entre les services de renseignement et les autorités judiciaires, la pratique met à jour que la relation est plus complexe que ce que la loi prévoit. Ensuite, certaines questions, comme la dénonciation d'infractions constatées par les agents du renseignement lors de leur enquête, le témoignage anonyme par ces mêmes agents et l'utilisation des preuves illégales récoltées par les services de renseignement, méritent un débat de fond avec l'avis des professionnels du secteur.

### *V.2.1. L'équilibre entre l'enquête de renseignement et l'enquête judiciaire*

Le Comité R s'est inquiété du travail qu'effectuent les services de renseignement pour les autorités judiciaires en temps de crise<sup>339</sup>. Plus largement, il s'oppose à ce que les services de renseignement engagent leurs capacités dans des « *missions purement judiciaires* »<sup>340</sup>. L'administrateur général adjoint de la Sûreté de l'Etat, lui, exclut un transfert de la charge de travail entre la police et son service. La Sûreté ne doit pas être une solution à la surcharge de travail de la police fédérale. Il est d'avis que le choix qui doit s'opérer entre l'enquête judiciaire ou de renseignement doit être pensé selon deux éléments. D'une part, ce choix doit dépendre des finalités intrinsèques aux différents services. S'il s'agit de mener les auteurs d'une infraction devant les tribunaux, ce sera le travail de l'autorité judiciaire. S'il est question de mettre fin à une menace, les services de renseignement

---

<sup>339</sup> Comité R, « Rapport d'activité du Comité R 2016 ». op. cit. pp. 43-44.

<sup>340</sup> Ibidem. p. 51.

seront plus à même de trouver une solution puisqu'ils peuvent rediriger leurs actions vers d'autres autorités, telles que politiques ou administratives. D'autre part, ce choix doit se baser sur les capacités des différents services à atteindre la finalité privilégiée.<sup>341</sup>

Si la police judiciaire met la main sur des films photographique ayant servi à la production d'innombrables faux papiers lors de l'arrestation de l'individu les fabriquant, le parquet pourrait nommer un service de renseignement comme assistant technique. En effet, dans ce cas, il n'est pas nécessaire que la police judiciaire exploite l'ensemble du contenu de ces films pour constater l'infraction. La Sûreté de l'Etat, elle, pourrait s'intéresser à ces personnes afin de, soit rediriger l'information vers un service de police, soit vers un autre service qui en aura une utilité administrative.<sup>342</sup>

Cet exemple théorique démontre qu'un service de renseignement a un spectre bien plus large que l'unique finalité judiciaire. La police n'est qu'un des destinataires des informations récoltées par les services de renseignement. Si la menace terroriste est une priorité pour les services de renseignement, il y a un risque que de nombreuses enquêtes de renseignement se muent en enquêtes judiciaires puisque cette menace est punie pénalement. L'enquête de renseignement visant une affaire d'espionnage, d'ingérence ou de protection du potentiel économique et scientifique a, quant à elle, peu de chance de se retrouver dans les mains de la police.

Si la loi oblige les services de renseignement à rapporter les infractions qu'ils observent dans le cadre d'une mission, ce n'est pas pour autant que le parquet se sert de ces services de renseignement comme d'un service de police.

Tout d'abord, le parquet, les services de police et de renseignement se concertent, et ce sans doute à un rythme plus fréquent que par le passé<sup>343</sup>. A ce titre, la Commission des attentats prévoit d'établir un « *Joint decision centre* » dans chacun des cinq arrondissements de la police judiciaire spécialisé en terrorisme. Ces cellules prévoient des réunions hebdomadaires entre la police fédérale, les services de renseignement, l'OCAM et le parquet afin de décider de manière collégiale si une enquête doit être dans les mains du renseignement ou de l'autorité judiciaire<sup>344</sup>. La décision n'est pas prise de manière

---

<sup>341</sup> Entretien avec P. Pétry, Administrateur général adjoint de la Sûreté de l'Etat, août 2018.

<sup>342</sup> Ibidem.

<sup>343</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

<sup>344</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la

unilatérale par le parquet. Cette concertation permet de trouver le point d'équilibre entre le travail de renseignement et celui de la police avec l'accord de tous.

Par ailleurs, ce n'est pas systématiquement le parquet qui utilise les informations des services de renseignement, mais c'est parfois l'inverse. En effet, il arrive que les services de renseignement profitent qu'une enquête soit « déjudiciarisée » pour récolter des informations et nourrir leurs propres enquêtes<sup>345</sup>. C'est aussi le cas quand le parquet fédéral ouvre une enquête pour terrorisme. Dans ce cas, les services de renseignement sont nommés comme assistant technique. Ils ont accès aux dossiers et à de nombreuses informations qu'ils peuvent utiliser pour étoffer leurs propres renseignements<sup>346</sup>.

Ensuite, le parquet ne peut pas utiliser n'importe quelle information des services de renseignement. Il arrive qu'un service de renseignement alerte le parquet fédéral, mais sans pour autant transmettre une note déclassifiée. Dans ce cas-là, le parquet ne peut pas démarrer de procédures judiciaires. L'utilisation des services de renseignement dans une enquête judiciaire n'est pas forcément bénéfique au parquet. Par exemple, il est préférable que les écoutes téléphoniques s'opèrent dans une procédure judiciaire car celles-ci sont retranscrites dans des procès-verbaux sur base desquels les accusés pourront se défendre lors d'un procès. Les informations probantes des écoutes téléphoniques réalisées par les services de renseignement font l'objet d'une note générale qui a moins de force probante que le procès-verbal.<sup>347</sup>

Enfin, il se peut que deux enquêtes, l'une, de renseignement et l'autre, judiciaire, se déroulent en parallèle<sup>348</sup>. Dans ce cas, les services de police et de renseignement peuvent réaliser leur propre travail selon leur finalité. La Commission attentat a saisi la différence entre les finalités du renseignement et du judiciaire. C'est pour cette raison qu'elle admet la possibilité que deux enquêtes s'ouvrent pour atteindre deux objectifs différents. Dans un souci d'efficacité, elle souligne l'importance de recourir à cette possibilité seulement si cela s'avère nécessaire car deux enquêtes suscitent également deux fois plus de moyens<sup>349</sup>.

---

station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. p. 376.

<sup>345</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme, juillet 2018.

<sup>346</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

<sup>347</sup> Ibidem.

<sup>348</sup> Ibidem.

<sup>349</sup> Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la

Les travaux de renseignement et judiciaire poursuivent deux finalités différentes, mais qui parfois peuvent se rencontrer, surtout en matière de terrorisme. Le traitement d'une menace par le judiciaire n'est pas toujours la meilleure des solutions. Le renseignement permet de résoudre certaines menaces par des moyens politiques ou administratifs qui apporteront de meilleurs résultats. C'est pour cette raison que les services de renseignement et judiciaires doivent choisir ensemble la meilleure marche à suivre. Cette concertation permet de trouver un équilibre de complémentarité au lieu de mettre ces services en concurrence.

#### *V.2.2. La dénonciation d'une infraction par les services de renseignement*

Il est possible que la dénonciation de certaines infractions constatées par les services de renseignement soit postposée. Il peut y avoir plusieurs raisons à cela. Certaines infractions mineures sont parfois commises dans l'optique d'un projet ayant de plus lourdes conséquences. Si ces premières infractions n'intéressent pas les autorités judiciaires, alors il est préférable que les services de renseignement continuent leur enquête en rapportant des faits plus graves qui intéresseront le parquet par la suite. Parfois, une dénonciation rapide de l'infraction peut mettre en danger des techniques utilisées et mettre à mal une enquête complète. Le temps peut permettre de ne pas mettre en péril une enquête de renseignement et de nouveaux éléments peuvent corroborer les premières informations afin de ne pas dévoiler les techniques utilisées.<sup>350</sup>

Il apparaît que la loi qui oblige les services de renseignement ou tout fonctionnaire à rapporter la moindre infraction n'est pas aussi systématique que cela. La loi doit composer avec la vie de terrain. L'incapacité des parquets à poursuivre la moindre infraction et le risque que peut entraîner la dénonciation d'une infraction ne permet pas cette automaticité. C'est aussi pour cette raison que les « *Joint decision centres* » sont importants. Ils offrent une concertation entre les professionnels du terrain et les magistrats. Cette composition doit permettre d'assurer l'efficacité des services de sécurité tout en préservant l'Etat de certains abus dans le choix des infractions poursuivies ou non.

#### *V.2.3. Le témoignage d'un agent de renseignement en pratique*

En Belgique, le témoignage anonyme des officiers de police judiciaire est prévu, mais rien n'est prévu pour les agents du renseignement. Aujourd'hui, les services de

---

station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017. p. 377.

<sup>350</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

renseignement transmettent une note contenant leurs informations aux différentes parties d'un procès à propos d'une personne suspectée de terrorisme. Cette note n'est pas un élément probant suffisant, elle doit être corroborée par d'autres éléments de preuves. En effet, les notes des services de renseignement orientent de manière efficace les enquêtes menées par les autorités judiciaires, mais elles sont insuffisantes pour inculper quelqu'un. Le témoignage anonyme n'a d'intérêt que s'il apporte des éléments probants par rapport à la note. En France, l'homologue de la Sûreté de l'Etat, la Direction générale de la sécurité intérieure (DGSI), endosse un rôle à la fois de service de renseignement et de service judiciaire. Les agents de la DGSI peuvent témoigner sous anonymat complet car il leur arrive de constituer des dossiers judiciaires. Ce n'est pas le cas des services de renseignement belges. Ces derniers orientent le travail du parquet et des services de police, et souvent avec succès, mais ils ne constituent pas eux-mêmes des dossiers judiciaires. Dès lors, le témoignage anonyme d'un agent du renseignement belge n'aura pas de plus-value par rapport à la note qui émane de la direction de son service et il n'y a donc pas d'intérêt à mettre en place cette possibilité.<sup>351</sup>

#### *V.2.4. L'utilisation des preuves illégales en pratique*

L'hypothèse de l'utilisation d'une preuve illégale récoltée par les services de renseignement semble très théorique pour deux raisons.

La dernière modification de la loi sur les méthodes de recueil de données est basée sur l'expérience de la mise en place de plus de 4000 méthodes. La loi semble en parfait accord avec les capacités de la Sûreté de l'Etat. Les procédures administratives sont aussi adaptées afin de ne pas entraver ou empêcher la mise en place de telles mesures. Les services de renseignement n'ont aucun intérêt à ne pas respecter les règles puisque celles-ci leur permettent de réaliser leurs tâches convenablement. Il peut arriver qu'il y ait un défaut de procédure, comme une date ou une signature manquante. Si la méthode mise en place est suspendue ou annulée, les services de renseignement ont la possibilité de rectifier le tir ou de soumettre une nouvelle demande de mise en place d'une méthode sans défaut.<sup>352</sup>

La seconde raison avancée est que le Comité R empêche que des preuves illégales soient utilisées contre un justiciable<sup>353</sup>.

---

<sup>351</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme, juillet 2018.

<sup>352</sup> Entretien avec P. Pétry, Administrateur général adjoint de la Sûreté de l'Etat, août 2018.

<sup>353</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

Cependant, certains se demandent comment ils pourraient savoir qu'une méthode est illégale ou irrégulière<sup>354</sup>. D'autres doutent de la capacité de la Commission BIM à contrôler la régularité de toutes les informations par les méthodes entreprises par les services de renseignement<sup>355</sup>.

Il arrive que des enquêtes judiciaires soient ouvertes sur la base d'une note d'un service de renseignement. Ces notes ne font pas état du cheminement de l'information, mais simplement d'un renseignement essentiel pour orienter le travail judiciaire. Elles sont brèves et laconiques. Si ce renseignement est le fruit d'un recoupement entre plusieurs informations, dont une proviendrait d'une méthode illégale ou irrégulière, il est difficile de faire abstraction de cette information.<sup>356</sup>

L'utilisation d'un élément récolté de manière illégale semble impossible compte-tenu de la destruction des données ordonnée par le Comité R. Bien que cette hypothèse ne soit que théorique, elle a été soulevée par le Comité R. Dès lors, il serait utile de prévoir les effets de cette hypothétique situation, si un jour elle se présente. La question des conséquences sur l'utilisation judiciaire d'un renseignement provenant d'une méthode de renseignement contenant une erreur de procédure reste plus floue. En d'autres termes, il faut savoir si une enquête judiciaire peut s'ouvrir sur base d'informations fournies par une méthode de renseignement dont la procédure est imparfaite. Il serait utile de clarifier les conséquences de telles erreurs.

### V.3. L'utilisation administratives des informations en pratique

Si l'OCAM peut requérir des mesures de retrait de carte d'identité, de passeport ou de gel des avoirs envers un individu non privé de liberté, il ne fait aucun doute que ces réquisitions sont fortement appuyées par les services de renseignement<sup>357</sup>. Dès lors, il faut se demander pourquoi la loi a alloué cette compétence à l'OCAM et pas directement aux services de renseignement. Il existe deux raisons complémentaires à cela.

---

<sup>354</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme, juillet 2018.

<sup>355</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

<sup>356</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme, juillet 2018.

<sup>357</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

L'une avance que ces mesures ont été dévolues par le fait que le terrorisme est une menace extrême. Certains n'imaginent pas développer ce type de disposition pour d'autres menaces. Cette menace déstabilisatrice et spectaculaire pousse les autorités à développer des moyens plus ostentatoires. Ces mesures seraient une réponse proportionnelle à la menace existante.<sup>358</sup>

L'autre propose que l'OCAM service multidisciplinaire en charge de la menace terroriste et extrémiste, rassemble les informations des services d'appui et des services partenaires à propos des individus représentant une menace. En d'autres termes, il est le mieux placé pour savoir si un individu représente une menace ou non. Octroyer ces compétences à l'OCAM force la concertation entre les différents acteurs de la sécurité en Belgique et évite les abus qu'il pourrait y avoir s'il s'agissait d'un service uni-disciplinaire. De plus, seuls les individus présents dans la banque de donnée de l'OCAM peuvent faire l'objet de ces trois mesures. Il ne s'agit pas de soumettre un nom, mais un dossier est constitué afin de motiver la réquisition de l'OCAM. Pour toutes ces raisons, s'il fallait habilitier un seul service à détenir de telles capacités ostentatoires, il valait mieux que ce soit l'OCAM plutôt qu'un autre service uni-disciplinaire.<sup>359</sup>

D'un point de vue démocratique, ces mesures sont acceptables puisque la personne ciblée par ces restrictions a une possibilité de recours auprès des différentes instances ayant pris la décision (CNS, ministre de l'Intérieur ou des Affaires étrangères). Ces mesures sont des décisions administratives, et non de justice, car il s'agit de moyens de prévention.<sup>360</sup>

Il est essentiel que la décision de telles mesures soit prise en concertation avec les autorités judiciaires. Une personne faisant l'objet d'une enquête judiciaire peut fuir si elle apprend que ces restrictions sont prises à son encontre avant qu'elle soit privée de liberté. Dans ce cas, les mesures font l'effet inverse de celui qu'elles devraient avoir et mettent à mal le travail judiciaire.<sup>361</sup>

Il serait erroné de croire que ce sont les seules possibilités administratives indirectes des services de renseignement. Par exemple, les services de renseignement peuvent donner une information au Commissariat général des réfugiés et des apatrides (CGRA) qui

---

<sup>358</sup> Entretien avec G. Dallemagne, Député à la Chambre des représentants de Belgique et membre de la commission permanente de l'accompagnement du Comité permanent P et du Comité permanent R, juillet 2018.

<sup>359</sup> Entretien avec un membre de l'OCAM, juillet 2018.

<sup>360</sup> Entretien avec P. Somers, substitute du procureur du Roi au parquet fédéral, juillet 2018.

<sup>361</sup> Entretien avec un juge d'instruction chargé des affaires de terrorisme, juillet 2018.

prendra la décision de retirer ou d'accorder ou non la reconnaissance de la qualité de réfugié à un individu.<sup>362</sup>

Ces différentes possibilités, que ce soit avec l'aide de l'OCAM ou avec l'appui d'une administration, démontrent l'incapacité des services de renseignement à prendre directement des mesures et illustrent la philosophie des services de renseignement belges. Ceux-ci ne sont pas pensés pour agir de manière administrative, mais pour informer afin que d'autres instances puissent prendre les décisions adéquates.

#### V.4. Conclusion sur l'utilisation des informations

Les coulisses de l'utilisation politique et judiciaire des informations récoltées par les services de renseignements indiquent qu'il y a un contraste entre ce que prévoit la loi organique des services de renseignement et ce qui se passe réellement, sans que ce soit illégal pour autant, puisque ce rôle est institué par d'autres arrêtés.

La loi organique des services de renseignement prévoit que le SGRS conseille les ministres compétents en matière de sécurité et de défense, alors qu'aucun article comparable de cette loi n'est prévu pour la Sûreté de l'Etat. Bien que cette dernière dépende des ministres de l'Intérieur et de la Justice, aucun article n'aborde le rôle qu'elle doit endosser par rapport à l'élaboration de politiques de sécurité. Néanmoins, les arrêtés royaux qui instituent le Conseil national de sécurité, le Comité stratégique et le Comité de coordination du renseignement et de la sécurité prévoient ce rôle de « consultant » politique pour les deux services de renseignement, mais aussi pour la police, l'OCAM et les autres administrations présentes dans ces différents comités. Le rôle des services de renseignement belges va au-delà de sa mission de rechercher et d'analyser les informations relatives à une menace sur l'intégrité de l'Etat légiférée par la loi organique. Les services de renseignement sont de véritables acteurs dans l'élaboration des politiques de sécurité par leur participation à la TFN du Plan R et au Comité de coordination du renseignement et de la sécurité. Il leur arrive aussi de se limiter à informer le pouvoir politique non seulement fédéral, mais aussi local. La Sûreté de l'Etat avait tiré la sonnette d'alarme lorsqu'il est apparu que des investissements chinois dans le réseau de distribution électrique avaient des liens avec le parti communiste et les services de

---

<sup>362</sup> Entretien avec un membre de la VSSE et un membre du SGRS, juillet 2018.

renseignement chinois<sup>363</sup>. C'est cette mission de prévention qui est caractéristique d'un service de renseignement, en théorie. Sa participation dans l'élaboration des politiques de sécurité dépasse sa fonction d'informateur, mais reste dans sa mission de consultant. Les services de renseignement ne dictent rien, ils proposent. Ce sont les ministres qui décident de la politique de sécurité à mener.

L'analyse du cadre juridique de l'utilisation des informations par les autorités judiciaires a mis en exergue une forte primauté de la mission judiciaire sur la mission de renseignement. La pratique fait apparaître qu'aucune infraction ou danger n'est couvert par les services de renseignement ou les autorités judiciaires, mais que la priorité est donnée soit au renseignement soit au judiciaire suite à une concertation. L'objectif de cette concertation est de trouver la meilleure solution, politique, judiciaire, ou administrative pour mettre fin à une menace.

La loi n'habilite aucun service de renseignement à prendre directement des mesures de coercition administrative envers une personne et la pratique confirme ce fait. Néanmoins, lorsque les informations récoltées par les services de renseignement sont transmises aux bons destinataires, celles-ci peuvent avoir des conséquences administratives.

Les trois utilisations possibles des informations récoltées par les services de renseignement ne sont jamais prises directement par les services de renseignement belges eux-mêmes. Ce fait révèle que la réussite des services de renseignement belges dépend, entre autres, de l'action de leurs partenaires. Ces services décident de leurs priorités, des pistes qu'ils vont suivre, du moment auquel ils vont transmettre un renseignement, et entreprennent chaque jour des actions pour contrecarrer une menace. Cependant, ils ne sont pas le « bras opérationnel » par lequel la mesure coercitive sera mise en place afin d'arrêter une menace. La Sûreté de l'Etat et le SGRS récoltent et traitent tous les informations possibles et transmettent leur renseignement au moment opportun pour déclencher l'action de leurs partenaires afin de mettre fin à une menace. Comme aime le rappeler l'administrateur général adjoint de la Sûreté de l'Etat, leur rôle est de « *prévenir, conseiller, déranger* », du moins pour la Sûreté de l'Etat<sup>364</sup>.

---

<sup>363</sup> RTBF, « L'entrée des Chinois dans Eandis électrise la Flandre », le 27 septembre 2016. [En ligne] [https://www.rtbf.be/info/economie/detail\\_l-entree-des-chinoise-dans-eandis-electrise-la-flandre?id=9415107](https://www.rtbf.be/info/economie/detail_l-entree-des-chinoise-dans-eandis-electrise-la-flandre?id=9415107)

<sup>364</sup> Entretien avec P. Pétry, Administrateur général adjoint de la Sûreté de l'Etat, août 2018.

## Conclusions

La mission du SGRS et de la Sûreté de l'Etat est de produire des renseignements et de les transmettre à un destinataire approprié qui pourra agir afin de contrecarrer la menace existante. Ils sont des diffuseurs de renseignement.

Pour collecter des informations, il est essentiel que les services de renseignement disposent de « capteurs ». Ces « capteurs » sont mis en place par leurs propres soins, comme le recrutement des sources humaines, l'emploi des méthodes de recueils de données, ou par les liens qu'ils entretiennent avec les administrations nationales et avec leurs homologues étrangers. La multiplication de ces « capteurs » favorise l'obtention d'informations aux services de renseignement et leur permettront de les recouper pour créer des renseignements en plus grande quantité et de meilleure qualité.

Concernant l'utilisation de ces renseignements, les liens que nouent ces services avec différentes administrations sont tout autant importants que les liaisons qui permettent la multiplication des « capteurs ». Les renseignements ne sont efficaces que s'ils sont transmis à un destinataire qui saura en faire usage, puisque, ni le SGRS, ni la Sûreté n'a la capacité de prendre des mesures politiques, judiciaires ou administratives de coercition. Ils agissent par truchement d'autres autorités ou administrations partenaires.

Ces deux éléments démontrent que l'efficacité des services de renseignement belges tient uniquement à leurs liens avec les différentes administrations, autant pour la collecte que pour utiliser l'information. Toutes les personnes interrogées ont souligné que ces liens n'existent que sur la base de la confiance et de la connaissance de l'autre. Cela vaut tant pour les relations internationales, que pour les liaisons intra-nationales. Au niveau international, la règle du tiers service est garante de cette confiance. Les liens intra-nationaux dépendent de la connaissance du travail de l'autre. Il y a une méconnaissance du rôle et du travail des services de renseignement en Belgique. Plus largement, les personnes interrogées ont aussi pointé du doigt les nombreuses fuites d'informations signe du manque de culture sécuritaire en Belgique. Ces deux éléments entravent l'efficacité des services de renseignement belges. Les protocoles, les réunions, les plateformes de concertation et les officiers de liaison sont des outils qui permettent une meilleure connaissance et une confiance mutuelle.

Si cette recherche a permis d'améliorer la connaissance théorique des services de renseignement nationaux, elle a aussi mis à jour un contraste entre les moyens mis à disposition afin de contrer le terrorisme et ceux qui existent pour traiter les autres menaces. Le terrorisme est bien présent et phagocyte une grande part des capacités des services de renseignement. L'OCAM, les plateformes du Plan R (TFN, TFL, CSIL) le retrait de la carte d'identité, celui du passeport et le gel des avoirs sont tous des éléments constitutifs de la solution pour contrer la menace terroriste. Tous ces moyens mis en place ont l'avantage de traiter la menace terroriste avec une approche globale. Aucune structure multidisciplinaire n'a été mise en place pour neutraliser une autre menace. Ce dispositif anti- et contre-terroriste a été rendu possible par des motivations et des mesures politiques suscitées par la particularité de la menace terroriste, plus spectaculaire et déstabilisatrice pour l'opinion publique que les autres dangers.

Les politiques et les services de renseignement eux-mêmes pourraient s'inspirer des moyens de contre- et d'anti-terrorisme mis en œuvre afin de créer de nouvelles structures adaptées à la lutte contre d'autres menaces. Plus difficile qu'une fusion complète entre le SGRS et la Sûreté de l'Etat, ce sont de véritables synergies avec des multiples acteurs qu'il faut développer. L'objectif est d'accroître celles-ci entre les administrations chargées de la sécurité et celles qui sont la cible de certaines menaces afin d'assurer leur protection. Les services de renseignement pourraient tisser des liens toujours plus étroits avec les universités ou les industries belges pour améliorer la protection du potentiel économique et scientifique. L'implication de multiples acteurs permet l'augmentation de l'efficacité des services de renseignement et est le départ de la solution pour déjouer n'importe quel type de menace. Dès lors, il faut décloisonner le travail des services de renseignement afin d'enclencher une réelle approche globale de la sécurité. Seulement, cela n'est possible que s'il y a une véritable connaissance et une confiance établie entre les différents acteurs.

L'approche multidisciplinaire, l'échange et l'utilisation des informations prouvent que les services de renseignement doivent être interconnectés. Le développement de ces interconnexions est de la responsabilité des services de renseignement et des autorités politiques. Cependant, seul le politique peut piloter les services de renseignement. Si ce dernier veut développer des politiques de « prévision » au lieu d'élaborer de réagir à l'actualité, il doit fixer les intérêts stratégiques de la Belgique pour cadrer le travail de ses services de renseignement.

Ces dernières années, le gouvernement s'est borné à mettre en place des politiques de prévention en réaction à l'actualité. N'est-il pas temps de se tourner plutôt vers des politiques de « prévision » en matière de renseignement ?

## Bibliographie

### *1. Monographie*

Baud, Jacques. « Le renseignement et la lutte contre le terrorisme : stratégies et perspectives internationales ». Lavauzelle, 2005.

Chopin, Olivier, Oudet, Benjamin. « Renseignement et sécurité ». Armand Colin, 2016.

Cools, Marc, et al., eds. « 1915-2015 : Het verhaal van de Belgische militaire inlichtingen-en veiligheidsdienst. Maklu », 2015.

Cousseran, Jean-Claude, et Hayez, Philippe. « Leçon sur le renseignement ». Odile Jacob, 2015.

De Valkeneer, Christian-paul, « Manuel de l'enquête pénale ». Bruxelles, Editions Larcier, 2018.

Moutou, Hugues, Poirot, Jérôme. « Dictionnaire du renseignement ». Perrin, 2018.

Rousseaux, Xavier, and David Somer. « Pour une histoire de la Surêté de l'Etat en Belgique. Essai autour de 175 années de pénombre », 2005.

### *2. Articles scientifiques & doctrine*

Bulinge, Franck. « Le cycle du renseignement : analyse critique d'un modèle empirique », Market Management 2006/3 (Vol. 6). pp. 36-52.

Coosemans, Thierry. « L'Union européenne et le renseignement : perspectives de coopération entre les États membres ». GRIP, Groupe de Recherche et d'Information sur la Paix et la Sécurité, 2004.

Goossens, Franky. « Les missions et compétences des services de renseignement et de sécurité belges », Journal des tribunaux 6066, 2002. pp. 617-630.

Lasoen. L. Kenneth. « 185 years of Belgian security service », Journal of Intelligence History, 2016. pp. 96-118.

Leroy, Patrick. « La communauté du renseignement belge : essai de définition ». *Revue militaire Belge* 12, 2016. pp. 85-99.

Lefebvre, Stéphane. « The Belgians Just Aren't up to It": Belgian Intelligence and Contemporary Terrorism ». *International Journal of Intelligence and Counter Intelligence* 30.1, 2017. pp. 1-29.

Rapaille, Guy, Van Laethem, Wauter. « La nouvelle loi sur les méthodes particulières de renseignement : une révolution pour les services de renseignement belges ». *Revue de droit pénal et de criminologie* 91, no. 9, 2011. pp. 813-845.

Stans, David. « Le contrôle des services de renseignements belges : émergence d'une légitimité ». *Revue de la Faculté de Droit de l'Université de Liège*, 2010. pp. 373-384.

Van Laethem, Wauter. « L'organe de coordination pour l'analyse de la menace : une analyse ponctuelle ». *Virgiles. Revue du droit de police*, 2007/4. pp. 109-127.

Warusfel, Bertrand. « Contraintes juridiques et culture du secret, comme freins à l'échange de données de sécurité en Europe ». Intervention au colloque sur l'échange de données dans l'espace de liberté, de sécurité et de justice de l'Union européenne. CESICE, Université Grenoble-Alpes, 18 novembre 2016. [En ligne] [http://www2.droit.parisdescartes.fr/warusfel/articles/SecretEchangeDonnees\\_resumWarusfel1116.pdf](http://www2.droit.parisdescartes.fr/warusfel/articles/SecretEchangeDonnees_resumWarusfel1116.pdf) Consulté le 5 juin 2016.

### *3. Textes législatifs*

Code d'instruction criminelle.

Loi organique du contrôle des services de Police et de renseignement et de l'Organe de coordination de la menace du 18 juillet 1991.

Loi sur la fonction de police du 5 août 1992.

Loi organique des services de renseignement et de sécurité du 30 novembre 1998.

Loi relative à la classification et aux habilitations, attestations et avis de sécurité du 11 décembre 1998.

Loi relative à l'analyse de la menace du 10 juillet 2006.

Arrêté royal portant sur l'exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace du 28 novembre 2006.

Arrêté royal relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme du 28 décembre 2006.

Sénat de Belgique. « Projet de loi relative aux méthodes de recueil des données des services de renseignement et de sécurité ». Document législatif n° 3-2138/1. Le 21 mars 2007.

Arrêté royal portant création du Conseil national de sécurité du 28 janvier 2015.

Arrêté royal portant création du Comité stratégique et du Comité de coordination du renseignement et de la sécurité du 2 juin 2015.

Loi modifiant la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques du 10 août 2015.

Loi portant modification du Code consulaire du 10 août 2015.

Loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique du 29 janvier 2016.

Loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259bis du Code pénal du 29 janvier 2016.

Loi portant des dispositions diverses Intérieur. - Police intégré du 21 avril 2016.

Arrêté royal relatif à la banque de données commune « *foreign terrorist fighters* » du 21 juillet 2016.

Chambre des Représentants de Belgique, « Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste ». Doc 54 1752/008, le 15 juin 2017.

Arrêté royal relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er bis « de la gestion des informations » du chapitre IV de la loi sur la fonction de police du 23 avril 2018.

#### *4. Jurisprudence*

CEDH, 22 juillet 2003 et 27 octobre 2004, *Edwards et Lewis c. Royaume-Uni*

Cour constitutionnelle, arrêt n° 202/2004 du 21 décembre 2004.

Cour de cassation de Belgique, arrêt P.04.1528.F du 23 mars 2005.

Cour de cassation de Belgique, arrêt P.05.0119.F du 12 octobre 2005.

Cour constitutionnelle, arrêt n° 105/2007 du 19 juillet 2007.

Cour constitutionnelle, arrêt n°145/2011 du 22 septembre 2011.

#### *5. Mémoire*

Lefebvre, Nicolas. « Les domaines de coopérations entre les services de renseignements et de sécurité européens en matière de lutte antiterroriste », (mémoire de master). Université catholique de Louvain, Louvain-la-Neuve, 2011. pp. 1-95.

#### *6. Rapports d'activités, communiqués de presse et autres sources non-scientifiques*

Best, Richard A. Jr. « Intelligence Information : Need-to-Know vs. Need-to-Share ». Congressional Research Service, 6 juin 2011. [En ligne] <https://fas.org/sgp/crs/intel/R41848.pdf> Consulté le 5 juin 2018. pp. 2-3.

Central Intelligence Agency. « The Intelligence Cycle ». 2007. [En ligne] <https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html> Consulté le 1er juin 2018.

Central Intelligence Agency. « INTelligence: Open Source Intelligence ». 2010 [En ligne] <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html> Dernière mise-à-jour le 30 avril 2013, consulté le 11 mars 2018.

Christophe Lamfalussy, « La Sûreté et le SGRS ne se parlent pas assez ». La Libre Belgique, le 19 mai 2016. [En ligne] <http://www.lalibre.be/actu/belgique/la-surete-et-le-sgrs-ne-se-parlent-pas-assez-573caee735702a22d77d49a9>

Comité R. « FAQ : Quelles sont les méthodes ordinaires, spécifiques et exceptionnelles de recueil de données pour les services de renseignement ? ». s.d. [En ligne] <http://www.comiteri.be/index.php/fr/34-pages-fr/303-queelles-sont-les-methodes->

[ordinaires-specifiques-et-exceptionnelles-de-recueil-des-donnees-pour-les-services-de-renseignement](#) Consulté le 10 mars 2018.

Comité R, « Rapport d'activité du Comité R 1996 ». 1996. [En ligne] <http://www.comiteri.be/images/pdf/Jaarverslagen/1996%20fr.pdf>

Comité R, « Rapport d'activité du Comité R 2004 ». [En ligne] <http://www.comiteri.be/images/pdf/Jaarverslagen/2004%20fr.pdf?phpMyAdmin=97d9ae9d92818b6f252c014a4a05bdfb>

Le comité permanent R, « Avis du Comité permanent R relatif à l'avant-projet de loi relatif aux méthodes de recueil de données des services de renseignement et de sécurité ». 2006. [En ligne]

<http://www.comiteri.be/images/pdf/franstalig/Avis%20projet%20loi%20methodes%20recueil%20donnees%20services%20renseignement%20et%20securite.pdf>

Comité R, « Rapport d'activité du Comité R 2016 ». 2016. [En ligne] [http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag\\_2016\\_FR.pdf](http://www.comiteri.be/images/pdf/Jaarverslagen/Activiteitenverslag_2016_FR.pdf)

Comité R, « Avis du Comité permanent R sur l'avant-projet de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) », *Annexe E*, 2016. [En ligne] <http://www.comiteri.be/index.php/fr/publications/avis>  
Consulté le 15 mars 2018.

Division de l'évaluation Secteur des politiques du Canada, « Rapport d'évaluation : sécurité en établissement ». Dossier n° 394-2-95. Février 2015. [En ligne] <http://www.csc-scc.gc.ca/publications/005007-2015-fra.shtml> Consulté le 6 mars 2018.

OTAN : communiqué de presse, « Communiqué sur le sommet de Varsovie » (2016) 100, §70, publié le 9 juillet 2016. [En ligne] [https://www.nato.int/cps/fr/natohq/official\\_texts\\_133169.htm](https://www.nato.int/cps/fr/natohq/official_texts_133169.htm)

RTBF, « L'entrée des Chinois dans Eandis électrifie la Flandre », le 27 septembre 2016. [En ligne] [https://www.rtbf.be/info/economie/detail\\_l-entree-des-chinoise-dans-eandis-electrifie-la-flandre?id=9415107](https://www.rtbf.be/info/economie/detail_l-entree-des-chinoise-dans-eandis-electrifie-la-flandre?id=9415107)

SPF Intérieur, « Plan R The action plan against radicalism », 2016



Noirhomme

Sébastien

*« L'échange et l'utilisation des informations récoltées par les services de  
renseignement belges »*

Promotrice : Professeure Maria Luisa Cesoni

Comment et avec qui les services de renseignement belges échangent-ils les informations qu'ils récoltent ? A quelles utilisations ces informations sont-elles destinées ? C'est à ces questions que cette étude tente de répondre. Ce mémoire a la particularité d'être centré sur la Belgique, tout en abordant au second plan l'essentiel des échanges d'informations au niveau international. Ainsi, il s'intéresse aux relations qu'entretiennent les services de renseignement belges, d'une part, entre eux, et, d'autre part, avec les autres administrations du pays. Enfin, ce travail présente une analyse de l'utilisation des informations collectées par les services de renseignement, d'un point de vue politique, judiciaire et administratif.

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve (Belgique)  
**[www.uclouvain.be/criminologie](http://www.uclouvain.be/criminologie)**