Table des matières

Résumé exécutif

Contexte de la recherche

Ce rapport de recherche est produit dans le cadre du projet « Folks, Authorities and Radicalism: between polarization and social construction » (FAR) financé par la Politique scientifique fédérale (BELSPO) (contrat #BR/175/A4/FAR). Ce projet, coordonné par le Centre d'Étude de la Vie Politique (CEVIPOL) de l'Université Libre de Bruxelles (ULB), et mené conjointement par le Interculturalism, Migration and Minorities Research Centre (IMMRC) de la Katholieke Universiteit Leuven (KU Leuven) et la Direction Opérationnelle Criminologie de l'Institut National de Criminalistique et de Criminologie (INCC) a pour objectif principal de questionner la notion de 'radicalisation' en Belgique ainsi que d'examiner les politiques publiques développées par rapport à ce phénomène à partir d'un triple niveau d'analyse : macrosociologique, mésosociologique et microsociologique [1] . Chaque équipe étant responsable d'un axe de recherche.

En charge du volet microsociologique, l'INCC a développé celui-ci à travers trois grandes questions de recherche :

Question 1 : Quels sont les systèmes d'enregistrement au sein de l'administration fédérale qui consignent de l'information en lien avec la radicalisation et comment celle-ci circule-t-elle?

Question 2 : Quelles sont les caractéristiques individuelles ainsi que celles, le cas échéant, des épisodes pénaux (carrières criminelles) des personnes signalées comme radicalisées par les autorités publiques belges ?

Question 3 : Quel est le sens donné par les personnes signalées comme radicalisées à leur parcours d'engagement ? Et plus particulièrement, quels sont les effets de leur expérience avec les autorités publiques (ou le système d'administration de la justice pénale) sur leur devenir, notamment en termes d'engagement ou désengagement de la violence ?

Le présent rapport de recherche (intermédiaire) ne rend compte que des résultats de la première question de recherche dont l'objectif est de proposer une description de la manière avec laquelle des banques de données existantes ou de nouvelles banques de données ont été aménagées suite à la mise à l'agenda politique du phénomène de la radicalisation. Les banques de données considérées sont au nombre de six : (1) la Banque de données Nationale Générale (BNG), (2) la Banque de Données Commune (BDC), (3) la banque de données du Tribunal de Première Instance (TPI/MaCH), (4) la banque de données des Parquets et des

1 Davantage d'informations sont disponibles sur le site web de BELSPO : https://www.belspo.be/belspo/brain-be/themes_4_Strategic_fr.stm-

Greffes de la jeunesse (PJG), (5) le Casier Judiciaire Central (CJC), et (6) la banque de données des établissements pénitentiaires (SIDIS-SUITE).

Méthodologie

Ce document rassemble une information dispersée, souvent peu visible, afin de la rendre accessible aux lecteurs peu habitués à la complexité et la technicité de cette matière. Pour ce faire, l'équipe de recherche s'est appuyée sur l'analyse de la législation et de la littérature grise disponibles. Le matériel comprend des travaux parlementaires ainsi que des avis du Conseil d'État, de la Commission de Protection de la Vie Privée (CPVP)[2] et des organes de contrôle tels que l'Organe de Contrôle de l'information policière (COC[3]) et le Comité permanent des renseignements (Comité R[4]). Leur compréhension du sujet a également bénéficié de plusieurs échanges et discussions avec des acteurs clés du développement des bases de données étudiées.

Résultats

Deux constats prédominent dans les évolutions constatées : d'une part, une volonté de repérage et d'enregistrement de plus en plus précoce des suspicions de toute forme de radicalité et d'autre part, l'ambition de parvenir à un partage de l'information et des données entre un grand nombre de services (police, renseignement, judiciaire, mais également locaux et socio préventifs, etc.) ainsi qu'à une coordination de leurs actions sur la base du modèle de 'multiagency'.

La lutte contre le terrorisme qui, autrefois, était plutôt l'apanage des services de renseignement, a muté, au fur et à mesure de l'évolution de la menace et de ses manifestations, vers le développement de dispositifs de prévention impliquant l'ensemble des services belges concernés. Pour évaluer la menace et coordonner les actions de prévention, les services (et plus particulièrement l'OCAM) doivent pouvoir disposer de l'information disponible aux différents niveaux de compétence. À cette fin, de nombreuses plateformes de discussion et de concertation ont été mises en place tant au niveau local qu'au niveau fédéral (CSIL-R, TFL, TFN, Joint Decision Centers, etc.). Parallèlement, l'échange et le partage d'informations que chaque service enregistre pour assurer ses propres missions s'est développé. Cet objectif s'est traduit d'une part, par la mise en place de banques de données communes dans lesquelles chaque service réenregistre les données dont il dispose à l'égard des entités considérées comme présentant des signes de radicalisation (violente) et d'autre part, par l'élargissement des accès aux (banques de) données propres à certains acteurs.

Ce système, assurément utile aux services de renseignement, pose néanmoins question à plusieurs niveaux. On peut y voir notamment les risques que chacun, quelle que soit sa

2 Entretemps devenue l'Autorité de Protection des Données (APD).
3 https://www.organedecontrole.be/services-de-police.
4 http://www.comiteri.be/index.php/fr/comite-permanent-r.

mission initiale, devienne (ou soit perçu comme) un informateur (des services de renseignement); que les frontières entre les missions et les finalités des différents services soient oblitérées; que la donnée collectée soit utilisée à d'autres fins et avec d'autres conséquences que celles pour lesquelles elle avait été initialement et légalement enregistrée, etc.

Ces questions se révèlent avec d'autant plus d'acuité que la palette des comportements considérés par les différents acteurs comme indicateurs d'un risque dans le cadre de la prévention du terrorisme et de l'extrémisme pouvant mener au terrorisme est large et variée. Au niveau de la police administrative, les informations relatives aux personnes impliquées dans les activités d'un groupement ou un phénomène, politiquement épinglé comme représentant potentiellement un risque pour l'ordre public, sont enregistrées. Au niveau de l'OCAM, toute personne qui a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme mode d'action en Belgique est dorénavant enregistrée dès lors que, selon les critères établis (par l'OCAM), elle présente un risque accru de violence. Au niveau des établissements pénitentiaires, les détenus sont observés dans leur quotidien pour détecter d'éventuels signes de radicalisation ou de prosélytisme. Et si le législateur s'est abstenu, dans le respect de la convention européenne des droits humains, de condamner la radicalisation en tant que telle, il n'en demeure pas moins qu'à ce niveau également, la formulation des infractions terroristes dans le Code pénal, réfère de plus en plus à des comportements bien en amont d'un passage à l'acte.

À l'instar de ce qui se fait en matière de prévention en santé publique vis-à-vis de la pandémie de la Covid-19, les politiques publiques sont soumises à un travail d'équilibriste délicat dans la mise en place de mesures de traçage et de partage d'informations entre d'une part, l'intérêt de tous de prévenir le (l'extension du) phénomène, et d'autre part, l'intérêt de chacun de sauvegarder ses libertés de pensée, d'expression et de mouvement.

*

* *

Executive summary

Background to the research

This research report is produced within the framework of the project 'Folks, Authorities and Radicalism: between polarization and social construction' (FAR) funded by the Belgian Public Science Policy (BELSPO) (contract #BR/175/A4/FAR). It was coordinated by the Centre d'Étude de la Vie Politique (CEVIPOL) of the Université Libre de Bruxelles (ULB), and conducted jointly by the Interculturalism, Migration and Minorities Research Centre (IMMRC) of the Katholieke Universiteit Leuven (KU Leuven) and the operational directorate of the National Institute for Forensic Sciences and Criminology (INCC/NICC). The main objective of this project was to question the notion of 'radicalisation' in Belgium as well as to examine the public policies developed in relation to this phenomenon based on a three-level analysis: macrosociological, mesosociological and microsociological.[5] Each team was responsible for one research axis.
The NICC, in charge of the microsociological component, developed its research through three major research questions:

Question 1: What registration systems exist within the federal government that record information related to radicalisation and how is this information circulated?

Question 2: What are the individual characteristics as well as, if any, the characteristics of criminal episodes (criminal careers) of persons reported as radicalised by the Belgian public authorities?

Question 3: What meaning do those reported as radicalised give to their pathways of engagement? And more specifically, what effects do their experience with public authorities (or the criminal justice administration system) have on their future, especially in terms of engagement or disengagement from violence?

This (interim) research report only reports on the results of the first research question, which aims to provide a description of how existing or new databases have been developed as a result of the radicalisation phenomenon becoming part of the political agenda. Six databases are considered: (1) the General National Database (BNG/ANG), (2) the Common Database (BDC/GGB), (3) the Court of First Instance Database (TPI/REA/MaCH), (4) the Public Prosecutor's Office and Youth Registry Database (PJG), (5) the Central Criminal Record (CJC/CSR), and (6) the Prison Database (SIDIS-SUITE).

5 More information is available on the BELSPO website: http://www.belspo.be/belspo/brain-be/themes_4_Strategic_en.stm.

Methodology

This document brings together information that is dispersed and often barely visible in order to make it accessible to readers who are not used to the complexity and technicality of this subject. In order to do so, the research team relied on an analysis of the available legislation and grey literature. The material includes parliamentary works as well as opinions of the Council of State, the Commission for the Protection of Privacy (CPP)[6] and supervisory bodies such as the Supervisory Body for Police Information (COC[7]) and the Standing Intelligence Agencies Review Committee (Comiteri[8]). The team's understanding of the subject was also enhanced through several exchanges and discussions with key actors involved in developing the databases studied.

Results

Two observations predominate in the developments observed: on the one hand, a desire to identify and register suspicions of any form of radicalism at an increasingly early stage and, on the other hand, the ambition to be able to share information and data among a large number of services (police, intelligence, judicial, but also local and socio-preventive, etc.) and also to coordinate their actions on the basis of the 'multi-agency' model.

The fight against terrorism, which hitherto was the prerogative of the intelligence services, has evolved, in line with evolution of the threat and its manifestations, towards the development of prevention mechanisms involving all the Belgian services concerned. In order to assess the threat and coordinate preventive actions, the services (and more particularly the Coordination Unit for Threat Analysis - CUTA) must have access to the information available at the various levels of competence. To this end, numerous discussion and consultation platforms have been set up both at local and federal level (Local Integral Security Cells (CSIL/LIVC R), Local Task Force, National Task Force, Joint Decision Centres, etc.). At the same time, exchange and sharing have been developed of information recorded by each service records in carrying out its own missions. This objective has resulted, on the one hand, in the establishment of common databases in which each service re-registers the data it has on entities considered to show signs of (violent) radicalisation and, on the other hand, in extended access to the databases of certain actors.

This system, which is certainly useful to the intelligence services, nevertheless raises questions at several levels. In particular, this includes the risks that any service whatever its initial mission will become (or be perceived as) an informer (for the intelligence services); that the boundaries between the missions and purposes of the various services will be blurred;

6 In the meantime it has become the Data Protection Authority (DPA).
7 https://www.controleorgaan.be/en/.
8 https://www.comiteri.be/index.php/en/standing-committee-i.

that the data collected will be used for purposes and consequences other than those for which they were initially and legally recorded, etc.

These questions are all the more acute as there is a wide and varied range of behaviours considered by the different actors as indicators of risk in the context of the prevention of terrorism and extremism that could lead to terrorism. At the level of the administrative police, information is recorded concerning persons involved in the activities of a group or phenomenon, politically singled out as a potential risk to public order. At the level of the CUTA, any person holding extremist views that justify the use of violence or coercion as a mode of action in Belgium is now registered if, according to the criteria established (by the CUTA), they present an increased risk of violence. At the level of prisons, inmates are observed in their daily life to detect possible signs of radicalisation or proselytising. Furthermore, while legislators, in compliance with the European Convention on Human Rights, have refrained from condemning radicalisation as such, the fact remains that, at this level too, the formulation of terrorist offences in the Criminal Code increasingly refers to behaviour well upstream of an act.

Following the example of public health prevention in relation to the Covid-19 pandemic, public policies in the implementation of tracking and information-sharing measures are subject to a delicate balancing act between, on the one hand, the interest of all in preventing the (spread of the) phenomenon and, on the other hand, the interest of each individual in safeguarding their freedom of thought, expression and movement.

*

* *

Liste des abréviations et expressions spéciales utilisées dans ce rapport

AFIS	Automated Fingerprint Identification System
AGMJ	Administration Générale des Maisons de Justice
ANPR	Automatic number-plate Recognition
ANS	Autorité Nationale de Sécurité
APD	Autorité de Protection des Données
AR	Arrêté Royal
BEPAD	BEstuurlijke Politie – Police Administrative
BDC	Banque de Données Commune
BNG	Banque de données Nationale Générale
BPS	Bruxelles Prévention & Sécurité
Celex	Cellule Extrémisme (de la Direction Générale des Établissements Pénitentiaires)
CEDH	Convention Européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales ou Convention Européenne des Droits de l'Homme
CEP	Commission d'Enquête Parlementaire
CESL	Conseil d'État Section Législation
CIA	Carrefour d'Information de l'Arrondissement
CJC	Casier Judiciaire Central
CNS	Conseil National de Sécurité
COC	Controleorgaan (op de Politionele Informatie) / Organe de Contrôle (de l'information policière)
Comité P	Comité permanent de contrôle des services de Police
Comité R	Comité permanent de contrôle des services de Renseignement
CPG	Collège des Procureurs Généraux
CSIL-R	Cellule de Sécurité Intégrale Locale - Radicalisme
CT	Condamnés pour infraction Terroriste
CTIF	Cellule de Traitement des Informations Financières
CPVP	Commission de Protection de la Vie Privée
DAO	Direction des Opérations de Police Administrative
DG EPI	Direction Générale des Établissements Pénitentiaires
DJ-SOC	Direction centrale pour la lutte contre la criminalité grave et organisée
D-Rad:EX	Aile spécifique d'une prison dédiée aux phénomènes d'extrémisme
DUMBO	Application informatique anciennement utilisée par les greffes concernant les mineurs d'âge
ECRIS	European Criminal Records Information System
EPV	Extrémiste Potentiellement Violent
FEEDIS	Feeding Information System

FTF	Foreign Terrorist Fighter
HTF	Homegrown Terrorist Fighter
ISLP	Integrated System Local Police
JIB	Joint Information Box
LFP	Loi sur la Fonction de Police
MaCH	Mammouth @ Central Hosting
MJ	Maison de Justice
OCAM	Organe de Coordination pour l'Analyse de la Menace
OE	Office des Étrangers
PH	Propagandiste de Haine
PGP	Personne Groupement Phénomène
PJG	Parquet Jeunesse Greffe
PJP	Application informatique anciennement utilisée par les parquets concernant les mineurs d'âge (Parquet_Jeunesse/Jeugd_Parket)
Plan M	Plan Mosquées
Plan P	Plan Prisons
Plan R	Plan Radicalisme
PNR	Passenger Name Record
RGPD	Règlement Général de Protection des Données
RAR	Rapport Administratif/ Administratief Rapport
RIR	Rapport d'Information/ Informatie Rapport
SAJP	Système d'Administration de la Justice Pénale
CSE	Centre de Surveillance Electronique
SIDIS	Système Informatique de Détention / Detentie Informatie Systeem
SGRS	Service Général du Renseignement et de la Sécurité
SIRS	Service d'Information et de Recherche Sociale
SIS	Système d'Information Schengen
SPS	Service Psycho Social
SPSC(EX)	Service PsychoSocial Central Extrémisme
SE	Sûreté de l'État
TF	Terrorist Fighter
TFL	Task Force Locale
TFN	Task Force Nationale
TPI	Tribunal de Première Instance
Bel PIU	Passenger Information Unit (de la Belgique)
VSSE	Veiligheid van de Staat / Sûreté de l'État

1. La Banque de données Nationale Générale (BNG)

1.1. Description générale

1.1.1 Base légale

Loi du 5 août 1992 relative à la fonction de police (LFP) telle que modifiée par

- Loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, *Mon.b.,* 28.03.2014 et
- Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *Mon.b.,* 19.06.2019 ;

Directive commune MFO-3 du 14 juin 2002 des ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et administrative, *Mon.b.,* 18.06.2002 et ses circulaires annexes (confidentielles) ;

La gestion de l'information policière a longtemps manqué de base légale et de transparence. En effet, la matière était réglée par des directives internes aux services de police et des circulaires confidentielles. C'est en 2014 qu'une première officialisation de ces règles a été réalisée[9]. Celles-ci ont a été revues en 2019[10] afin, notamment, de les rendre conformes à la nouvelle réglementation en matière de protection des données à caractère personnel.

De manière générale, la section 12 de la Loi sur la Fonction de Police (LFP), intitulée « De la gestion des informations » décrit dorénavant les grandes lignes à respecter dans la gestion de l'information mais prévoit de nombreuses délégations de pouvoir en faveur du pouvoir exécutif pour déterminer plus précisément quelles sont les données qui peuvent être enregistrées, quelles sont les personnes qui peuvent être suivies, qui a accès à la banque de données, selon quelles modalités, etc. Les directives et circulaires prises en exécution de cette législation sont toutefois éparses et souvent confidentielles ce qui rend difficile le travail d'en rendre compte. Ainsi, en 2017, la Commission d'Enquête Parlementaire sur les attentats (CEP) lors de son examen de l'architecture de la sécurité, a constaté, en ce qui concerne la gestion

[9] Loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle.
[10] Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière.

de l'information, qu'il subsistait encore beaucoup d'imprécisions dans les règlementations et dans la pratique[11].

La mission générale de la police est d'assurer la sécurité des citoyens et de garantir la démocratie. Cette mission générale se décline, d'une part, en missions de police judiciaire (i.e., la recherche des infractions, la collecte de preuves et la remise des auteurs présumés à la Justice) ; et, d'autre part, en missions de police administrative (i.e., le maintien et le rétablissement de l'ordre public[12] lequel correspond à la propreté, la tranquillité, la sécurité et la santé publiques).

Le manuel sur la fonction de police (Keuterickx V. et al., 2019) précise que « la tranquillité publique est l'absence de désordre et d'agitation. C'est l'état normal des choses. La sécurité publique est assurée lorsqu'aucun incident ou aucun risque impliquant des personnes ou leurs biens ne peut se produire. L'incident signifie une atteinte à la sécurité. La protection de la santé publique enfin consiste à protéger les personnes contre les maladies ou les risques de maladie, notamment en garantissant un environnement de qualité. Elle comporte l'hygiène des personnes, des biens privés et du domaine public ».

Dans la pratique, toutes les missions de police qui ne relèvent pas de la police judiciaire mais plutôt de la protection des personnes (et des biens) relèvent de la police administrative (e.g., la patrouille de police ou les mesures de surveillance générale).

Pour accomplir correctement ces différentes missions, les services de police doivent pouvoir collecter, traiter et transférer des informations et des données à caractère personnel.

Article 44/1 §1 LFP : Les services de police peuvent traiter des informations et données à caractère personnel pour autant que ces dernières présentent un caractère adéquat, pertinent et non excessif au regard des finalités de police administrative et de police judiciaire pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.

Ces données et informations sont enregistrées via des programmes informatiques distincts au niveau des polices locales (Integrated System Local Police, ISLP) et au niveau de la police fédérale (Feeding Information System, FEEDIS).

[11] Troisième rapport de la CEP Attentats sur le volet « Architecture de la sécurité », *op.cit.*, p. 180-181 : absence de vision et de stratégie globales ; surinformation accrue ; abondance de banques de données ; capacité d'analyse insuffisante ; cloisonnement et par conséquent, insuffisance de partage ; processus de traitement inefficaces et désuets. Deux lignes de fracture inutiles apparaissent : d'une part, entre le volet judiciaire et le volet administratif et d'autre part, entre la police fédérale et la police locale. C'est la raison pour laquelle la CEP plaide pour une Banque carrefour de la sécurité, à l'instar de la Banque Carrefour de la sécurité sociale.

[12] Sur la notion d'ordre public et plus particulièrement sur la question de savoir si des indices de radicalisation idéologique d'une personne peuvent être considérés comme un risque d'atteinte à l'ordre public et donc justifier l'action administrative de la police, voir notamment Xavier F. (2019).

Pour permettre la circulation de ces informations entre les différents services de police (tant fédéraux et locaux que judiciaires et administratifs), ces données et informations sont également transférées et structurées dans une banque de données policière opérationnelle.

> Article 44/2 §1 LFP : Lorsque l'exercice des missions de police administrative et de police judiciaire nécessite que les services de police structurent les données à caractère personnel et les informations visées à l'article 44/1 de sorte qu'elles puissent être directement retrouvées, celles-ci sont traitées dans une banque de données policière opérationnelle (…).

Il existe cinq types de banques de données policières opérationnelles : (1) la BNG, (2) les banques de données de base, (3) les banques de données particulières, (4) les banques de données communes et (5) les banques de données techniques. Leur nombre exact pour chaque catégorie reste cependant incertain et difficile à établir précisément. La BNG est une de ces banques de données policière opérationnelle, probablement la plus volumineuse d'entre elles. Elle fut créée à la suite de « l'affaire Dutroux » (Kaiser V, 2010 : 8) afin d'améliorer la circulation de l'information policière entre les différents services de police du pays. Cette banque de données recouvre, à titre principal, les données en matière judiciaire. À ce volet judiciaire, fut joint un volet administratif – BEPAD (BEstuurlijke Politie – Police Administrative) – lequel regroupe les données en matière administrative. BEPAD est considéré, moins pour des raisons techniques que légales, comme le volet « police administrative » de la BNG, ce afin de correspondre à la nomenclature des banques de données policières prévue par la loi sur la fonction de police.

1.1.2 Responsable et gestionnaire

Le responsable du volet administratif de la BNG est le Ministre de l'Intérieur tandis que le responsable du volet judiciaire est le Ministre de la Justice. Ce sont les ministres qui déterminent, par directives contraignantes, les mesures nécessaires en vue d'assurer la gestion et la sécurité des données dont notamment les aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité de celles-ci[13]. Les garants de la bonne exécution de ces directives sont les chefs de corps pour la police locale, le commissaire général et les directeurs pour la police fédérale. La gestion journalière de la BNG est quant à elle assurée par la direction générale de la gestion des ressources et de l'information de la Police fédérale[14].

1.1.3 Finalités du traitement

La loi sur la fonction de police détermine la finalité du traitement par référence à l'article 27 de la loi sur la protection des données, à savoir « la prévention et la détection des infractions pénales, les enquêtes et les poursuites en la matière, ou l'exécution de sanctions pénales, y

[13] LFP, article 44/4 §2 .
[14] LFP, article 44/11.

compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ».

L'enregistrement et le traitement des données à des finalités de police administrative et de police judiciaire sont conditionnés à leur caractère adéquat, pertinent et non excessif au vu de cette finalité[15].

1.1.4 Catégories de personnes

1.1.4.1 *En matière administrative*

Cinq catégories de personnes sont à distinguer[16] :

1. Les personnes qui représentent une association qui envisage un évènement dans l'espace public (manifestation, …) ;
2. Les personnes qui, selon différents critères, sont considérées comme représentant un risque pour le maintien de l'ordre public ;
3. Les personnes soumises à une mesure administrative ou à une condition judiciaire dont le respect doit être surveillé par les services de police ;
4. Les malades mentaux et les étrangers ;
5. Les personnes enregistrées en police judiciaire pour un fait infractionnel commis dans le cadre du maintien de l'ordre public ;

Pour être considérée comme représentant un risque pour le maintien de l'ordre public, la personne doit être impliquée dans un phénomène ou un groupement national ou international susceptible de troubler l'ordre public. La notion de phénomène est entendue comme un ensemble des problèmes portant atteinte à l'ordre public et nécessitant des mesures appropriées de police administrative, parce qu'ils sont de même nature et répétitifs, qu'ils sont commis par les mêmes personnes ou qu'ils visent la même catégorie de victimes ou de lieux[17]. Selon les travaux parlementaires de la loi du 18 mars 2014, par 'groupement', il faut comprendre « un ensemble de personnes avec un certain degré de structuration qui se traduit par exemple par l'organisation de réunions périodiques ou la hiérarchisation, la répartition des rôles entre les membres (rassembler des fonds pour le groupement, recruter pour le groupement, diffuser l'idéologie du groupement, …), ou le port d'un ou plusieurs identifiants communs » [18].

[15] LFP, article 41/1, §1.
[16] LFP, article 44/5, §1, 1° à 7°.
[17] LFP, article 44/5 §1, 2° et 3°.
[18] *Doc. parl*., Ch., 2013-2014, 53-3105/001, p. 28-29.

Les phénomènes et groupements répondant à ces définitions sont entérinés chaque année par le ministre de l'Intérieur sur la base d'une liste proposée par la Direction des opérations de police administrative de la police fédérale (DAO). Cette liste est établie à partir des constatations de terrain ayant été centralisées par la Police fédérale. Elle est ensuite soumise à l'avis préalable de la Direction centrale pour la lutte contre la criminalité grave et organisée de la police fédérale (DJ-SOC), l'Organe de coordination pour l'analyse de la menace (OCAM)[19], la Sûreté de l'État (SE) et le Service Général du Renseignement et de la Sécurité (SGRS). Les services ont ainsi d'une année à l'autre la possibilité de supprimer, ajouter ou maintenir un groupement ou un phénomène[20]. Cet acte posé par le pouvoir exécutif n'est pas contrôlé par le pouvoir législatif ni judiciaire. Il s'agit d'une liste éminemment politique et évolutive[21] qui est tenue confidentielle.

L'enregistrement d'une personne résulte d'observations de terrain et d'informations glanées par la police lors de contrôles d'identité, de fouilles ou encore d'arrestations administratives réalisés en marge d'événements, lesquelles lui permettent d'attester de la participation effective de la personne à l'un des groupements ou phénomènes répertoriés. L'appartenance à un groupement doit pouvoir être établie par un lien réel (carte de membre, soutien financier, soutien logistique, animation, etc.). La simple présence d'une personne à un événement (e.g., manifestation, rassemblement) ne suffit donc pas pour qu'elle soit consignée dans la banque de données.

1.1.4.2 *En matière judiciaire*

Les données personnelles et informations qui peuvent être enregistrées dans la BNG judiciaire sont celles relatives à[22] :

- des auteurs et suspects d'un fait pénal ou d'une infraction sanctionnée administrativement et constatée par la police ;
- des personnes condamnées (dans ce cas les modalités d'exécution de la peine sont également enregistrées) ;
- des personnes disparues, décédées de manière suspecte, évadées ;
- des victimes d'un fait pénal ;

[19] L'OCAM est placé sous l'autorité conjointe de la justice et de l'intérieur. Il a été créé par la loi du 10 juillet 2006 relative à l'analyse de la menace (dite loi OCAM). Ses compétences sont précisées dans l'arrêté royal du 28 novembre 2006 et ont depuis été systématiquement étendues.
[20] Si, au cours d'une année, un service de police estime qu'un nouveau groupement doit être suivi, ils peuvent en faire état auprès de DAO qui fera une demande au Ministre de l'Intérieur pour une modification de la liste. Entretemps, ils consignent tous les faits concrets qui attestent de l'existence du groupement. Conversation avec du 26 septembre 2017 avec un agent du Carrefour d'Information de l'Arrondissement (CIA) de Bruxelles-Capitale.
[21] *Doc. parl*., Ch., *op.cit*., p. 28-29.
[22] LFP, article 44/5 §3.

1.1.5 Données et informations

La donnée de base d'enregistrement en BNG est le fait et non la personne. Les faits sont donc enregistrés, indépendamment de leur association éventuelle avec une personne. Ainsi un fait dont l'auteur est inconnu est enregistré dans la BNG. Par contre, une personne ne peut être enregistrée en BNG qu'en rapport avec un fait. Les faits sont qualifiés par rapport à l'infraction pénale ou la situation non infractionnelle mais préoccupante qu'ils laissent soupçonner.

Sont enregistrées en BNG tant des informations relatives à des faits concrets (aussi appelées les informations 'dures') localisables dans le temps et dans l'espace – tels que, en matière administrative, l'annonce de l'organisation d'une manifestation ou, en matière judiciaire, le constat d'un vol – que des informations moins précises (non localisées, non confirmées, …) mais néanmoins utiles au regard des finalités policières (aussi appelées des informations 'douces') – tels que, en matière judiciaire, l'information reçue d'un informateur sur un projet de cambriolage ou en matière administrative, une rumeur de quartier circulant sur l'organisation de réunions clandestines d'un groupe extrémiste.

Les informations dures sont généralement consignées dans un procès-verbal qui décrit les éléments dont le policier a pris connaissance et les actes d'enquête qu'il pose en la matière tandis que les informations douces sont en principe consignées dans un rapport qui, dans le jargon policier, s'intitule en matière judiciaire, un RIR (Rapport d'Information/ Informatie Rapport) et en matière administrative un RAR (Rapport Administratif/ Administratief Rapport).

Tout PV doit être rédigé et transmis à la BNG endéans les trois semaines qui suivent la constatation du fait[23]. Les RIR et les RAR sont également enregistrés dans la BNG. Puisque le fondement d'un enregistrement dans la BNG est le fait (sans lequel il est impossible d'enregistrer une personne), ces rapports font office de faits « non-concrets ». Une personne peut donc être liée à de tels « faits » bien que le seuil infractionnel n'ait pas été franchi ou qu'il soit difficile de caractériser précisément le fait infractionnel dans l'espace ou le temps. Les rapports sont, en principe, d'abord communiqués à un tiers qui évalue la pertinence d'une communication de l'information à l'ensemble des services de police par le biais de l'enregistrement en BNG[24]. En principe, cette pertinence est évaluée par le chef de corps et par un service central au niveau de l'arrondissement qui s'appelle le Carrefour d'Information de l'Arrondissement (CIA)[25].

[23] http://www.stat.policefederale.be/assets/pdf/methodologie/note_methodologique_SPC_generale.pdf
[24] Troisième rapport de la CEP Attentats sur « l'architecture de la sécurité », *op.cit.*, p. 195-196.
[25] Directive commune MFO-3 et ses annexes confidentielles.

La non transmission de données et d'informations par un fonctionnaire de police est en revanche punissable pénalement[26].

Par ailleurs, le contenu des rapports enregistrés en BNG n'est pas toujours accessible. Dans certains cas, en effet, le contenu du rapport ne peut être divulgué tel quel pour, par exemple, ne pas mettre en danger la personne à la source de l'information. À cette fin, des codes sont assignés aux RIR par le rédacteur du rapport pour définir son statut. Le code 11 signifie que l'information est exploitable opérationnellement, le code 10 que l'information est exploitable mais sans mention de la source de l'information. Le code 01 signifie que l'information ne peut être utilisée qu'après consultation avec l'auteur du RIR et le code 00 que l'information ne peut tout simplement pas être exploitée. En cas de code 01, le fonctionnaire de police consultant la banque de données voit qu'il existe un RIR mais son contenu n'est pas lisible. En cas de code 00, la personne qui consulte la BNG ne voit rien. En cas de consultation de la BNG concernant une personne pour laquelle il existe des RIR codés 01 ou 00, un signal électronique est envoyé au rédacteur du RIR afin qu'il sache que la personne faisant l'objet de son enregistrement a fait l'objet d'un contrôle en BNG.

1.1.6 Les accès aux données et informations contenues dans la BNG

Outre l'accès pour l'ensemble des membres des services de police, la LFP envisage également la possibilité de communication des données enregistrées à des tiers en en précisant les modalités[27]. Il s'agit soit de l'octroi d'un droit d'accès direct qui correspond à une liaison automatisée à la BNG permettant une prise de connaissance de l'ensemble des données y enregistrées (y compris au niveau des liens relationnels), soit de l'octroi d'une droit d'interrogation directe qui permet, au détenteur de ce droit, de se renseigner, après l'aval du gestionnaire de la base de données, sur (1) l'existence ou non d'un enregistrement en BNG pour une personne considérée, et en cas de correspondance trouvée (un 'hit') sur (2) la qualification retenue concernant les faits pour lesquels la personne est enregistrée, (3) les données nécessaires pour obtenir plus d'informations auprès de l'autorité compétente (par exemple : quel est le service de police qui a enregistré ladite information ?), (4) les mesures de contrôle policier à laquelle la personne est soumise. On peut lire dans les travaux parlementaires que ce système d'interrogation doit permettre une meilleure coordination entre les partenaires de la chaîne pénale[28]. Ainsi, le partenaire externe mis au courant de l'existence d'un enregistrement dans la BNG par rapport à son objet d'étude, doit prendre contact avec le service de police pour obtenir de l'information complémentaire. Ces contacts doivent permettre aux deux services d'enrichir réciproquement leurs données ou, éventuellement, de les corriger.

[26] LFP, article 44/11/1.
[27] LFP, article 44/11/4.
[28] *Doc. parl*., Ch., *op.cit.*, p. 54-55.

Dans certaines circonstances spécifiques décrites dans la loi, la police peut également trannsmettre les données demandées à certaines instances spécifiées dans la loi[29].

Sous certaines conditions, les données peuvent également être transmises à des services (policiers) étrangers ou des organisations internationales de coopération judiciaire et policière[30].

Les organismes auxquels la loi autorise l'octroi d'un droit d'accès direct sont : (1) l'Organe de Coordination pour l'Analyse de la Menace (OCAM) et (2) les services de renseignement[31]. Les organismes auxquels elle autorise l'octroi d'un droit d'interrogation directe sont : (1) l'Office des Etrangers, (2) la Cellule de Traitement des Informations Financières (CTIF) et (3) les services d'enquête et de recherche de l'administration des douanes et accises[32].

Toutefois, la LFP conditionne encore la réalité de l'exercice de ces droits à la détermination par arrêté délibéré en conseil des ministres de leurs modalités. A notre connaissance, à ce jour (juin 2021), l'accès direct est limité aux services de police, aux autorités judiciaires[33] et aux services en charge du contrôle afin de leur permettre d'exercer leurs missions légales[34] et un droit d'interrogation directe a été accordé d'une part, à l'Office des Étrangers (OE)[35] et d'autre part, au Service Public Fédéral Justice[36].

L'octroi de ce droit à l'OE vise à lui permettre[37] [38] « dans le cadre de ses missions légales de délivrance de titres de séjour sur le territoire belge ou d'ordre de quitter le territoire, (… d') obtenir rapidement les données qui permettront de pouvoir évaluer si le demandeur étranger constitue ou non un danger pour l'ordre public ou la sécurité nationale ».

Quant au SPF Justice, l'objectif poursuivi est de favoriser la traçabilité des individus dans l'intégralité du système pénal, en ce compris dans ses phases d'exécution de la peine ou de mesures privatives de liberté ou d'une mesure de sûreté[39]. L'idée est d'identifier toute

[29] WPA, artikel 44/11/7 tot en met 11 en artikel 44/11/13.
[30] LFP, art. 44/11/13. Au-delà du respect des règles de droit international et des accords de coopération conclus, l'avis de l'organe de contrôle (COC) doit également être demandé pour l'échange de données entre services de police des États membres de l'Union européenne et d'Interpol.
[31] LFP, article 44/11/12 §1.
[32] LFP, article 44/11/12 §2.
[33] LFP article 44/11/7.
[34] LFP, article 44/11/8.
[35] LFP article 44/11/8bis et AR 28 avril 2016 relatif à l'interrogation directe de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police par les membres du personnel désigné de l'Office des étrangers.
[36] AR 11 mars 2019 relatif aux modalités d'interrogation directe de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police au profit du Service public fédéral justice dans le but de contribuer à l'identification unique des détenus .
[37] *Doc. parl*., Ch., *op.cit*., p. 57.
[38] Rapport au Roi précédant l'AR du 28 avril 2016, *op.cit.*
[39] AR 11 mars 2019, *op.cit.*

personne écrouée à l'aide de ses empreintes digitales, ce qui permet de garantir l'unicité du dossier de détention d'une même personne. On remarquera que le concept dorénavant utilisé pour identifier les personnes n'est plus celui de l'identité qui deviendrait de plus en plus relatif[40], mais bien celui d'identification[41] via, notamment, les empreintes digitales. Lorsqu'après comparaison, les données d'identité enregistrées dans la BNG ne correspondent pas à celles du titre de détention du détenu, il y a lieu pour l'administration pénitentiaire de diligenter une enquête administrative afin d'identifier plus avant la personne écrouée.

Par contre, à notre connaissance, aucun autre service que ceux sus mentionnés ne s'est vu accorder le bénéfice d'un droit d'accès direct aux données enregistrées dans la BNG. A l'inverse, la loi du 5 mai 2019 est venue conditionner la communication des données aux services de renseignement à une sorte de réciprocité 'temporelle'[42]. Les services de renseignement ne peuvent donc, à l'heure actuelle (juin 2020) obtenir des informations enregistrées dans la BNG que par le biais d'une interrogation relative à une affaire/personne précise et ils n'ont pas accès au modèle relationnel de la BNG, ni aux rapports d'information (RIR et RAR).

1.1.7 Durée de conservation des données et archivage

1.1.7.1 *En matière administrative*

Les données relatives à une personne doivent être effacées au maximum cinq ans à dater du dernier incident connu la concernant. Ce délai est toutefois renouvelé dès qu'un nouvel élément suspect est constaté endéans les cinq ans (ex: la personne est arrêtée administrativement lors d'une manifestation, elle fréquente un lieu suspect, elle envoie de l'argent). Après cette période, les données relatives à la personne sont archivées pour une période de 30 ans. L'unité gestionnaire ayant effectué l'enregistrement dans la base de données administratives peut aussi décider d'initiative que la personne n'a plus lieu d'être suivie, elle a alors la possibilité d'archiver manuellement l'enregistrement de la personne pour autant qu'elle justifie cet acte en encodant la raison de cet archivage prématuré. Dans la pratique, cette option ne serait cependant pas utilisée[43].

Une fois archivée, l'information n'est donc plus accessible. Dans le cas où la police constate de nouvelles activités, après l'archivage, les activités antérieures de la personne ne sont pas réactivées. La personne fait simplement l'objet d'un nouvel enregistrement. Cependant, les

[40] AR 11 mars 2019, *op.cit.,* Rapport au Roi.
[41] Attribution sur la base de celle-ci d'une référence dactyloscopique unique appelée numéro AFIS.
[42] LFP, article 44/11/8bis al. 2 : « les modalités de communication vers la police des données des services de renseignement sont déterminées dans un instrument juridique dont la date d'entrée en vigueur est simultanée à celle de l'accès direct des services de renseignement et de sécurité à la BNG ».
[43] Correspondance électronique du 17 décembre 2017 avec un agent de la Direction des opérations de police administrative de la police fédérale.

informations archivées restent à titre exceptionnel consultables par certaines personnes dûment mandatées.

1.1.7.2 *En matière judiciaire*

Le délai d'archivage des données relatives à une personne enregistrée dans la BNG judiciaire varie en fonction de la gravité du fait. Il est d'un an à partir de l'enregistrement du fait s'il s'agit d'une contravention. S'il s'agit d'un délit, le délai d'archivage est de dix ans. Dans le cas d'un crime, il est de 30 ans.

1.2. Enregistrements en matière de radicalisation

1.2.1. En matière administrative

Depuis 2006, la Belgique dispose d'un Plan d'Action Radicalisme (le Plan R)[44] qui prévoit des mesures administratives destinées à agir sur les différentes formes de radicalisme[45]. À la suite de l'attentat déjoué à Verviers le 15 janvier 2015, le Conseil national de sécurité (CNS) a adopté le 14 décembre 2015 une version actualisée du Plan R, lequel poursuit deux objectifs principaux : « dresser la carte des individus et groupements ayant un effet radicalisant sur leur entourage et réduire les vecteurs de radicalisation » [46]. Cette double tâche à caractère préventif relève essentiellement des compétences des services de sécurité et de renseignements (e.g., OCAM, SE et SGRS) ainsi que des services de police en charge des missions de police administrative.

Depuis août 2016, une table *Personne Groupement Phénomène* (PGP) a été introduite notamment pour concrétiser le projet de faire de BEPAD le volet « police administrative » de la BNG [47]. L'objectif premier de BEPAD lors de sa mise en œuvre visait à permettre l'enregistrement des événements à venir intéressant l'ordre public (au sens large) et les moyens policiers qui doivent y être affectés (moyens propres, renforts demandés, etc.) ainsi que les coordonnées des personnes responsables de ces événements. Grâce à la table PGP, il est désormais possible de consulter la base de données par rapport à quatre types d'entités différentes : (1) les personnes, (2) les groupements, (3) les phénomènes et (4) les événements. Les quatre entités sont reliées entre elles.

[44] Ce Plan d'Action Radicalisme est une version revue et augmentée du Plan M (Plan Mosquées) élaboré à la suite des attentats du 11 septembre 2001 aux États-Unis et approuvé fin 2002.
[45] Le contenu exact de ce plan n'a jamais été rendu public officiellement. Selon le Comité R, « la confidentialité de ce plan est davantage motivée par la sensibilité politique du sujet que par une quelconque nécessité opérationnelle » (Comité R, 2006 : 14).
[46] Plan R, 2016, p. 5.
[47] Correspondance électronique du 17 septembre 2020 avec un agent du Service d'information et de communication d'arrondissement (SICAD) de Bruxelles.

Les phénomènes en raison de la nature et de la récurrence des comportements visés, se voient attribués dans PGP des appellations génériques (e.g., le squattage problématique, les nuisances autour des gares), au contraire des groupements qui reçoivent des dénominations particulières (e.g., supporters à risque d'un club de football déterminé)[48]. Les groupements et phénomènes faisant l'objet d'un suivi sont de nature diverse et variée. À l'heure actuelle, on retrouve des groupements et phénomènes relevant entre autres des catégorisations suivantes : extrémisme de gauche, extrémisme de droite, extrémisme religieux, extrémisme environnemental, terrorisme, groupements violents, bandes de motards, activisme en faveur du droit des animaux, activisme informatique, etc. (Mine et al., à paraître). Tous auraient cependant pour caractéristique commune le fait d'être associés à la radicalité, l'extrémisme ou la violence, et d'être susceptibles de troubler l'ordre public (par exemple en occasionnant un désordre matériel de par leurs activités)[49].

Une même personne peut être enregistrée pour son appartenance à plusieurs groupements ou phénomènes. Le rôle qu'elle entretient avec le groupement ou le phénomène est précisé (e.g., dirigeant, membre, soutien financier).

1.2.2. En matière judiciaire

Les faits sont qualifiés par rapport à l'infraction pénale qu'ils laissent soupçonner. En matière de radicalisation et terrorisme, en fonction des faits visés et de la précision des informations dont le policier dispose, les faits étaient principalement enregistrés soit sous le code de prévention « 35 » qui est relatif aux infractions terroristes, soit sous le code « 45 » qui reprend le large spectre des agissements suspects.

Pour enrichir l'information enregistrée et son partage, il fut décidé dès 2013, de reprendre également dans la BNG judiciaire sous la forme de fait non concret, le contenu des rapports d'information établis par les polices locales relativement à des suspicions de radicalisation. À cette fin, ces rapports sont envoyés au Carrefour d'Information de l'Arrondissement (CIA) qui décide, en fonction des informations en sa possession si leur enregistrement en BNG est justifié.

Dans le climat de panique engendré par les menaces émanant du conflit syrien, la pratique des enregistrements au niveau local est cependant rapidement devenue ingérable. En effet, un RIR de suspicion de radicalisation enregistré en BNG à l'égard d'une personne entrainait, en cas de contrôle, également la suspicion des personnes entrées en contact avec cette

[48] Cependant, un même groupement peut être enregistré sous des dénominations différentes ou se décliner en sous-groupements (e.g., représentation locale du groupement) car l'enregistrement se fait dans un champ libre ce qui peut générer des doublons. Lorsqu'ils sont identifiés, ceux-ci sont fusionnés par la DAO.

[49] Correspondance électronique du 5 février 2019 avec un agent de la Direction des opérations de police administrative de la police fédérale.

dernière. Ce processus impliquait deux effets négatifs. D'une part, il augmentait excessivement le nombre de personnes suspectées de radicalisation. D'autre part, il menait à une surévaluation du risque puisque la personne connue pour radicalisme voyait son nombre de signalements augmenter. Ce problème a été résolu par l'introduction de la notion de « RIR contrôle », ce qui fait qu'aujourd'hui le policier effectuant le contrôle d'une personne connue pour radicalisme ne rédige plus un nouveau RIR « extrémisme » mais bien un RIR spécifique « contrôle ».

Par ailleurs, en février 2015, il fut décidé d'introduire, dans la BNG judiciaire, un nouveau code de qualification spécifique (QLF n° 7780), intitulé *comportement en lien avec une radicalisation violente*. La particularité de ce nouveau code de qualification, est qu'il est destiné à appréhender des faits non infractionnels, et a fortiori non punissables (au même titre que les suicides, les objets perdus, etc.), mais pour lesquels un procès-verbal est tout de même établi. Ceci a permis de donner une plus grande visibilité à ces constats qui, auparavant, étaient noyés dans la catégorie des agissements suspects.

Si la police se réfère[50] aux notions de terrorisme, extrémisme et radicalisme issues du Plan National de Sécurité (2016-2019), elle ne précise pas toutefois ce qu'il y a lieu d'entendre par un comportement en lien avec une radicalisation violente.

[50] Ainsi, on trouve, dans sa description des phénomènes pris en compte dans les statistiques de criminalité (http://www.stat.policefederale.be/assets/pdf/notes/definitions_fig_crim_avril_2018.pdf.), la phrase suivante : « Le radicalisme est une notion large. Il peut revêtir de nombreuses formes et peut notamment être inspiré par la politique et la religion. Toute personne aspirant à des changements fondamentaux au sein de la société ne constitue pas pour autant un danger pour l'ordre juridique démocratique. Cependant, certains groupes ou individus qui se radicalisent font l'apologie d'actes de violence, représentent un danger pour l'ordre juridique démocratique et/ou visent le démantèlement, voire la destruction, du système démocratique. Le comportement de ces groupes ou individus peut les conduire à des activités illégales. Le processus de radicalisation est dynamique et commence par une distanciation de l'environnement proche et ensuite de la société et du système politique. On observe par après une intolérance croissante envers des idées qu'on ne partage pas et une disposition croissante à accepter la violence comme moyen d'imposer ses propres idées aux autres. L'extrémisme violent est une phase successive dans le processus d'évolution vers la violence. Il n'y a plus d'espace pour l'acceptation de l'existence d'une idéologie différente de celle à laquelle on croit et on est disposé à justifier la violence et l'oppression, à les défendre et les utiliser comme méthodes pour imposer sa propre idéologie. Il est même question d'une identification positive avec des méthodes violentes. Le terrorisme comme phase finale: il est fait usage de violence pour terroriser les individus et la société et leur occasionner des dommages importants. L'usage de la violence et ses conséquences visent à créer un terrain fertile qui rend envisageables ou entraîne même des transformations sociales et politiques.».

2 Banque(s) de données commune(s) (BDC)[51]

2.1 Base légale

- Loi 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.,* 9 mai 2016, p. 30567, ci-après dénommée « loi BDC ». ;
- Arrêté royal 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters 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*, M.B.,* 22 septembre 2016, p. 63970, ci-après dénommé « AR FTF » ;
- Arrêté royal 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters 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 et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters *M.B*., 30 mai 2018, p. 45079, ci-après dénommé « AR HTF » ;
- Arrêté royal du 23 avril 2018 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 *M.B*., 30 mai 2018, p. 45056, ci-après dénommé « AR PH » ;
- Arrêté royal 20 décembre 2019 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de Haine et portant exécution de certaines dispositions de la section 1er bis « de la gestion de l'information » du chapitre IV de la loi sur la fonction de police, *M.B.*, 27 janvier 2020, p. 3256, ci-après dénommé « AR EPV »;

Consécutivement au départ d'un certain nombre de ses ressortissants vers les zones de conflits irako-syriennes, et plus particulièrement à la suite des attentats de Paris en 2015 et de Bruxelles en 2016, l'État belge a décidé de créer une banque de données commune (BDC) spécifiquement dédiée au phénomène du 'terrorisme et de l'extrémisme pouvant mener au terrorisme'[52] laquelle peut être consultée et alimentée par différents acteurs, notamment ceux du système d'administration de la justice pénale et des services de sécurité et de renseignement. L'objectif poursuivi par cette banque de données est d'aboutir à un partage

[51] Cette section consacrée aux banques de données communes ne comprend pas de sous-section intitulée « enregistrements relatifs à la radicalisation » car tel est son objet. Celles-ci sont une évolution en soi dans la mesure où bien qu'elles étaient en projet, elles ne préexistaient pas à la mise à l'agenda politique du phénomène de la radicalisation.

[52] Article 44/2 §2 de la Loi sur la Fonction de Police (ci-après dénommée « loi LFP ») introduit par la loi du 27 avril 2016 relative à des mesures complémentaires en matière de terrorisme, ci-après dénommée « loi BDC ».

étendu d'informations et de données à propos des entités[53] – personnes, groupements ou phénomènes – considérées comme une menace pour la sécurité du pays. Selon les travaux parlementaires[54], « il apparait en effet primordial dans ces domaines touchant directement à la sécurité des personnes que ces différents services soient guidés dans leurs actions quotidiennes et dans leurs prises de décisions, non seulement par les données et informations dont chacun d'eux dispose dans son propre système d'enregistrement mais également par celles issues de la mise en commun de différents services ». Remarquons que l'origine de cette volonté remonte historiquement à des évènements terroristes bien antérieurs à la crise en Syrie (Van Hoey, 2020 : 266-297).

Les premiers enregistrements eurent lieu dans la *Joint Information Box* (JIB) élaborée par l'OCAM consécutivement aux recommandations du Plan Radicalisme (plan R) lesquelles prévoient plusieurs mesures administratives destinées à agir sur les différentes formes de radicalisme (Thomas, 2020 : 30-33). Il s'agissait d'un fichier de travail (comportant une liste de noms) visant à assurer la collecte structurelle d'informations sur les entités suspectées par les services de renseignement d'être des vecteurs de radicalisation. La décision d'intégrer ou non une entité dans la JIB était prise par consensus au sein du groupe de travail dénommé « Task Force Nationale » (TFN)[55]. Au début de la crise syrienne et dans l'urgence, l'OCAM a développé parallèlement une autre liste (la 'liste OCAM') reprenant sous différentes catégories le nom des personnes suspectées d'être parties ou de vouloir partir vers la zone de conflit syro-irakienne. Cette liste était complétée, voire corrigée, manuellement, à intervalles réguliers (d'abord tous les trimestres puis tous les mois), et envoyée par email à différents acteurs en charge de la sécurité, dont la police et les services de renseignement. En août 2015, une circulaire conjointe du Ministre des Affaires étrangères et du Ministre de la Justice est venue encadrer cet échange d'informations[56]. À l'évidence, d'un point de vue strictement légal, cet acte à diffusion restreinte ne suffisait pas pour autoriser la collecte, le traitement et surtout le partage de données personnelles et informations entre services. Par ailleurs, les autorités locales se plaignaient de ne pouvoir assurer le suivi sur le terrain, faute

[53] Si en théorie le mot « entité » est l'expression générique désignant les personnes, groupements ou phénomènes constituant une menace, il semble que, dans la pratique, ce ne sont que des personnes qui sont à l'heure actuelle enregistrées dans la BDC.

[54] Projet de loi du 21 mars 2016 relatif à des mesures complémentaires en matière de lutte contre le terrorisme (ci-après dénommé « projet de loi BDC »), *Doc. Parl.,* Ch., 2015-2016, 54/1727/001, p. 13. Ce projet de loi est devenu la loi BDC, *op.cit.*

[55] Selon le plan R, « Au niveau fédéral se situe la Taskforce nationale, l'organe stratégique et politique. Ce groupe de travail (« taskforce ») se réunit tous les mois et est composée de membres de l'OCAM, de la Sûreté de l'État, du Service Général du Renseignement et de la Sécurité, de représentants de la police fédérale et de la police locale, du SPF Affaires étrangères, du SPF Justice – Direction générale des Établissements pénitentiaires, de la Cellule de traitement de l'information financière, du SPF Intérieur, de l'Office des Étrangers et de la Direction générale du Centre de crise, un représentant de la Direction générale Sécurité et Prévention du SPF Intérieur, du Ministère public et des représentants des communautés et régions ».

[56] Circulaire confidentielle conjointe du Ministre des Affaires étrangères et du Ministre de la Justice concernant l'échange d'informations et le suivi des Foreign Terrorist Fighters, du 21 août 2015. Cette circulaire fait suite à une autre circulaire du 25 septembre 2014 – confidentielle et à laquelle nous n'avons pas pu avoir accès – relative à la gestion de l'information et aux mesures de suivi concernant les Foreign Terrorist fighters.

de canal d'informations direct avec l'OCAM et les services de renseignement. C'est la raison pour laquelle les parlementaires votèrent la loi du 27 avril 2016 qui permet, entre autres, la création de banques de données communes et dynamiques (c'est-à-dire continuellement mise à jour) dans lesquelles différents services (limitativement énumérés) peuvent enregistrer des données à caractère personnel ainsi que les informations dont ils disposent à propos de entités identifiées pour leur implication dans les activités d'une organisation terroriste ou d'extrémisme pouvant mener au terrorisme.

Cette loi fixe le cadre général de l'établissement de banques de données communes à différents services mais laisse au pouvoir exécutif le soin de déterminer l'objet des enregistrements (à savoir qui sont les personnes visées) ainsi que les types de données traitées, les règles de responsabilité, les conditions d'utilisation, de conservation et d'effacement des données. Dans la foulée, en juillet 2016, un arrêté royal[57] est venu spécifier d'une part, les personnes dont les données peuvent être enregistrées dans ce qui fut la première banque de données commune – celles des 'Foreign Terrorist Fighters' (FTF) – et d'autre part, les modalités d'accès et d'alimentation de ce nouvel outil par les différents services concernés.

Depuis lors, ce principe d'échange de données s'est progressivement étendu à des catégories de personnes de plus en plus éloignées de la notion de terrorisme de type djihadiste. Ainsi, en avril 2018, deux arrêtés royaux ont été adoptés dans ce sens. Le premier élargit les enregistrements de la première banque de données commune à tout résident présentant des velléités terroristes (pour quelque idéologie que ce soit)[58] – les 'Homegrown Terrorist Fighters' (HTF). Le second crée une nouvelle banque de données commune afin d'y enregistrer toute personne propageant une idéologie haineuse – les Propagandistes de Haine (PH)[59]. En décembre 2019, ce principe a été étendu aux individus considérés comme des extrémistes potentiellement violents (EPV) ainsi qu'aux « condamnés terro » (CT)[60].

[57] Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters 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, *M.B.*, 22 septembre 2016, p. 63970, dénommé « AR FTF ».

[58] À ce moment, la BDC FTF a été rebaptisée « BDC TF » et fut subdivisée en deux catégories distinctes, à savoir d'une part les FTF et d'autre part les HTF. Arrêté royal du 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters 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 et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters, ci-après dénommé « AR HTF ».

[59] Arrêté royal du 23 avril 2018 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, ci-après dénommé « AR PH ».

[60] Arrêté royal 20 décembre 2019 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist fighters et l'arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er bis « de la gestion de l'information » du chapitre IV de la loi sur la fonction de police, ci-après dénommé « AR EPV ».

En résumé, au niveau des textes légaux, nous avons donc deux BDC, l'une intitulée BDC TF[61] qui reprend les FTF, les HTF, les EPV et les CT, l'autre[62] intitulée PH qui ne reprend, quant à elle, que les PH. En pratique, il semble toutefois qu'il n'existe qu'une seule et même BDC qui reprend les 5 catégories (FTF, HTF, EPV, CT et PH).

2.2 Responsables et gestionnaires

Les ministres de l'Intérieur et de la Justice sont responsables conjointement des traitements effectués dans le cadre des BDC tandis que l'OCAM en est le responsable opérationnel et la police fédérale le gestionnaire[63].

La police est chargée de la gestion technique et fonctionnelle alors qu'il appartient à l'OCAM d'assurer d'une part, la coordination et la collaboration entre les différents services et d'autre part, la qualité des données.

2.3 Missions/objectifs

La loi autorise la création de BDC pour « la prévention et le suivi du terrorisme et de l'extrémisme pouvant mener au terrorisme, en ce compris le processus de radicalisation ».

> Article 44/2 §2 LFP : lorsque l'exercice conjoint, par tout au partie des autorités, organes, organismes, services, direction au commission visés à l'article 44/11/3ter, chacun dans le cadre de ses compétences légales, des missions de prévention et de suivi du terrorisme (…), nécessite que ceux-ci structurent les données à caractère personnel et les informations relatives à ces missions de sorte qu'elles puissent pétré directement retrouvées, ces données à caractère personnel et ces informations sont enregistrées dans les banques de données commune, sous leur responsabilité et suivant leurs procédures internes de validation, conformément aux règles qui sont déterminées par le Roi après avoir recueilli l'avis de l'organe de contrôle.

[61] AR TF consolidé.
[62] AR PH.
[63] LFP, article 44 /3 bis §9 et §10 et article 4 AR TF et AR PH.

Les notions de terrorisme, d'extrémisme et de processus de radicalisation[64] sont empruntées aux services du renseignement[65] pour atteindre « le plus grand dénominateur commun »[66]. Toutefois, l'extrémisme n'est volontairement envisagé que dans sa dimension « pouvant mener au terrorisme »[67].

La notion de *suivi* du terrorisme ou de l'extrémisme pouvant mener au terrorisme est, quant à elle, entendue dans un sens large et couvre les actions nécessaires pour lutter contre ces phénomènes. Concrètement, il faut entendre par là, outre le suivi plus stratégique et le suivi dans le cadre du travail des services de renseignement, les missions de police judiciaire et de police administrative ainsi que la recherche et les poursuites pénales. Dans ce cadre, les banques de données communes doivent permettre aussi aux autorités administratives, de police administrative ou de police judiciaire de prendre des décisions, dont des mesures.

2.4 Finalités du traitement

Les finalités du traitement[68] sont l'analyse, l'évaluation et le suivi de personnes enregistrées. Autrement dit, la mise en commun des données vise à permettre l'évaluation de la menace potentielle que représentent ces personnes et assurer un suivi afin d'anticiper et d'empêcher de possibles actes terroristes de leur part.

Tout comme en matière de données policières, l'enregistrement et le traitement des données est conditionné à leur caractère adéquat, pertinent et non excessif au vu de cette finalité[69].

Les BDC jouent ainsi un rôle important dans le suivi des entités de type HTF, FTF, PH, EPV ou CT car elles assurent un flux d'informations permanent. Ces BDC sont un instrument permettant d'établir la meilleure image possible de l'intéressé, de procéder à une évaluation

[64] Le processus de radicalisation est entré dans la notion de terrorisme par la loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259 bis du Code pénal.
[65] Article 8, 1° b et c et article 3, 15° loi du 30 novembre 1998 : Terrorisme : le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ces objectifs par la terreur, l'intimidation ou les menaces ; Extrémisme : les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'Etat de droit ; Processus de radicalisation : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes.
[66] Avis CPV 57/2015 sur l'avant-projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme, *Doc. Parl.,* Ch, 54 1727/001, p. 71.
[67] Loi BDC, *Doc.Parl.*, Ch., 54 1727/001, p. 13 : « L'objectif poursuivi par le projet de loi est de limiter le champ d'application possible en matière d'extrémisme, car, comme le souligne la Commission (de protection de la vie privée), l'extrémisme au sens de la loi du 30 novembre 1998 n'est pas une infraction ou un fait punissable ».
[68] Article 2 AR TF consolidé et AR PH.
[69] Article 4, al. 5 AR TF consolidé et AR PH.

pertinente de la menace individuelle et d'organiser le suivi approprié. À cette fin, toutes les informations et tous les renseignements relatifs aux entités dont disposent les différents services concernés, sont centralisés par le biais d'une *fiche de renseignement* personnelle[70].

De manière générale, la confrontation des données des différents services relativement à une même entité dans la BDC doit également permettre aux services concernés de détecter plus aisément d'éventuelles contradictions dans les données et d'y apporter les corrections qui s'imposent.

2.5 Catégories de personnes

Théoriquement, les BDC peuvent viser des enregistrements relatifs à des personnes physiques mais aussi à des personnes morales, des groupements ou des phénomènes (au sens de l'article 44/5 §1 LFP). Il semble toutefois qu'en pratique, seules les données relatives à des personnes physiques soient effectivement enregistrées.

Les définitions successives des entités visées ont épousé la chronologie des évènements tragiques qui ont touché la Belgique et le reste de l'Europe suite à la guerre en Syrie et l'avènement du proto État islamique (Daech).

2.5.1 Foreign Terrorist figther

Entre 2011 et 2014, un engouement est observé dans certains quartiers belges vis-à-vis de l'évolution de cette guerre, suivi d'un nombre inattendu et relativement élevé de départs vers les zones de conflit. En considération des conséquences potentiellement dramatiques de ces départs tant pour les personnes elles-mêmes que pour la sécurité du pays, les autorités tenteront de suivre le parcours de ces personnes. Le recours à la notion de 'Foreign Terrrorist Fighters' est ainsi totalement situé dans l'actualité politique de la guerre en Syrie.

Article 6, AR FTF

Toute personne résidant en Belgique ou ayant résidé en Belgique, ayant ou non la nationalité belge et qui, dans le but de se rallier à des groupements terroristes ou de leur fournir un soutien actif ou passif, se trouve dans l'une des situations suivantes :

- elle s'est rendue dans une zone de conflit djihadiste ;
- elle a quitté la Belgique pour se rendre dans une zone de conflit djihadiste ;
- elle est en route vers la Belgique ou est revenue en Belgique après s'être rendue dans une zone de conflit djihadiste ;
- elle a, volontairement ou involontairement, été empêchée de se rendre dans une zone de conflit djihadiste ;
- elle a l'intention de se rendre dans une zone de conflit djihadiste à la condition que des indications sérieuses démontrent cette intention ;

Sont également enregistrées les personnes à propos desquelles il existe de sérieux indices qu'elles puissent remplir les critères du FTF.

[70] Article 1, 11° AR TF consolidé et article 1, 14° AR PH.

Cinq catégories ont été créées. Numérotées de 1 à 5, elles correspondent à la situation des personnes concernées. La catégorie 1 regroupe les personnes présumées en Syrie ou en Irak, la catégorie 2 les personnes présumées en route vers les zones de conflit djihadistes, la catégorie 3 les personnes présumées en Belgique après un séjour en Syrie ou en Irak, la catégorie 4 les personnes présumées avoir tenté d'aller en Syrie ou en Irak et la catégorie 5 les personnes considérées comme des candidats potentiels. L'intitulé des catégories comme leur importance ont évolué au cours de temps en fonction du conflit.

La zone de conflit djihadiste est définie [71] comme « le territoire en proie à une lutte livrée afin de propager, d'imposer ou de protéger de manière violente une vision de la religion islamique. Pour coordonner les visions opérationnelles et politiques, ces territoires sont définis par le Conseil national de sécurité, sur proposition conjointe des ministres de l'Intérieur et de la Justice qui, eux-mêmes, se basent notamment sur une analyse stratégique effectuée par l'OCAM ».

2.5.2 Homegrown Terrorist Fighter

En 2015, la situation en Belgique devient critique dans la mesure où, sur son territoire même, une cellule djihadiste (dite Cellule de Verviers) est signalée et démantelée avant qu'elle ne puisse commettre un attentat. La menace extérieure devient intérieure. Il faut pouvoir suivre dans la BDC les personnes qui souscrivent à l'idéologie djihadiste mais qui n'ont pas l'intention de se rendre en Syrie. Les enregistrements doivent être étendus à tous ceux qui soutiennent cette idéologie, qu'ils aient ou non l'intention de partir en zone djihadiste. Mais l'État belge profite de cette situation pour également viser toute personne ayant des velléités terroristes, de quelque bord qu'elles soient. On parle dès lors de Homegrown Terrorist Fighters (HTF).

Article 7 AR HTF qui modifie l'article 6 de l'AR FTF en ajoutant dans la BDC TF la catégorie suivante :
Toute personne physique qui a un lien de rattachement avec la Belgique lorsqu'au minimum une des deux conditions suivantes est remplie :

a) il existe des indications sérieuses que la personne concernée a l'intention de recourir à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces ;
b) il existe des indications sérieuses que la personne donne intentionnellement un soutien, notamment logistique, financier ou aux fins de formation ou de recrutement, aux personnes visées sous a) ou aux personnes enregistrées en tant que Foreign Terrorist Fighters pour lesquelles il existe des indications sérieuses qu'elles ont l'intention de commettre un acte violent.

Sont également enregistrées les personnes à propos desquelles il existe des indications sérieuses qu'elles puissent remplir les critères du HTF.

Toutes les formes d'extrémisme sont donc dorénavant visées et non plus seulement les velléités 'djihadistes'.

[71] Article 1, 13° AR TF consolidé.

Le rapport au Roi[72] précise que les indications sérieuses ne peuvent se fonder uniquement sur les motivations personnelles du potentiel HTF mais également et surtout sur des actes matériels préparatoires d'un attentat. Une indication sérieuse a trait à une situation qui peut être étayée par des éléments concrets[73].

Les exemples suivants des situations visées dans la condition a) sont repris dans le rapport au Roi :

- un partisan de l'État islamique qui, depuis une prison en Belgique, projette de commettre un attentat après sa libération, et ce pour le compte de l'État islamique ;
- un partisan belge de l'État islamique qui est sollicité ou inspiré depuis la Syrie ou l'Irak par des membres de l'État islamique en vue de commettre des attentats en Belgique ;
- un militant d'extrême-droite préparant des actions terroristes contre un centre de réfugiés pour des motifs idéologiques.

Et d'ajouter, « par contre, ne sera pas reprise comme H.T.F. une personne qui, par exemple, part se battre en Ukraine de l'Est ».

En ce qui concerne les situations visées dans la condition b), le rapport au Roi cite, à titre d'illustrations :

- une personne apportant volontairement un soutien financier à un groupe belge d'extrême-droite connu pour planifier des actes de terrorisme en Belgique ;
- une personne apportant un soutien financier à une autre personne, cette dernière recrutant personnellement d'autres personnes en Belgique afin de les envoyer combattre dans une zone de conflit djihadiste.

Par contre, ne sera pas reprise comme HTF une personne belge radicalisée, sympathisante de l'État islamique, dès lors qu'elle n'apporte aucun soutien quelconque (logistique, financier, ...) à l'État islamique. Cette personne pourra par contre se retrouver dans la base de données de la police (voir ci-avant la section relative à la BNG).

En ce qui concerne la notion de rattachement avec la Belgique, le rapport au Roi précise qu'il y a nécessité de maintenir une certaine flexibilité : ce qui importe, c'est de déterminer un lien fondé, qu'il soit d'ordre juridique ou factuel entre le HTF et la Belgique. Par exemple, dans le cas d'un HTF, de nationalité belge qui aurait l'intention de réaliser un attentat en France, le lien retenu serait d'ordre juridique, à savoir la nationalité belge de l'intéressé. Dans le cas d'un HTF de nationalité étrangère et résidant en France qui donnerait intentionnellement un soutien logistique à un groupe terroriste basé en Allemagne en vue de réaliser un attentat en

[72] Rapport au Roi précédent AR HTF.
[73] Rapport au Roi précédent AR HTF.

Belgique, le lien retenu serait d'ordre factuel, c'est-à-dire le lieu de l'attentat potentiel, à savoir la Belgique.

2.5.3 Propagandiste de haine

Depuis l'adoption du plan R et la mise en place d'une JIB, l'OCAM tenait une liste des entités considérées comme des vecteurs de radicalisation, il fut néanmoins décidé, en 2018, de créer une BDC qui vise cette fois, les personnes qui n'ont pas à proprement parler de velléité terroriste mais qui, par leurs paroles ou leurs écrits, incitent d'autres à se rebeller de manière violente contre le statu quo démocratique.

Article 6 AR PH
Les personnes physiques ou morales, les associations de fait et les moyens utilisés, indépendamment de leur nationalité, de leur lieu de résidence ou lieu d'établissement, qui répondent aux critères cumulatifs suivants :

a) ont pour objectif de porter atteinte aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux fondements de l'Etat de droit ;
b) justifient l'usage de la violence ou de la contrainte comme moyen d'action ;
c) propagent leurs convictions pour exercer une influence radicalisante ;
d) ont un lien de rattachement avec la Belgique.

Sont également enregistrées les entités à propos desquelles il existe de sérieux indices qu'elles puissent remplir les critères de propagandiste de haine.

Le but, cette fois, est de mettre en commun les données et informations relatives aux vecteurs de la radicalisation, étant personnes physiques ou morales, associations de fait ainsi que de l'ensemble des moyens utilisés par ceux-ci (tels que un site web, des tracts, des messages radio ou télévisé, des chaines de radio ou de télévision, des centres de propagande ou culturels, des locaux, etc.).

En ce qui concerne la violence, le commentaire par article de l'arrêté royal précise que toutes les formes de violence ou de force sont visées : physique, psychique, intra et extrafamiliale, homophobe, cyber-attaques, etc. L'intention (de porter atteinte aux institutions démocratiques) doit être extériorisée publiquement, au travers par exemple d'une publication et la notion d' « influence radicalisante » s'entend comme le fait pour la personne de soutenir ou de participer à un processus de radicalisation.

L'entité doit être active en Belgique ou développer des activités, par divers moyens, dont les effets radicalisants sont perceptibles dans notre pays, mais elle ne doit pas nécessairement ni avoir la nationalité belge, ni séjourner en Belgique ou avoir séjourné en Belgique.

On trouve ainsi dans le commentaire par article, les exemples suivants [74] :

[74] AR PH, commentaire article 6.

- une personne manifestant publiquement, en Belgique, son intention de radicaliser d'autres personnes. Le lien juridique retenu dans ce cas est la nationalité belge du propagandiste de haine ;
- une personne étrangère qui réside en Belgique mais exerce son influence radicalisante à l'étranger. Le lien juridique retenu dans ce cas est le séjour en Belgique ;
- Une personne étrangère, résidant à l'étranger et qui diffuse dans d'autres pays que la Belgique un message à la suite duquel une influence radicalisante s'exerce spécifiquement en Belgique ou vise la Belgique. Dans ce cas, le lien factuel retenu sera l'influence radicalisante exercée effectivement en Belgique.

Toujours selon le rapport au Roi, les différentes conditions d'application de cette définition permettrait d'éviter l'enregistrement de personnes ayant 'simplement' une idéologie radicale précise.

2.5.4 Extrémistes Potentiellement Violents

Ce focus sur la prévention, bien en amont des actes terroristes, a, en sus de la terreur engendrée par les attentats eux-mêmes, suscité chez les autorités publiques la volonté de repérer et surtout enregistrer tout ce qui, selon leur propre définition, pouvait être suspecté de radicalisation. Cette multiplication des définitions comme des listes dressées[75] a poussé les autorités à vouloir recentraliser cette information dans la première BDC en en élargissant le champ d'application aux Extrémistes Potentiellement Violents (EPV). Cependant, ce faisant, la définition des entités visées par les BDC est devenue extrêmement large et particulièrement complexe.

AR 20 décembre 2019, article 6 modifiant l'article 6 de l'AR 21 juillet 2016, ajout dans la BDC TF de la catégorie suivante :
Toute personne qui a un lien avec la Belgique et qui remplit les critères cumulatifs suivants :

a) elles ont des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique ;
b) il existe des indications fiables qu'elles ont l'intention de recourir à la violence, et ce en relation avec les conceptions mentionnées en a)
c) elles répondent au minimum à une des conditions suivantes augmentant le risque de violence :

- elles entretiennent systématiquement des contacts sociaux systématiques au sein de milieux extrémistes ;
- elles ont des problèmes psychiques constatés par un professionnel compétent en la matière ;
- elles ont commis des actes ou présentent des antécédents qui peuvent être considérés comme soit :
    - un crime ou un délit portant atteinte ou menaçant l'intégrité physique ou psychique de tiers ;
    - des instructions ou des formations relatives
        - à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses
        - ou pour d'autres méthodes ou techniques spécifiques ou vue de commettre des infractions terroristes conformément à l'article 137 du Code pénal
    - des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation ou d'un réseau terroriste/extrémiste ;

[75] Dont par exemple au niveau de la Direction Générale des Etablissements Pénitentiaires, les suivis Celex.

- des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.

Sont également enregistrées les personnes à propos desquelles il existe de sérieux indices qu'elles puissent remplir les critères d'extrémisme potentiellement violent.

Selon le ministre de la Justice[76], « cette extension est justifiée par le souci de centraliser l'information relatives aux ' radicalisés ' et ainsi éviter la création et l'existence de listes diverses basées sur des critères différents. Ainsi, les personnes suspectées par l'administration pénitentiaire comme ' en voie de radicalisation ' durant leur séjour en prison et alors qu'elles ne sont pas suspectées, ni condamnées pour une infraction terroriste, et ne peuvent être considérées ni comme FTF, ni comme HTF, ni comme PH, seront dorénavant inscrites dans la BDC sous la catégorie EPV». Comme nous le verrons ci-après, l'administration pénitentiaire recense et suit effectivement (« suivis Celex ») les personnes soupçonnées, au sein de l'établissement, de radicalisation (Nederlandt, 2019 :153-162).

Selon le rapport au Roi, le raisonnement qui sous-tend la création de cette nouvelle catégorie se base sur le fait qu'il s'est avéré indispensable de pouvoir suivre à travers la banque de données Terrorist Fighters, une fraction d'individus dont les services estiment qu'ils représentent un risque accru de violence, même s'ils ne sont pas encore passés à l'acte.

Le gouvernement reconnaît que la définition des EPV présente de fortes similitudes par rapport à celle des HTF mais les distingue néanmoins en les considérant comme complémentaires. Selon le rapport au Roi, la validation en tant qu'HTF suppose que l'individu a déjà fait des démarches ou entrepris des actes d'exécution. Il s'agit dans «presque tous les cas de personnes qui sont arrêtées in extremis dans la mise en exécution d'un projet concret ou de personnes qui sont parvenues à mettre à exécution leurs projets sans avoir été repérées par les services concernés » [77]. Il n'en est pas de même en ce qui concerne les EPV pour lesquels aucun acte matériel préparatoire ne doit avoir été posé[78].

Toujours selon le rapport au Roi, les critères utilisés sont en grandes lignes les mêmes indicateurs qui sont actuellement à la base des « instruments d'évaluation des risques » qui sont utilisés pour estimer dans quelle mesure certains individus comportent un risque plus élevé de violence extrémiste. Les indicateurs relatifs aux EPV ne sont donc pas choisis au hasard, mais sont considérés comme étant les éléments principaux à prendre en compte afin de juger s'il s'agit d'un risque accru de violence. La raison d'être de cette nouvelle catégorie est donc grâce à un suivi commun et intégral, de dresser les priorités au sein de la fraction du spectre extrémiste qui peut être considérée comme comportant un risque élevé de violence. Il s'agit aussi bien d'individus incarcérés que de personnes en liberté.

[76] Communiqué de presse de Koen Geens du 9 décembre 2019.
[77] Rapport au Roi précédent AR EPV.
[78] On peut se demander dans ce cas comment peut être justifié l'enregistrement d'une telle entité dans une banque de données intitulée 'Terrorist Fighters', mise en place dans le cadre de la prévention du terrorisme et de l'extrémisme pouvant mener au terrorisme.

Le lien de l'EPV avec la Belgique peut être d'ordre juridique (nationalité belge, droit de séjour en Belgique, …) ou factuel (un séjour - légal ou non - en Belgique, un séjour dans une prison belge ou dans une institution belge pour internés, …). Il importe de déterminer un lien fondé et durable, qu'il soit d'ordre juridique ou factuel. Il y a nécessité de maintenir une certaine flexibilité dans l'établissement du lien avec la Belgique[79].

Les conceptions extrémistes de la personne doivent justifier l'usage de la violence ou de la contrainte comme méthode d'action en Belgique. Le rapport au Roi cite, à titre d'exemple, un partisan de l'État Islamique étant donné que ce groupement terroriste propage des actions violentes en Occident et en Belgique. Les EPV sont donc des individus qui ont intériorisé une idéologie, une religion ou une conception politique qui justifie l'usage de la violence comme méthode d'action en Belgique.[80]

Un degré de certitude élevé des conceptions doit être établi. *«* Il convient d'analyser le contexte particulier pour faire cette déduction. Une personne qui s'exprime sur les réseaux sociaux comme un fervent partisan de l'État Islamique, ne jure que par ce groupement et applaudit aux attentats perpétrés par les partisans de ce groupement en Europe peut être considérée comme ayant des conceptions qui justifient l'usage de la violence dans notre pays pour des raisons idéologiques/religieuses. Il en va de même pour un fervent partisan d'un groupement d'extrême droite réputé pour sa légitimation de la violence ou pour son incitation à recourir à celle-ci contre, par exemple, les demandeurs d'asile ou les musulmans. En tout cas, le degré de certitude doit être élevé quant à l'exactitude de l'information relative aux attitudes et conceptions de la personne concernée *»*[81].

Le deuxième critère porte sur l'existence d'indications selon lesquelles la personne concernée a l'intention de recourir à la violence, et ce en conformité avec ses conceptions extrémistes. Il s'agit d'indications préliminaires révélant une certaine intention dans le chef de la personne concernée, sans qu'il y ait d'indications sérieuses relatives à des actes préparatoires.

Le fait qu'il existe une certaine intention dans le chef de la personne concernée peut être établie de différentes manières. Il peut s'agir par exemple « de menaces spécifiques qui sont adressées par la personne concernée à des tiers (avec ou sans fonction officielle), ou de renseignements indirects recueillis par les services. En tout cas, aucune action matérielle spécifique ne doit encore être présente pour pouvoir parler de l'existence de " l'intention ". Toutefois, l'information dont l'on dispose pour conclure qu'il existe une certaine " intention " dans le chef de la personne concernée, doit être jugée comme étant fiable et ne peut être basée que sur de simples rumeurs »[82].

[79] La description et le commentaire de l'ensemble des critères et sous critères de cette nouvelle catégorie EPV se retrouvent dans le Rapport au Roi précédent AR EPV.
[80] Rapport au Roi précédent AR EPV.
[81] Rapport au Roi précédent AR EPV.
[82] Rapport au Roi précédent AR EPV.

Le troisième critère constitue en réalité une analyse de risques de la personne. Il s'agit, selon le rapport au Roi, de facteurs présents dans le chef de la personne concernée et qui augmentent le risque de violence.

Ainsi, si une personne entretient systématiquement des contacts avec d'autres extrémistes et est fortement impliquée dans un tel environnement, cela peut légitimement être considéré comme un facteur de risque supplémentaire. Il peut s'agir de personnes ayant déjà un statut spécifique (HTF, PH, FTF), mais cela ne doit pas nécessairement être le cas, étant donné qu'également des individus sans "statut" ont parfois des conceptions très extrémistes.

Un deuxième sous-critère concerne les problèmes psychiques. Il s'agit de la présence ou de l'absence d'un ou de plusieurs problèmes psychiques qui augmentent le risque que survienne un comportement violent (troubles de la personnalité, troubles psychiatriques, trouble lié à une substance). Les problèmes psychiques doivent toujours être constatés par un professionnel compétent en la matière. C'est l'OCAM, in fine, qui apprécie le plus précisément possible, sur la base de ces informations, le danger représenté par la personne en question.

Le troisième sous-critère se concentre sur les actes et les antécédents spécifiques de la personne : « On examine notamment les antécédents violents (judiciaires) et les capacités d'une personne. Il se peut que la personne concernée ait déjà été condamnée par le passé pour des infractions violentes ou qu'elle ait suivi des formations spécifiques au maniement des armes ou à la fabrication d'explosifs ou à d'autres méthodes et techniques en vue de commettre des infractions terroristes. De même, la personne concernée peut avoir déjà prouvé qu'elle n'hésite pas à utiliser la violence comme méthode d'action, à la suite de quoi certains " seuils " ont déjà été dépassés. Il peut également arriver que la personne concernée commette ou ait commis des actes qui peuvent être considérés comme apportant un soutien matériel à une organisation ou à un réseau terroriste/extrémiste, par exemple, en soutenant financièrement un tel groupe ou en rendant divers autres services. Ces actes doivent être suffisamment graves et intentionnels pour être repris dans ce critère. L'intention de porter gravement préjudice en apportant un soutien à une organisation ou un réseau terroriste/extrémiste doit être claire »[83].

Enfin, est également envisagé comme un critère de risque accru le fait que la personne concernée présente des comportements qui impliquent une vigilance anormale à l'égard de la sécurité, p. ex. l'utilisation de certaines techniques de contre-surveillance.

2.5.5 Les condamnés pour une infraction terroriste

[83] Rapport au Roi précédent AR EPV.

Pour terminer, sont dorénavant également enregistrés dans les BDC, les condamnés pour une infraction terroriste.

AR 20 décembre 2019, article 6 modifiant l'article 6 de l'AR 21 juillet 2016, ajout dans la BDC TF de la catégorie suivante :
Les personnes physiques qui ont un lien avec la Belgique et qui remplissent les deux critères cumulatifs suivants :
a)

- elles ont été condamnées par un jugement ou un arrêt passé en force de chose jugée pour une infraction terroriste visée au Livre II, Titre Ier du Code Pénal ou elles ont été condamnées à l'étranger par un jugement ou un arrêt passé en force de chose jugée pour des faits qui peuvent être qualifiés d'infractions terroristes visées au Livre II, Titre Ier du Code Pénal ou,
- elles ont fait l'objet d'une mesure de protection passée en force de chose jugée prise par un tribunal de jeunesse pour des faits qualifiés d' infractions terroristes visées au Livre II, Titre Ier du Code Pénal ou elles ont fait l'objet d'une telle mesure ou ont été condamnées définitivement à l'étranger pour des faits qui peuvent être qualifiés d'infraction terroriste sur la base du Livre II, Titre Ier du Code Pénal ou,
- elles ont fait l'objet d' une décision judiciaire d'internement passée en force de chose jugée, pour une infraction terroriste visée au Livre II, Titre Ier du Code Pénal, ou ont fait l'objet d'une telle mesure à l'étranger pour des faits qui peuvent être qualifiés d'infraction terroriste sur la base du Livre II, Titre Ier du Code Pénal ;

b) L'OCAM leur a attribué un niveau de la menace « Niveau 2 ou MOYEN », « Niveau 3 ou GRAVE » ou « Niveau 4 ou TRES GRAVE » conformément à l'article 6, § 1er, de l'arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace.

Selon le rapport au Roi, l'objectif de l'insertion des condamnés pour infraction terroriste dans la BDC est d'assurer le flux d'information vers tous les services de base et partenaires. De la sorte, tous les acteurs qui doivent assurer un suivi de 'personnes condamnées pour terrorisme' (tels que la DG EPI, les Maisons de Justice, la police, les centres fermés, la Sûreté de l'État, les TFL, …) peuvent être informés, de manière proactive et en temps utile, de la situation des personnes concernées. Concrètement, des informations peuvent par exemple être échangées à propos de l'évolution de la personne, ses contacts, sur ses perspectives de libération.

Une condamnation définitive pour terrorisme à l'étranger est également visée.

2.6 Données et informations

Concrètement au niveau des personnes, le spectre de l'information enregistrable est très large. Il s'agit des données socio biographiques (nationalité, lieu de résidence, …), judiciaires (détention préventive dont la mise sous surveillance électronique, libération conditionnelle, existence d'un mandat d'arrêt international ou européen, fixation d'une affaire pénale devant une instance judiciaire, condamnation/acquittement pour un délit terroriste, …), administratives (décision de l'Office des Étrangers, …), de police administrative (appartenance à un groupement suspecté de terrorisme, …), des services de renseignements (médias sociaux, …).

La même limite générale[84] que pour les bases de données de la police s'impose aux BDC, à savoir que les données ne peuvent être enregistrées et conservées que si elles sont :

- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ;
- exactes et si nécessaires, mises jour.

Les BDC ne contiennent officiellement que des informations non classifiées[85].

2.7 Le processus d'alimentation des BDC

Les BDC ne sont pas alimentées par une liaison automatique avec d'autres banques de données mais bien par de nouveaux enregistrements réalisés par différents acteurs en fonction des informations dont ils disposent, éventuellement dans leur propre banque de données.

L'information initiale peut provenir soit du terrain local[86] qui, constatant des signes de « radicalisation » en informe les instances supérieures[87] (circuit ascendant), soit des services fédéraux qui prennent alors l'initiative de l'insertion dans les BDC, l'information devenant ainsi disponible aux autorités locales (circuit descendant).

L'inscription d'une nouvelle entité dans une BDC ne peut être réalisé que par un des quatre services dits de « base », à savoir la police, la Sûreté de l'Etat, le Service Général du Renseignement et de la Sécurité ou encore l'OCAM ; en fonction de l'information dont il dispose, le service peut soit introduire l'entité sous le statut de « pré-enquête »[88], soit sous une des cinq catégories des BDC (FTF, HTF, PH, EPV, CT).

L'inscription d'une entité en « pré-enquête » démarre une phase d'enrichissement de l'information notamment par les services « partenaires » qui sont : (1) la Direction générale des Établissements pénitentiaires, (2) les établissements pénitentiaires, (3) la Direction générale du Centre de Crise (SPF Intérieur), (4) la Direction générale Sécurité et Prévention

[84] Article 4 al. 4 AR TF et article 4, 4° AR PH.

[85] Il est néanmoins clairement dit dans le rapport au Roi précédent l'AR FTF que les informations classifiées ne seront néanmoins pas ignorées. Ces informations seront traitées dans d'autres systèmes et seront notamment partagées au sein des TFL, ou alors elles seront déclassifiées.

[86] Bourgmestres, Cellule Sécurité Intégrale Locale (CSIL) R, Task Force Locale (TFL), maisons de justice, établissement pénitentiaires.

[87] OCAM, Task Force Nationale (TFN).

[88] L'enregistrement d'un condamné pour une infraction terroriste dans la catégorie de pré-enquête n'est pas possible puisque dans ce cas, on ne peut, à l'évidence, parler de soupçons devant être confirmés ou infirmés par une phase d'enquête. Le fait d'avoir été condamné pour une infraction relevant de la législation « anti terroriste » suffit à être enregistré sous le statut de « condamné terro ».

du Service public fédéral Intérieur, (5) le Ministère public[89], (6) la Cellule de traitement des informations financières (CTIF), (7) l'Office des Étrangers (OE), (8) l'Autorité Nationale de Sécurité[90] (ANS), (9) le Service des Cultes du SPF Justice (pour ce qui concerne les PH[91]) et (10) l'administration générale de la trésorerie du SPF Finances [92]. Cet enrichissement doit permettre à l'OCAM, au bout de maximum 6 mois, de confirmer ou non l'inscription de l'entité sous un statut des BDC (FTF, HTF, PH, EPV) [93].

L'enrichissement de l'information est continu et dynamique. Autrement dit, tous les services qui ont accès aux BDC ont l'obligation d'alimenter constamment celle-ci grâce aux données et informations dont ils disposent relativement à l'entité considérée[94]. Selon le gouvernement, un tel flux a un double usage. Il permet non seulement d'évaluer à tout moment la menace éventuelle présentée par l'entité et de décider de la réponse à y apporter, mais aussi, en confrontant les informations communiquées par différents services, de vérifier leur qualité, une discordance indiquant un problème potentiel.

Dans le cadre de leurs missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions, les maisons de justice participent également à ce processus d'alimentation[95].

Afin de garantir la qualité des enregistrements, un double système de validation est mis en place : (1) en interne, par le service qui souhaite introduire l'information dans la BDC[96] ; (2)

[89] Si le Ministère Public a accès direct aux BDC, il est cependant dispensé d'une obligation d'alimentation car celle-ci est réalisée par la police, voir COL CPG 22/2016, point 1.6. : « L'article 44/11/3ter §4 énumère les services devant alimenter les banques de données communes. Ce principe ne s'applique pas au ministère public, qui a donc un accès direct mais n'est pas un service fournisseur immédiat. En ce qui concerne les informations à caractère judiciaire, l'alimentation par la police est en effet suffisante, puisque l'enquête pénale est réalisée par celle-ci, sous la direction et l'autorité du ministère public et que les renseignements figurant dans le dossier du parquet proviennent presque entièrement de la police et qu'ils sont, quoiqu'il en soit, partagés avec elle ».

[90] Article 8, AR TF consolidé et AR PH. L'objectif est de permettre à l'ANS de faire état dans la BDC de ses décisions en matière d'habilitations de sécurité.

[91] Article 7 §1er al.3, AR TF consolidé et AR PH.

[92] L'autorité compétente en matière de sanctions financières par le gel des fonds et des ressources économiques des personnes et entités qui commettent ou tentent de commettre des infractions terroristes, les facilitent ou y participent. L'objectif est d'une part lui permettre de répondre aux questions des autres États et d'autre part, pouvoir insérer dans la BDC les décisions qu'elle prend à l'égard d'une personne reprise dans les BDC, Rapport au Roi précédent l'AR EPV, *op.cit*.

[93] Étant donné cette période d'incertitude quant à la validité de la donnée enregistrée sous la catégorie de « pré-enquête », tant qu'elle n'a pas été confirmée par l'OCAM, le système prévoit que les services qui ont pris connaissance de cette inscription en « pré-enquête », par la voie d'une interrogation directe (voir ci-après sous les accès aux BDC) sont obligés de réinterroger la BDC, à l'issue de ce délai maximum de 6 mois, pour savoir si ladite inscription a été validée ou non.

[94] Toujours dans la limite générale de la pertinence, de l'adéquation et du caractère non excessif de cette transmission au regard des finalités des BDC.

[95] Article 7 §1, al.5,, AR TF consolidé et AR PH.

[96] Article 8 §1, AR TF consolidé et AR PH.

par l'OCAM lors de son évaluation de la pertinence de l'insertion de l' information dans la BDC[97].

2.8 Les accès aux données et informations contenues dans les BDC

De nombreux services ont, d'une manière ou d'une autre, un intérêt, pour exercer leurs missions, à avoir accès aux données enregistrées dans les BDC. Tous ne sont cependant pas sur un pied d'égalité à cet égard. Certains collectent davantage d'informations tandis que d'autres ont plutôt besoin des informations collectées pour assurer le suivi des personnes dont ils ont la charge. Étant donné le caractère sensible des données concernées, il y a lieu de veiller à l'équilibre (difficile) entre la protection des citoyens contre l'utilisation abusive de données les concernant et la nécessité d'échanger certaines informations pour assurer la sécurité de l'ensemble de la société. C'est la raison pour laquelle une gradation des accès aux BDC a été prévue en fonction des services concernés.

On distingue à cet égard les services qui ont un accès direct aux BDC, ceux qui disposent d'un droit d'interrogation directe et ceux à qui un service de base peut, sous certaines conditions, communiquer l'information[98].

2.8.1 L'accès direct

L'accès direct[99] à l'ensemble des données et informations contenues dans les BDC est réservé aux services de base ainsi qu'aux services 'partenaires' suivants : la DG EPI et les établissements pénitentiaires, le Ministère Public, la Cellule de Traitement des Informations Financières et l'Office des Étrangers.

Certains autres services 'partenaires' disposent également d'un droit d'accès direct mais limité à certains domaines. Il s'agit (1) des services assurant des missions légales d'accompagnement judiciaire et de la surveillance d'auteurs d'infractions. Leur accès direct est limité aux données et informations des personnes dont ils assurent le suivi[100] (2) de l'Autorité Nationale de Sécurité (ANS) aux fins d'y intégrer ses propres décisions en matière d'habilitations, d'attestations et d'avis de sécurité, et (3) de l'administration générale de la

[97] En cas d'insertion par un service de base directement sous un des statuts de la BDC, l'OCAM dispose d'un délai de 15 jours pour valider ou non l'information, AR TF consolidé et AR PH, article 4, al. 2.

[98] Ce sont les mêmes modalités que celles prévues pour l'accès aux données de la BNG (voir ci-avant) mais ici, ces droits d'accès sont une réalité par les arrêtés d'exécution qui ont été pris, à l'inverse de ce qui se passe pour la BNG où la loi (LFP) autorise le principe des accès mais où aucun arrêté royal (sauf pour l'OE et de manière limitée pour le SPF Justice) ne les implémente concrètement.

[99] Article 7 §1, al.1 AR TF consolidé et AR PH.

[100] Article 7 §1, al. 5 et 6 AR TF consolidé et AR PH. Ces services sont considérés comme des partenaires de la chaine pénale et à ce titre, doivent d'une part, être informés des éventuelles dérives radicales des personnes dont le suivi leur est confié et d'autre part, alerter les services en charge de la sécurité, lorsqu'elles soupçonnent une éventuelle dérive radicale dans le chef d'un justiciable qu'elles suivent.

Trésorerie du Service Public Fédéral Finances[101] dont le droit est limité à son cadre de compétence en matière de sanctions financières[102].

2.8.2 L'interrogation directe

À côté de ces droits d'accès direct, il fut également considéré que certains services, pour exercer leurs missions, puissent avoir un intérêt à interroger les BDC sur l'une ou l'autre entité qu'ils ont dans le viseur. Dans ce cas, ces services doivent demander à un des services de base si la personne ou entité qu'ils visent, est ou non enregistrée dans une BDC. Dans l'affirmative, ils peuvent alors prendre contact avec le service de base qui a introduit la donnée pour lui demander de plus amples renseignements.

Ce droit est reconnu aux services suivants : la Direction générale du Centre de crise, la Direction générale sécurité et Prévention du SPF Intérieur le SPF Affaires étrangères (Direction générale des Affaires consulaires) et les services d'enquête et recherche de l'Administration générale des douanes et accises[103].

Le Service des Cultes du SPF Justice dispose également d'un droit d'interrogation directe mais uniquement à la BDC PH[104].

Dans la perspective du développement d'une synergie entre les services (multiagency approach), ces interrogations directes doivent également être prises en compte par les services de base pour évaluer la situation de l'intéressé : par quel service la demande est faite, dans quel cadre, … et devrait permettre d'instaurer un nouveau système de communication entre le service interrogeant et le service de base.

2.8.3 La communication de certaines informations

2.8.3.1 *Aux autorités locales*

Dans la lignée du plan R et de la mise en place des Cellules de Sécurité Intégrale Locales en matière de Radicalisme[105], les autorités considèrent que la prévention du terrorisme et de l'extrémisme pouvant mener au terrorisme passe également et même principalement, par le niveau local. Selon cette idée, c'est au niveau local que, d'une part, les premiers signes de radicalisation d'une personne peuvent être décelés et que, d'autre part, le suivi des entités

[101] Rapport au Roi précédent l'AR EPV.
[102] Article 7 §1, al.7
[103] Article 7 §1, al.3 AR TF consolidé et article 7 §1, al.4 AR PH.
[104] Article 7 §1er al.3 de l'AR PH.
[105] Plan R, « Les cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme « CSIL-R » sont des plates-formes de concertation communales locales. Elles veillent à la cohérence des actions de prévention, de répression et de suivi ». Leur création est devenue obligatoire avec la promulgation de la loi du 30 Juillet 2018. Toutes les communes de Belgique sont désormais tenues d'en créer.

déstabilisées mais non dangereuses peut être assuré de manière socio-préventive. À cette fin, il a été prévu qu'une partie de l'information relative à une entité reprise dans une des BDC soit transmise au bourgmestre de la commune de résidence de la personne ou de celle qu'elle fréquente régulièrement ou qu'elle fréquente pour y organiser des activités [106] Le bourgmestre peut, en outre, au sein des CSIL-R, transmettre cette information aux services communaux et aux services des Communautés sur la base d'une évaluation de leur « besoin de savoir » contrebalancé par l'intérêt de protéger les données personnelles des personnes considérées[107].

En ce cas, ce n'est pas l'information complète[108] qui est transmise mais seulement les données à caractère personnel de la personne concernée[109], l'estimation par l'OCAM de la menace que la personne représente, la Task Force Locale[110] compétente et les mesures et modes de suivi adoptées. Ce modèle réduit est appelé 'carte d'information'. Sa transmission est strictement limitée au besoin d'en connaître du destinataire et ne peut concerner les entités encore sous la catégorie de « pré-enquête ». Pour celles-ci, seule une liste de noms peut être transmise.

2.8.3.2 *À des « tiers »*

Les services de base peuvent également transmettre des listes de noms pour les entités confirmées à des autorités ou services publics si la finalité de la liste s'inscrit dans les missions légales du destinataire et s'avère nécessaire au regard des objectifs spécifiques qui lui sont assignés.[111.]

[106] Article 12 §1 AR TF consolidé et AR PH.
[107] Article 12 §2 AR TF consolidé et AR PH.
[108] Article 1, 11° AR TF consolidé et article 1, 14° AR PH, La fiche de renseignement est la fiche personnelle qui continent toutes les données à caractère personnel et informations non classifiées (…), provenant de l'ensemble des services qui alimentent la banque de donnée.
[109] Article 1, 12° AR TF consolidé et article 1, 15° AR PH : La carte d'information est la fiche personnelle qui consiste en un extrait de la fiche de renseignements, contenant les données à caractère personnels et informations non classifiées (…), strictement limitées au besoin d'en connaître du destinataire (…). Si la personne est enregistrée sous le statut de FTF, on mentionnera également la catégorie à laquelle elle appartient : (1) s'est rendue en zone de conflit djihadiste, (2) a quitté la Belgique pour se rendre en zone de conflit djihadiste, (3) en route vers la Belgique après s'être rendue dans une zone de conflit djihadiste, (4) a été empêchée de se rendre en zone de conflit djihadiste, (5) a l'intention de se rendre en zone de conflit djihadiste.
[110] Selon le Plan R : « Les Taskforces locales (TFL) sont des plates-formes de concertation opérationnelles et stratégiques destinées notamment aux services de police et de renseignement et sont installées au sein d'une zone géographique délimitée. Elles se situent au niveau des arrondissements. Les TFL opérationnelles sont ancrées au niveau (supra)local, elles suivent les individus et groupements radicalisants au niveau local et proposent des mesures pour réduire l'impact de ces individus et de ces groupes. Elles échangent des informations, renseignements et analyses, les font concorder et entretiennent des contacts structurels et/ou ponctuels avec les autorités locales et leurs services. Elles peuvent proposer l'introduction d'informations dans la Joint Information Box, ou leur suppression. Elles offrent un appui aux intervenants de première ligne non spécialisés de la police qui sont confrontés aux signes d'une éventuelle radicalisation et elles peuvent proposer des mesures préventives ainsi que des mesures destinées à contrecarrer le processus et les faire appliquer ».
[111] Article 12 de l'AR TF consolidé et article 15 AR PH.

Cette possibilité est fortement encadrée par la législation : (1) la liste ne peut être communiquée qu'aux autorités publiques et organismes publics, (2) La finalité de la transmission doit s'inscrire dans les missions légales du destinataire, (3) l'utilisation de la liste par le destinataire n'est autorisée que dans le cadre de la finalité précisée, (4) les listes ne peuvent être conservées pour une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles ont été obtenues[112].

Il semblerait toutefois qu'à l'heure actuelle, les destinataires de ces listes soient nombreux et que la transmission de ces informations ne corresponde pas toujours aux exigences de sécurité et de finalité des textes de loi[113].

2.8.3.3 À des services de police, de renseignement ou d'analyse de la menace *situés à l'étranger*

Enfin, les données et informations peuvent également être transmises, y compris sous la forme de listes, par un service de base, et sous certaines conditions[114], à des services de police, de renseignement ou d'analyse de la menace situés à l'étranger.

2.9 Conséquences de l'enregistrement dans la BDC

Les individus enregistrés dans les BDC font l'objet d'un suivi policier proactif et de (très) nombreux signalements dont au niveau policier, au niveau du *Passenger Name Record*[115], dans le programme de l'union européenne de contrôle des frontières, Système d'information Schengen (SIS)[116] et dans la BNG si l'individu fait l'objet d'un ordre de quitter le territoire ou d'une interdiction d'entrée, … .

Dans le cadre du processus d'alimentation et d'enrichissement de l'information, tous les services 'partenaires' sont amenés à enquêter sur tous les aspects de la vie de la personne

[112] Rapport au Roi précédent AR EPV.
[113] Rapport concernant le contrôle conjoint de la banque de données commune Terrorist Fighters et Prédicateurs de Haine par le comité permanent R et l'organe de contrôle de l'information policière (à diffusion restreinte), 2019. Toutefois, il semblerait, selon une correspondance récente avec les services de l'OCAM, que cette problématique fasse actuellement l'objet d'une sérieuse réévaluation et devrait aboutir, prochainement, à une sécurisation plus importante de la BDC.
[114] Article 44/11/3quinquies LFP et article 15 de l'AR TF consolidé et AR PH.
[115] Au moment des départs ou arrivées sur le territoire belge, un croisement entre les données de voyage (avions) et les données des individus repris dans la BDC est opéré par l'Unité d'Information des Passagers (BelPIU).
[116] Le programme SIS II permet aux autorités compétentes des États Schengen d'entrer et de consulter des alertes concernant des personnes et des objets. Les motifs de l'alerte sont notamment le refus de l'entrée d'une personne qui n'a pas le droit d'entrer ou de rester sur le territoire Schengen, la recherche et la détention d'un individu pour lequel un mandat d'arrêt européen a été émis, la recherche d'une personne disparue, ou pour trouver des biens volés ou perdus, tels qu'une voiture ou un passeport, https://edps.europa.eu/data-protection/european-it-systems/schengen-information-system_fr#do;

concernée (Thomas, 2020 : 35-36) Celle-ci pourra donc faire l'objet d'enquêtes aux niveaux professionnel, fiscal, financier, social, etc.

De nombreuses mesures peuvent également être prises à son égard, tels que le retrait d'habilitations, des documents de voyage (passeports)[117], un gel de ses avoirs[118].

La nature, l'ampleur et le poids des mesures et du suivi varient en fonction de la catégorie à laquelle la personne est soupçonnée appartenir (FTF, HTF, PH, EPV, CT) mais également, en fonction de l'évaluation du risque qu'elle représente. Si le risque est grand, le dossier sera plutôt traité par les instances judiciaires. Si le risque est mitigé, un suivi plus administratif via les services communaux pourra être envisagé.

2.10 Durée de conservation des données et archivage

La règle générale est que la donnée ou l'information doit être supprimée de la BDC dès lors qu'elle ne présente pas ou plus un caractère adéquat, pertinent et non excessif par rapport à la finalité de la BDC[119]. C'est l'OCAM qui est chargé d'évaluer cette condition. Lorsqu'il considère que la donnée doit être supprimée de la BDC, il en informe également le service qui avait introduit la donnée en question pour lui permettre d'éventuellement adapter les enregistrements y relatifs dans sa propre banque de données.

À l'inverse, la suppression d'une donnée dans une banque de données propre à un des services alimentant n'entraine pas automatiquement la suppression de la donnée qui a été transmise à la BDC[120]. Cette situation résulte de l'existence de finalités différentes entre la banque de données « source » du service à l'origine de l'information et la BDC. Elle peut aussi apparaître en raison de règles de traitement différentes dont par exemple, la durée maximale de conservation des données.

Au-delà de ces règles générales, la législation prévoit qu'une évaluation du lien direct de la donnée avec les finalités de la BDC doit être effectuée par l'OCAM tous les 3 ans après le dernier traitement[121].

[117] sur décision de l'OCAM quand la personne présente un risque substantiel pour le maintien de l'ordre ou de la sécurité publique.
[118] sur la base d'une évaluation de l'OCAM, le Conseil des Ministres, sur l'avis du Conseil National de Sécurité, peut inscrire l'individu sur la liste nationale des personnes dont les fonds et les ressources économiques sont gelés ; cette liste est publique, voir à ce propos Remacle C. (2019).
[119] Article 4, al.5 AR TF consolidé et article 4, 4° AR PH. En tout état de cause, les enregistrements sous la catégorie de « pré-enquête » doivent être supprimés passés le délai de 6 mois après leur introduction dans la BDC, à moins que l'entité n'ait été confirmée par l'OCAM sous une des autres catégories des BDC.
[120] Article 8 §2 al.2 AR TF consolidé et AR PH.
[121] Article 44/11/3bis, §5, al.2.

Toutefois, arguant d'une nécessité d'analyse des phénomènes de terrorisme sur un temps long[122], le délai maximum de conservation des données a été porté à 30 ans après le dernier traitement et tout ce qui doit être effacé peut encore être archivé durant 30 ans[123]. Passé ce délai (60 ans), les données sont définitivement effacées.

[122] Loi BDC, *Doc. Parl.*, 54/1727/001 p. 24: « Les phénomènes de terrorisme et d'extrémisme pouvant conduire au terrorisme ne peuvent en effet pas être traités utilement sur des courtes périodes vu que les réponses opérationnelles à apporter sont tributaires d'une compréhension historique, anthropologique et sociétale de ceux-ci. Il peut en effet s'avérer que des données recueillies prennent plus de sens ou un éclairage différent après de nombreuses années, à la lumière de nouvelles informations ou d'évènements nouveaux. De même, les premières phases d'identification, de recrutement et d'activation des personnes ou de cellules dormantes peuvent être espacées par de nombreuses années. Certaines organisations laissent leurs membres parvenir à des fonctions-clés avant de les solliciter à nouveau. L'allongement de la durée de vie amène à devoir concevoir l'implication de personnes dans des organisations ou des mouvances sur une durée plus longue correspondant à cette mutation démographique ».

[123] La consultation des archives n'est toutefois possible que dans trois cas (l'appui à la définition d'une politique, le traitement des antécédents dans le cadre d'une enquête relative à un fait criminel de terrorisme, la défense des autorités en justice, article 44/11/3bis, §7, LFP) et, en cas de travail d'appui à une politique, les données doivent être rendues anonymes.

3 Tribunal de Première Instance (TPI/MaCH[124])

3.1 Description générale

Le travail de description et de documentation des banques de données au sein du ministère public a été entamé mais n'est pas encore abouti à l'heure actuelle. Ainsi, il n'y a pas encore de base légale unique pour l'administration des banques données au sein du ministère public ou de l'ordre judiciaire[125]. Le processus de mise en conformité des enregistrements avec le RGPD est toutefois en cours[126]. Ainsi, la loi du 5 mai 2019 qui prévoit notamment la publication des jugements et arrêts[127], a relancé le débat sur la conservation et la gestion des décisions judiciaires, ainsi que sur la circulation de la jurisprudence au sein de l'ordre judiciaire. En outre, il y a également l'objectif de se conformer à la législation « Only once »[128] du 5 mai 2014, qui vise à garantir le principe de la collecte unique des données dans le fonctionnement des services et instances.

L'entrée en vigueur de la loi du 5 mai 2019 a été repoussée au 1er septembre 2021, le temps que les mesures nécessaires soient prises. Pour ce faire, le Collège du Ministère public collabore actuellement avec le SPF Justice, le Collège des cours et tribunaux, la Cour de Cassation et l'Institut de Formation Judiciaire afin de mettre en œuvre les outils et les mesures techniques et organisationnelles nécessaires. À cette fin, une description des transmissions, des accès, etc. sont actuellement à l'étude[129].

Dans la pratique, tout procès-verbal rédigé par la police doit être transmis au Ministère public de l'arrondissement dans lequel les faits[130] sont suspectés avoir été commis et par rapport auxquels celui-ci devra prendre une décision (p. ex. classement sans suite, médiation pénale, jonction, renvoi vers le juge, etc.).

Ces procès-verbaux sont enregistrés par chaque parquet dans le système informatique mis à leur disposition à des fins de gestion administrative des dossiers. Le système fournit des

[124] MaCH pour Mammouth @ Central Hosting.
[125] Ce sont actuellement diverses missions et tâches données au ministère public et à ses collaborateurs qui fondent les bases légales pour la conservation de données (p.ex. l'art. 176 du Code judiciaire).
[126] En ce qui concerne la compatibilité ou incompatibilité de ce système d'enregistrement avec la loi de protection des données personnelles, voir Liégeois (2020).
[127] Loi modifiant le Code d'instruction criminelle et le Code judiciaire en ce qui concerne la publication des jugements et des arrêts.
[128] Loi garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de, ou exécutent, certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier.
[129] Correspondance électronique du 4 février 2021 avec le service des analystes statistiques près du Collège des Procureurs généraux.
[130] Sauf pour les faits (suspectés) commis ou subis par des mineurs d'âge, pour lesquels la compétence du parquet est déterminée non par le lieu des faits mais par le domicile du mineur.

informations assez complètes relatives aux poursuites d'affaires pénales par les parquets correctionnels près les tribunaux de première instance et par le parquet fédéral mais présentait tout de même certaines difficultés en raison de sa vétusté[131]. C'est pourquoi, depuis 2016, le Ministère Public, à l'instar de nombreuses autres juridictions (notamment les parquets et tribunaux de police), a entamé l'installation progressive de la nouvelle application MaCH[132] [133].

Dans MaCH, l'affaire constitue l'unité de compte primordiale, celle-ci est enregistrée sous le code de prévention principal qui est indiqué sur le procès-verbal transmis par la police. Ces codes font référence à la nomenclature des infractions pénales[134].

Des analyses sont également possibles au niveau de la personne car depuis le 1er mars 2010, les différents dossiers relatifs à un même prévenu ont été fusionnés grâce à la création d'un numéro de « casier-parquet » unique sur le plan national à partir du numéro de casier-parquet local, lequel est un identifiant unique des prévenus au sein de chaque parquet. Cela signifie qu'il est désormais possible de connaître le nombre de dossiers ouverts dans les différents arrondissements du pays pour un même prévenu.

Le parquet est responsable de l'exécution des peines. En vertu de la circulaire 'info – flux'[135], il lui appartient notamment d'organiser la circulation de l'information entre lui-même, les services de police et les maisons de justice pour les personnes condamnées qui exécutent leur peine dans la communauté. Cependant, le parquet n'assume pas toujours dans la pratique le rôle qui lui revient. Par conséquent les services d'accompagnement, de suivi et de contrôle des justiciables manquent parfois d'informations pour assurer leurs missions, voire établissent d'autres canaux de communication informels entre eux afin, notamment, de pouvoir vérifier la situation du justiciable et plus particulièrement le respect des conditions qui lui ont été imposées (Jonckheere et al., 2021, Jonckheere & Maes 2017). C'est notamment pour remédier à cette situation qu'a été mise en place, au niveau des établissements pénitentiaires, la nouvelle banque de données appelée « Registre des Conditions » (voir ci-après sous SIDIS SUITE).

[131] Pour un aperçu des analyses réalisées par les analystes statistiques près du Collège des procureurs généraux, voir notamment https://www.om-mp.be/stat/intro_f.html.
[132] Communiqué de presse du ministre de la Justice de l'époque, Koen Geens, Centralisation et numérisation des dossiers dans MaCH, du 15 mai 2019, https://justice.belgium.be/fr/nouvelles/communiques_de_presse_29.
[133] Celle-ci était toujours en cours de développement au moment de nos demandes d'extractions de sorte que notre matériel comporte deux jeux de données pour une même instance.
[134] Disponible sous https://www.om-mp.be/stat/jeu/f/nomenclat.html.
[135] Circulaire du 7 juin 2013 adoptée conjointement par le Ministre de la Justice, le Ministre de l'Intérieur et le Collège des Procureurs généraux près les cours d'appel chargée d'assurer une politique criminelle cohérente à l'échelle de la Belgique.

3.2 Enregistrements en matière de radicalisation

Suite aux différentes circulaires ministérielles adoptées en vue d'assurer l'échange d'informations et le suivi des FTF[136], HTF, PH[137] et EPV, le Collège des Procureurs Généraux a précisé, dans des circulaires successives, les lignes directrices de l'approche judiciaire à adopter à l'égard de ces entités[138]. Tout récemment, le Collège a compilé le contenu de ces différentes circulaires dans un texte de synthèse[139].

Globalement, au niveau des enregistrements dans la banque de données, rien ne change. L'enregistrement se fait toujours sur la base du code de prévention (35 en cas de suspicion d'infraction terroriste et sinon 45 pour les agissements suspects) et, respectant en cela la loi pénale, aucun nouveau code de prévention n'a été introduit[140]. Par contre, les pratiques d'échange d'informations et surtout de concertation entre les différentes autorités (notamment judiciaires et administratives) sont précisées dans le but d'assurer la cohérence du suivi.

Deux distinctions majeures sont établies : d'une part, entre les affaires qui impliquent des majeurs et celles qui concernent des mineurs, et d'autre part, entre les affaires qui laissent suspecter une infraction terroriste selon sa définition pénale, et celles qui relèvent de la catégorie plus générale des 'agissements suspects'.

Le système d'enregistrement dans TPI_MaCH ne concernant que les affaires impliquant des majeurs (ou dont l'auteur est inconnu), nous n'abordons pas, dans cette partie, la situation des mineurs. Les enregistrements relatifs à ces derniers sont traités sous le titre suivant Parquet Jeunesse Greffe (PJG) qui est le programme d'enregistrement à la disposition des juridictions de la jeunesse.

En ce qui concerne les majeurs, la circulaire précise les codes de prévention sous lesquels ces affaires doivent être enregistrées : s'il y a suffisamment d'indices sérieux de l'existence d'une infraction terroriste, un procès-verbal code « 35 » (terrorisme) est dressé et le dossier est

[136] Circulaire ministérielle conjointe du Ministre des Affaires Etrangères et du Ministre de la Justice concernant l'échange d'informations et le suivi des Foreign Terrorists Fighters, du 21 août 2015, confidentielle.
[137] Circulaire ministérielle conjointe du Ministre de la Sécurité et de l'Intérieur, du Ministre de la Justice relative l'échange d'informations et au suivi des Terrorist Fighters et des Propagandistes de Haine, 22 mai 2018, confidentielle, qui abroge la circulaire ministérielle conjointe des Ministres de la Sécurité et de l'Intérieur, des Affaires Etrangères, de la Justice et de la Défense et du secrétaire d'Etat à l'Asile et la Migration concernant l'échange d'informations et le suivi des propagandistes de haine, 18 juillet 2016 , confidentielle.
[138] COL 10/2015 (FTF), COL 2/2016 (HP), COL 22/2016 (GGB), confidentielles.
[139] COL 18/2020 relative à l'approche judiciaire en matière des Foreign Terrorist Fighters, des Homegrown Terrorist Fighters, des Propagandistes de Haine, des Extrémistes Potentiellement violents et des personnes Condamnées pour Terrorisme, confidentielle.
[140] S'il n'y a effectivement pas d'infraction de 'radicalisation', l'extension dans la loi pénale de l'infraction terroriste à des comportements très en amont de celle-ci peut être considérée comme se rapprochant de la notion de radicalisation, voir à cet égard Moreau C. (2018).

immédiatement notifié par le parquet local au parquet fédéral. Remarquons que sont comprises dans les infractions « terroristes », non seulement les infractions visées au Livre I, Titre Ier du Code pénal, mais aussi, dans certains cas, celles contenues dans des lois spéciales (par exemple les infractions visées à l'article 20 de la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie et à l'article 22 de la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination). Prédiquer la haine peut en effet constituer un acte de participation aux activités d'un groupe terroriste sur la base de l'article 140 Code pénal. D'autre part, l'article 140 bis prévoit explicitement la condamnation des actes de diffusion ou de mise à disposition du public d'un message avec l'intention d'inciter à la commission d'une infraction terroriste.

Si les informations doivent encore être confirmées ou étayées, un procès-verbal d'information code « 45 » (agissements suspects) est dressé. Dans ce cas, le parquet local doit mener des actes d'enquête en vue de préciser la situation, via notamment une vérification du profil du suspect (contextualisation des faits, sur la personne, sur son entourage, …), un contrôle dans les banques de données policières et judiciaires. En cas de suspicion de volonté de départ vers une zone djihadiste ou de retour vers la Belgique, il y a lieu de procéder également à un contrôle de l'itinéraire, des documents de voyage et d'identité, une enquête sur les services de téléphonie, un suivi des médias sociaux, une visite domiciliaire avec consentement du suspect, des saisies des appareils multimédias et des documents de voyage, des auditions, etc. Dès qu'un élément d'enquête révèle des indices sérieux de l'existence d'une infraction terroriste le dossier sera immédiatement notifié au parquet fédéral sans changement du code. Aussi longtemps que le dossier n'est pas fédéralisé, le parquet local reste responsable de l'enquête.

L'autorité judiciaire doit communiquer à l'OCAM toutes les décisions prises dans ces dossiers relativement à la détention préventive (éventuellement sous surveillance électronique), la remise en liberté sous conditions, l'existence d'un mandat d'arrêt international ou européen, la fixation d'une affaire pénale devant le tribunal correctionnel, la cour d'appel et la cour d'assises, la condamnation ou acquittement pour une infraction terroriste. L'OCAM mentionne ces informations dans la fiche de renseignements (voir ci-avant sous le point Banques de Données Communes). De même, l'autorité judiciaire avertit la Direction Générale des Établissements Pénitentiaires (DG EPI) de la détention préventive. Elle n'est par contre pas tenue d'alimenter les BDC et peut s'opposer à un enregistrement en cas de risque pour l'enquête (« embargo judiciaire »).

S'il y a suffisamment de charges, le classement sans suite de l'affaire pénale est en principe exclu.

Dès qu'il y a ouverture d'une enquête pénale (locale ou fédérale), les services de police doivent signaler les TF et PH pour « contrôle approfondi » [141] au niveau national mais également au niveau international[142] , les condamnés pour terrorisme et les EPV font, quant à eux, l'objet d'un « contrôle discret ».

Les magistrats ne participent ni aux Task Force Locales (TFL), ni aux Cellule de Sécurité Intégrale en matière de Radicalisme (CSIL-R)[143] mais les considèrent néanmoins comme des lieux de discussion importants pour d'une part, éviter la sur judiciarisation quand des mesures locales, administratives et préventives peuvent s'avérer plus appropriées et d'autre part, parvenir à une cohérence des mesures administratives et judiciaires, éventuellement simultanées. Ainsi, le contenu des mesures d'enquête (p.ex. l'écoute téléphonique, le contrôle visuel discret, etc.) ou des méthodes particulières de recherche (le recours aux informateurs, l'observation, l'infiltration et l'infiltration civile) prises dans le cadre d'une enquête pénale à l'insu de la personne intéressé, peut être partagé (oralement) au sein d'une TFL pour autant que cette communication ne mette pas en péril la bonne exécution de la mesure.

[141] Sauf si le magistrat-titulaire est d'avis qu'un tel contrôle pourrait mettre en péril l'enquête pénale. Dans ce dernier cas, la personne concernée sera signalée pour surveillance discrète.

[142] Au niveau Schengen, le majeur fera l'objet d'un signalement standard conformément à l'article 36.2 « Contrôle ». En cas de signalement national pour arrestation, il sera signalé conformément à l'article 26 « Arrestation ». À cet effet, le magistrat compétent émettra un mandat d'arrêt européen. En cas de signalement national pour refus d'admission ou de séjour sur le territoire d'un majeur non européen, ce dernier sera signalé conformément à l'article 24 « Non-admission ou interdiction de séjour sur le territoire ». Au niveau Interpol, le majeur sera signalé de manière standard au moyen d'une diffusion bleue « Contrôle ». En cas de signalement national pour arrestation, il sera signalé au moyen d'une diffusion rouge « Arrestation ». À cet effet, le magistrat compétent émettra un mandat d'arrêt international.

[143] Il existe par ailleurs au niveau du Collège des Procureurs Généraux un réseau d'expertise en la matière ('Ren Terro').

4 Parquet_Jeunesse_Greffe (PJG)

4.1 Description générale

Par le passé, les parquets et les greffes de la jeunesse disposaient chacun d'un programme informatique spécifique pour l'enregistrement de leurs données relatives aux affaires impliquant un mineur d'âge (PJP pour les parquets et DUMBO pour les greffes). Ces applications possédaient une structure décentralisée, comprenant une banque de données distincte dans chaque parquet/greffe de la jeunesse du pays. Depuis la fin de l'année 2016, l'application PJG (Parquet_Jeunesse_Greffe) a été implantée en remplacement de PJP/DUMBO. Ce nouveau programme suit une structure centralisée, qui comporte une banque de données partagée par l'ensemble des parquets et des greffes de la jeunesse.

Cette banque de données est gérée par le service informatique (ICT) du SPF Justice et est alimentée par les parquets et les greffes locaux à des fins de gestion administrative de leurs dossiers. L'utilisation de ces données à d'autres fins connait des limites dues, notamment, à un manque d'uniformité dans les pratiques locales d'enregistrement. Tout récemment, le Collège des Cours et Tribunaux a édicté quelques règles de base au niveau des enregistrements, pour parvenir a minima, à la détermination de la charge de travail de ces instances[144].

De manière générale, les juridictions de la jeunesse sont compétentes pour traiter des affaires de mineurs (0-18 ans), soit étant considéré comme à protéger en raison du comportement d'autrui ou de leur propre comportement, soit suspecté d'avoir commis un fait qualifié infraction. C'est le service de police qui, en fonction de l'information dont il dispose quant à l'âge du suspect, choisit d'adresser le procès-verbal au parquet de la jeunesse. Ce dernier l'enregistre à son niveau dans l'application PJG sous le code de prévention principal retenu dans ledit procès-verbal, code de prévention qui fait soit référence à une situation de danger pour l'enfant (principalement 42 O), soit à une infraction suspectée commise par le mineur.

L'unité de compte utilisée est aussi bien "l'affaire" que "le mineur (unique)".

Au niveau des Tribunaux de la jeunesse, un dossier personnel est ouvert par mineur au moment de la première saisine du juge. Tout mineur ne possède dès lors en principe qu'un seul dossier personnel, lequel sera clos à sa majorité. Un mineur peut être impliqué dans plusieurs affaires tant de 'mineur en danger' que de 'mineur ayant commis un fait qualifié infraction'. Même si ces affaires sont portées séparément devant le Tribunal de la jeunesse, elles sont toutes conservées dans le dossier personnel du mineur.

[144] https://www.tribunaux-rechtbanken.be/sites/default/files/college/richtlijnen/2020-01_directives-cct_tpi-jeunesse.pdf

La détermination des mesures qui peuvent être prononcées à l'égard de ces mineurs est communautarisée de sorte que ce sont trois législations spécifiques qui s'appliquent[145]. Dans certaines circonstances particulières toutefois, le Tribunal de la jeunesse peut décider de se dessaisir de l'affaire au profit de la chambre spécifique jeunesse du Tribunal correctionnel auquel cas ce sont les peines et mesures du droit pénal qui pourront être appliquées à son auteur.

Les informations enregistrées dans PJG sont archivées à la majorité du jeune.

4.2 Enregistrements en matière de radicalisation

Si les circulaires ministérielles adoptées en vue d'assurer l'échange d'informations et le suivi relativement aux entités TF, PH, EPV et CT ne font généralement que peu de distinctions en fonction de l'âge de la personne considérée, il n'en est pas de même au niveau de l'approche judiciaire. En effet, la compétence exclusive et spécifique des juridictions de la jeunesse à l'égard des mineurs d'âge oblige à un traitement particulier de ce type d'affaires.

Tout comme au niveau des parquets correctionnels, le programmes et règles d'enregistrement n'ont pas été modifiés en vue d'un enregistrement spécifique des affaires de terrorisme ou de radicalisation. Toutefois, la circulaire du Collège des Procureurs Généraux apporte des précisions en fonction de la situation du mineur et de son âge.

En ce qui concerne les mineurs de moins de 12 ans, il est communément admis que ceux-ci ne peuvent être considérés comme responsables de leurs actes. Ils doivent dès lors être enregistrés comme 'mineur en danger' (code de prévention 42 O) quelle que soit finalement la nature des éventuels actes qu'ils auraient commis. Les services d'aide à la jeunesse des communautés doivent être alertés. L'intervention visera l'aide et l'accompagnement. En fonction des résultats de l'enquête, une information sera ouverte à l'égard des parents.

En ce qui concerne les mineurs âgés (au moment des faits) de plus de 12 ans, tout dépendra de leur situation spécifique. Si le mineur est suspecté avoir commis une infraction terroriste ou assimilée (incitation à la haine, …), son affaire sera enregistrée sous le code de prévention « 35 ». Si les informations doivent encore être confirmées ou étayées, c'est le code «42 O » (mineur en danger) qui sera utilisé. Dans le même sens, s'il n'est suspecté « que » de radicalisation, il sera également enregistré sous le code « 42 O ». Toutefois, si le mineur considéré comme « en danger » révèle durant son audition avoir commis des faits punissables, la circulaire enjoint l'ouverture en parallèle d'un dossier sous le code « 35 ». Au surplus, la circulaire préconise, en tous les cas, la rédaction d'un nouveau procès-verbal initial à charge du mineur dès l'obtention de sa majorité.

[145] Pour plus d'informations à ce sujet, voir Goedseels E. et Ravier I. (2020).

Tout comme pour les majeurs, une enquête approfondie (famille, amis, médias sociaux, enregistrement dans les banques de données, …) doit être menée afin de cerner tant la personnalité du mineur que son environnement. Il est évident que la philosophie de cette enquête est différente selon que l'enfant est considéré comme une victime ou comme un auteur.

De même, le mineur est signalé au niveau national, international et Schengen avec une interdiction de voyage, même avec ses parents. Ses parents sont, quant à eux, signalés pour un contrôle spécifique.

5 Casier Judiciaire Central (CJC)

5.1 Description générale

Le Casier judiciaire central fut établi par une circulaire ministérielle du 31 décembre 1888 mais ne fut légalement consacré que par la loi du 8 août 1997[146]. Celui-ci est placé sous l'autorité du Ministre de la Justice et a officiellement, depuis la circulaire ministérielle du 5 novembre 1897[147], une double fonction : « d'une part, délivrer l'information principalement aux autorités judiciaire[148] d'autre part, procéder à l'élaboration de statistiques criminelles » (Seron, 2010 : 225).

Seules les décisions pénales définitives doivent être transmises au Casier judiciaire central pour enregistrement. Cela signifie qu'en cas de jugement par défaut, le délai pris en considération est le délai d'opposition ordinaire, « cela a pour conséquence que les décisions enregistrées au casier doivent pouvoir être ultérieurement effacées suite à une décision d'acquittement rendue à la suite d'un recours en opposition introduit durant le délai extraordinaire » (Willems, 2007 : 11).

Les acquittements ne sont pas transmis ni, a fortiori, enregistrés dans le Casier judiciaire central. C'est également le cas des condamnations ne comportant comme décision principale qu'une amende inférieure à 26 euros, pour autant que celle-ci ne soit pas motivée par des infractions au Code pénal (ou d'ivresse publique) et ne soit pas assortie d'une déchéance du droit de conduire. Il n'est cependant pas impossible de retrouver dans la base de données des bulletins qui ne respectent pas cette restriction (Willems, 2007 : 12).

L'enregistrement des bulletins de condamnation s'effectue en deux temps. Le personnel du Casier judiciaire central encode tout d'abord les informations socio-biographiques de la personne, laquelle reçoit un numéro d'identification unique (« numéro de dossier » ou « numéro de casier judiciaire »). Ensuite, il procède à l'enregistrement des informations relatives à la procédure, à la juridiction, aux décisions et aux faits. Contrairement aux données socio-biographiques qui sont enregistrées une fois pour toutes dans la base de données, l'enregistrement de ces informations peut être multiple.

La qualité des informations enregistrées manuellement reste toutefois tributaire de la dextérité et de la vigilance du personnel qui encode ainsi que de la mise à jour des différentes nomenclatures utilisées lors de l'encodage. Toutefois, depuis 2012, la nouvelle application

[146] Loi du 8 août 1997 relative au casier judiciaire central.
[147] Circulaire ministérielle du 5 novembre 1897 – Statistiques criminelles – Emploi des bulletins du casier judiciaire complétés – Suppression du registre des annotations.
[148] L'article 589 du Code d'instruction criminelle définit très explicitement et très limitativement les autorités et personnes auxquels les renseignements enregistrés dans le casier judiciaire central sont communiqués.

informatique du Casier judiciaire central limite les possibilités d'erreurs lors de la saisie des informations en recourant à des champs pré-structurés et des menus déroulants. Par ailleurs, depuis le 1er janvier 2015, une liaison existe entre les données des tribunaux de police enregistrées dans MaCH et le Casier. Cette automatisation a réduit drastiquement le travail d'encodage au sein du Casier judicaire central puisque le roulage constitue le contentieux majeur.

Les informations enregistrées dans la base de données du Casier judiciaire central concernent principalement les décisions des cours et tribunaux de droits communs belges et étrangers[149], mais aussi (pour la Belgique) les décisions des juridictions militaires, des juridictions de la jeunesse[150] et des juridictions d'instruction, les décisions prises par les juridictions de jugement sur base de la loi de défense sociale (c'est-à-dire les mesures de sûreté, telles que l'internement et la mise à disposition) ou encore, les suspensions du prononcé de la condamnation. Seuls les individus nés après 1930 (et, à partir de 1999, les personnes morales) dont le jugement définitif prononcé par une juridiction belge ou étrangère a été communiqué et enregistré au Casier judiciaire central figurent dans la base de données[151]. Depuis 2012, le système ECRIS (système informatisé d'échange d'informations sur les casiers judiciaires) permet l'interconnexion entre les casiers judiciaires des pays membres de l'Union européenne[152]. Ce système facilite l'échanges d'informations relatives aux décisions définitives rendues par les juridictions nationales et permet ainsi de répondre plus rapidement à des demandes d'extraits européens et la notification des condamnations de citoyens européens aux Etats membres peut se faire plus rapidement.

Les condamnations ne restent cependant pas éternellement sur l'extrait du casier judiciaire. En fonction de la gravité de la peine prononcée, certaines condamnations sont effacées. Ainsi, sauf dans des cas exceptionnels, les condamnations à une peine de police (c'est-à-dire à un emprisonnement d'un à sept jours ou à une amende d'un à 25 euros, ou à une peine de travail de 20 à 45 heures) sont automatiquement effacées après un délai de trois ans. Cet effacement n'est soumis à aucune condition et est gratuit. Par ailleurs, une procédure de réhabilitation

[149] En l'occurrence, il s'agit plus précisément des « décisions rendues en matière pénale par des juridictions étrangères à charge de Belges, qui sont notifiées au Gouvernement belge en vertu de conventions internationales, ainsi que les mesures d'amnistie, d'effacement de condamnation ou de réhabilitation prises par une autorité étrangère, susceptibles d'affecter ces dernières décisions, qui sont portées à la connaissance du Gouvernement belge ». Art. 590, 16° du Code d'instruction criminelle.

[150] Pour les mesures prononcées à l'égard des mineurs ayant commis un fait qualifié infraction.

[151] L'article 590 du Code d'instruction criminelle énumère avec précision les informations qui figurent dans le casier judiciaire central. Avant la nouvelle application (29/06/2012), en raison d'une infrastructure devenue obsolète, il est tout à fait possible que certaines personnes (décédées, réhabilitées, etc.) aient été purement et simplement supprimées de la base de données dans le cadre d'opérations de nettoyage. Aujourd'hui lorsqu'un bulletin doit être effacé, il est tagué « effacé » mais il reste dans la base de données bien qu'il n'apparaisse pas sur l'extrait de casier judiciaire délivré.

[152] Décision-cadre 2009/315/JAI du Conseil européen du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres ; Décision 2009/316/JAI du Conseil européen du 6 avril 2009 relative à la création du système européen d'information sur les casiers judiciaires (ECRIS).

existe pour les peines qui ne sont pas automatiquement effacées[153]. Cette procédure est en revanche payante et à charge du demandeur.

5.2 Enregistrements en matière de radicalisation

Le Casier Judiciaire Central ne reprend que les informations relatives aux décisions judiciaires définitives, par conséquent aucun enregistrement ne concerne des « faits » de radicalisation puisqu'il ne s'agit pas d'une infraction susceptible d'être sanctionnée par la justice pénale. Outre les condamnations pour des infractions terroristes, on peut y retrouver des condamnations pour incitation à la haine, racisme, xénophobie, ou encore discrimination ainsi que celles pour atteintes à l'ordre public et à la sûreté de l'État.

Par contre, du fait de l'élargissement – en vue d'assurer la prévention du terrorisme – des comportements condamnables en raison de leur intention (supposée) (Thomas 2020 :12, Moreau 2018 :13), on peut bien entendu y retrouver des condamnations relatives à des comportements révélant une certaine radicalisation. Ainsi sont dorénavant condamnables[154] – pour autant que l'intention terroriste puisse être établie – l'incitation, le recrutement, la formation tant dans le chef de celui qui la donne que dans le chef de celui qui la suit (éventuellement en auto apprentissage), le voyage, les actes préparatoires, l'aide matérielle.

Ce qui a également changé récemment, ce sont les droits d'accès à l'information contenue dans le Casier : auparavant limités aux officiers de police judiciaire, aux magistrats[155] et aux administrations[156], les accès au Casier ont été récemment étendus[157] aux membres des services de police administrative, aux membres de la Cellule de traitement des informations financières et aux organes de contrôle des services de police et de renseignement.

Dorénavant, tous les services de police qui, pour l'exercice de leurs missions légales (leurs missions de police judiciaire comme leurs missions de police administrative) ont besoin de certaines informations reprises dans le Casier Judiciaire Central ont accès à la banque de données. Cet accès est toutefois soumis à une condition : les fonctionnaires doivent avoir fait constater préalablement leur besoin de connaître certaines informations et ils doivent avoir été préalablement et nominativement désignés par leur supérieur hiérarchique.

Les modalités d'accès sont fixées dans un protocole d'accord.

---

[153] Article 619 et sv. du Code d'instruction criminelle.
[154] Articles 137 à 141 du Code pénal.
[155] Ministère public [y compris le membre belge d'Eurojust], juges d'instruction, juges de paix, juges et assesseurs des tribunaux de l'application des peines.
[156] Autorités administratives chargées de l'exécution des décisions rendues en matière pénale et des mesures de défense sociale.
[157] Loi 5 mai 2019 portant dispositions diverses en matière d'informatisation de la justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés, *op.cit.*

6 Système Informatique de Détention/Detentie Informatie Systeem (SIDIS-SUITE)

6.1 Description générale

Sur le plan technico-informatique, le secteur pénitentiaire est celui où la constitution de bases de données informatisées est la plus ancienne. En 1974 déjà, la Direction Générale de l'Administration Pénitentiaire (DG EPI) mettait en place un premier système de base de données (BS2000). Depuis lors, il a subi de nombreuses adaptations visant toujours à en améliorer le fonctionnement. En 1997-1998, le système est remplacé par une nouvelle application, le système SIDIS (Système Informatique de Détention/Detentie Informatie Systeem) qui récupère les informations de l'ancienne application et introduit quelques adaptations notamment au niveau des codes d'infractions. Cette application est axée sur l'enregistrement et la gestion des détentions et mouvements de chaque détenu, elle reprend entre autre les données suivantes: date d'écrou, date de transfert, date d'octroi des modalités d'exécution de la peine (i.e., congé pénitentiaire et permission de sortie), date et modalité de libération, situation légale, etc. (Maes, 2002 : 340-341). En 2001-2002, une nouvelle base de données est directement articulée à l'application SIDIS (Cour des comptes, 2011 :37). Il s'agit de l'application GREFFE laquelle a remplacé dans la pratique les fiches d'écrou papier (Drossens, 2008 :11). Tout en maintenant les fonctionnalités déjà existantes dans SIDIS, le programme Greffe en ajoute de nouvelles qui offrent nettement plus de possibilités pour la réalisation d'analyses détaillées et scientifiquement pertinentes (Vanneste et al. 2004)[158]. La gestion de SIDIS et de GREFFE était assurée par le service Gestion administrative de la DG EPI, ces applications pouvaient être consultées par les différents greffes des prisons bien que la gestion des données relatives à un détenu en particulier relevait de la compétence du greffe de l'établissement pénitentiaire où cette personne était détenue (Drossens, 2008 : 11).

En septembre 2014, une nouvelle adaptation a été réalisée par la DG EPI : les données ont ainsi migré de SIDIS-Greffe vers une nouvelle application intitulée SIDIS-Suite. Cette dernière est une application Web destinée à la gestion des établissements pénitentiaires, laquelle reprend l'ensemble des informations relatives aux détentions des personnes incarcérées. La finalité poursuivie par SIDIS-Suite était double : améliorer la gestion des processus de détention (e.g., gestion de la capacité et de l'accueil, planification de la détention, classification d'après le statut ou le régime) et poursuivre le développement de SIDIS-GREFFE pour en faire « une application centralisée et performante » (Cour des comptes, 2011 :38). La Cour des comptes (2011 : 38) explique que l'application vise ainsi à terme à faciliter l'échange

[158] D'autres applications ont également été développées et étroitement articulées à SIDIS, parmi lesquelles l'application EPICURE qui gère les dossiers médicaux des détenus, l'application ACCESS qui gère l'enregistrement des accès et la sécurité des établissements pénitentiaires ou encore l'application PIA qui gère l'argent des détenus. Voir Plan de management et opérationnel intégré du Service Public Fédéral Justice, 19 avril 2004, 74.

de données, à accroître leur qualité ainsi qu'à améliorer la transparence du flux d'informations. Ces données sont non seulement accessibles aux services centraux de l'administration pénitentiaire et aux différentes prisons mais aussi consultables par des instances externes.

Ce programme a récemment fait l'objet d'une réforme législative importante afin, notamment, de permettre une meilleure circulation de l'information entre les différents partenaires du système d'administration de la justice pénale[159].

Plus précisément, la loi du 5 mai 2019 a étendu les enregistrements aux personnes qui font l'objet d'une mesure limitative de liberté sans pour autant passer par un établissement pénitentiaire. Cela concerne, par exemple, les personnes libérées sous conditions par le juge d'instruction, les personnes condamnées avec sursis ou suspensions probatoires et celles condamnées à une peine autonome (probation ou surveillance électronique) et d'autre part, élargi les accès à la base de donnée à de nombreux nouveaux acteurs[160]. Au surplus, elle a créé une nouvelle banque de données (le 'Registre des Conditions') reprenant spécifiquement les modalités d'exécution des peines et mesures de manière à permettre aux différents acteurs concernés par l'exécution des peines, d'être informés et de collaborer en la matière (Nederlandt, 2019 :71).

La finalité de ce Registre des Conditions est de fournir une vision plus globale du suivi des personnes faisant l'objet d'une mesure privative ou limitative de liberté et d'établir un flux d'informations plus intégré entre les différents services et autorités concernées dans la prise de décision et le suivi de celles-ci.

> Article 10 : il est créé une banque de données informatisée dont le ministre de la Justice est responsable du traitement. Dans cette banque de données sont traitées les données à caractère personnel et informations nécessaires à l'exercice adéquat des missions légales ou réglementaires de suivi, d'accompagnement et de contrôle par les autorités, les organes ou les services visés aux articles 12 à 13, des personnes qui font l'objet d'une décision pénale, de protection de la jeunesse ou d'internement et qui, moyennant le respect de conditions, sont en liberté, ont été mises en liberté, ont été laissées en liberté.

[159] Loi 5 mai 2019 portant dispositions diverses en matière d'informatisation de la justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés, *op.cit.*

[160] Article 7 loi 5 mai 2019: un droit de lecture est ainsi accordé aux services de police, à la Sûreté de l'État, au Service Général du Renseignement et de la Sécurité, à l'Organe de Coordination pour l'Analyse de la Menace, au Ministère Public et aux secrétariats des parquets, aux magistrats du siège, aux assesseurs au Tribunal de l'application des peines et les greffes, à l'Office des Étrangers, au Commissariat aux Réfugiés et aux Apatrides ; aux services des Communautés qui accomplissent des missions dans le cadre de la procédure judiciaire ou de l'exécution de décisions judiciaires, y compris le service qui assure la mise en œuvre et le suivi de la surveillance électronique, les personnes ou services chargés de l'aide et des services aux détenus , le conseil central de la surveillance pénitentiaire et les commissions de surveillance, les huissiers de justice, les organismes ou services chargés d'une application relative à la sécurité sociale ou à l'assistance sociale et les services d'inspection en charge du contrôle du respect des conditions d'octroi des avantages ou allocations octroyées en application de cette législation, les administrations communales, le praticien professionnel non désigné par l'administration pénitentiaire visé à l'article 2, 3° de la loi du 22 août relative aux droits du patient.

6.2 Enregistrements en matière de radicalisation

Depuis 2006, la DG EPI et la Sûreté de l'État (SE) collaborent sur la problématique de la 'radicalisation' et se sont liées par un protocole d'accord, conclu dans le cadre du plan fédéral de lutte contre la radicalisation (Plan R)[161]. Depuis 2009, ces deux organes tiennent des réunions régulièrement (Brion, 2019 :6). Le plan Prisons (Plan P)[162] souligne l'importance de cette plate-forme de concertation.

Dans ce cadre, la DG EPI a mis en place en 2015 une cellule 'Extrémisme' (Celex). Sa mission première est de renforcer la collaboration entre les services de sécurité et la DG EPI en améliorant l'échange d'informations en interne et en externe dans le cadre de l'analyse du risque en matière d'extrémisme, radicalisme et terrorisme. Ces échanges se concrétisent sous forme d'avis remis selon les besoins en la matière de la DG EPI[163]. À cette fin, SIDIS Suite permet de distinguer les 'suivis Celex'[164]. Au fil du temps, les catégories d'enregistrement ont été modifiées. La première catégorisation (2015) distinguait d'une part, les terroristes et d'autre part, les Foreign Fighters. Sous la catégorie des « terroristes », le rôle de la personne était précisé (leader, leader ayant commis attentat, personne ayant commis attentat, personne ayant fourni un soutien élémentaire, membre d'une organisation, personne ayant fourni un soutien logistique). De même au niveau de la catégorie des Foreign Fighters, étaient distingués, les prédicateurs ou recruteurs, les prédicateurs ou recruteurs encourageant la commission d'attentats en Belgique, les returnees militants, les returnees passifs, les personnes appartenant à un réseau de recruteurs avec un rôle d'appui ou de facilitateur (Brion, 2019 :11).

Cette première catégorisation a été révisée en avril 2016 et une nouvelle fois[165] en octobre 2018 de la manière suivante :

- Catégorie A : terroristes = poursuivis ou condamnés pour infraction terroriste ;
- Catégorie B : assimilés = ni poursuivis, ni condamnés pour infraction terroriste mais qui, sur base de leur titre de détention, ont un lien clair avec le terrorisme et/ou qui, par des mots ou des actes, démontrent fortement appartenir au profil d'extrémistes violents selon une appréciation de la Celex ;
- Catégorie C : Terrorist Fighters qui ont combattu ou voulu combattre à l'étranger et sont à ce titre enregistrés dans la BDC sous la catégorie de FTF ou HTF ;

[161] https://www.besafe.be/sites/default/files/2019-06/brochure_radicalisme_fr.pdf. L'axe 7 de ce plan concerne directement le domaine pénitentiaire.

[162] Plan d'action contre la radicalisation dans les prisons, 11 mars 2015, https://justice.belgium.be/sites/default/files/downloads/Plland%27actionradicalisation-prison-FR.pdf.

[163] Correspondance électronique avec un membre de la Celex, 3 février 2021. Selon les instructions Particulières Extrémisme (IPEX) de la DG EPI du 2 octobre 2018 (non publiées), il s'agit d'un service « responsable de la collecte d'informations et l'émission d'avis dans le cadre du suivi de la radicalisation et de l'extrémisme dans le domaine pénitentiaire » (Nederlandt, 2019 :230).

[164] Les critères de reprises parmi ces suivis sont décrits dans les IPEX de la DG EPI.

[165] DG EPI, IPEX, 8 octobre 2018, non publiées. Cette dernière catégorisation a encore été revue en octobre 2020 (IPEX 8 octobre 2020) pour y inclure dorénavant également les extrémistes potentiellement violents et les condamnés pour une infraction terroriste.

- Catégorie D : les détenus suspectés (par les agents pénitentiaires, le SPS local ou encore les directeurs) de se radicaliser ou de radicaliser d'autres personnes détenues ;
- Catégorie E : les prédicateurs de haine, à savoir les personnes détenues reprises dans la BDC en tant que PH ;

Cette catégories ont encore été récemment revues (octobre 2020) de manière à viser également les « extrémistes potentiellement violents » et les « condamnés terro » suite à leur intégration dans les banques de données communes (voir ci-avant dans la section relative aux Banques de Données Communes).

L'information peut venir soit des services de la Sûreté de l'État[166] , de l'OCAM ou de la DJ-SOC de la police fédérale qui en informent l'administration pénitentiaire, soit de l'observation réalisée par les membres du personnel au sein de la prison. Ces derniers sont en effet invités à « être attentifs en permanence et au maximum à des signes de radicalisation et d'extrémisme chez les détenus » (Nederlandt 2019 :157). L'administration pénitentiaire disposant d'un droit de lecture et d'enregistrement dans les BDC en tant que service de soutien de l'OCAM [167] elle enrichit également ses propres données sur la base des informations qu'elle y trouve par rapport à la population détenue dans la mesure où il lui appartient de détecter parmi la population carcérale les entités visées par les BDC.

Chaque jour, les agents doivent observer le détenu et noter dans une « fiche d'observation » des informations fouillées sur plusieurs domaines de vie. Tous les deux mois, les constatations ou indications pertinentes quotidiennes sont évaluées par la direction et le SPS local et cette évaluation est transmise à la Direction régionale, à la Cellule Extrémisme, ainsi qu'aux services psycho sociaux (SPS) centraux[168].

Parmi d'autres conséquences, on notera que tant le régime de détention que les modalités d'exécution de la peine peuvent être modifiés du fait de l'inscription parmi les suivis Celex[169]. Cela dépend du pouvoir discrétionnaire du décideur (e.g., direction locale, direction gestion de la détention) et de l'importance comme des conséquences que cette instance y attache.

Une personne classée Celex peut voir son nom supprimé des suivis, et ce, sur proposition de la direction de la prison où elle est incarcérée, ou sur initiative de la direction régionale de la DG EPI ou du SPSC(EX) ou de la Celex et ce, s'il existe suffisamment d'indications permettant

[166] L'échange d'information se fait en vertu du protocole conclu entre la DG EPI et la Sûreté de l'Etat.
[167] Voir ci-avant, dans la section relative aux Banques de Données Communes.
[168] Au sein du service psychosocial central de la DG EPI, un service psychosocial central extrémisme, appelé « SPSC(EX) », a été créé en 2015 et est « responsable de l'évaluation des risques et l'émission d'avis dans le cadre du suivi de la radicalisation et de l'extrémisme dans le domaine pénitentiaire », DG EPI, IPEX, 8 octobre 2018, p.3.
[169] Ainsi, la personne (idéologue ou recruteur) peut être envoyée sur la base d'un screening et d'un avis motivé dans une aile spécifique dédiée aux phénomènes d'extrémisme (D-Rad:EX) et l'octroi à de modalités d'exécution de la peine (e.g., congé pénitentiaire) ou d'une libération anticipée (e.g., libération conditionnelle) peut être conditionnée de manière spécifique (e.g., parcours de désengagement) par le Tribunal de l'application des peines ou de la Direction Gestion de la détention de l'administration pénitentiaire.

d'appuyer cette décision. La décision est prise, après évaluation de toutes les informations disponibles, par Celex, après concertation avec le SPSC(EX), la direction régionale de la DG EPI et le Directeur général de la DG EPI[170].

Les personnes ne sont pas toutes officiellement mises au courant de leur classification Celex et n'ont aucun recours à l'encontre de cette classification. Le détenu s'en rend généralement compte lorsqu'il rencontre la direction, qui elle en est informée, pour prendre connaissance de l'imposition de mesures particulières à son encontre.

Les instructions prévoient que la Cellule Extrémisme de la DG EPI est responsable de gérer le flux d'informations venant de la prison vers les organes de sécurité et de renseignement de l'État (en l'occurrence principalement la Sûreté de l'État et l'OCAM), la DJ-SOC 'Terro' (service décentralisé de la police judiciaire fédérale chargé de la coordination des enquêtes relatives aux faits de terrorisme).

Lorsqu'un détenu Celex bénéficie d'une modalité d'exécution de la peine en dehors de la prison dont le suivi est confié aux maisons de justice ou au centre de surveillance électronique, l'information sur le suivi Celex est notifiée, par mail, par l'administration pénitentiaire à ces organes. Lorsque le détenu bénéficie d'une libération anticipée, l'assistant de justice qui sera en charge du suivi, rencontre en général le détenu quelques mois avant sa libération afin d'éviter une rupture de la prise en charge. À l'inverse, lorsqu'un justiciable suivi par une maison de justice, se fait incarcéré, il est également prévu que la direction de la maison de justice transmette une copie des rapports le concernant au service psychosocial de la prison[171].

Les informations relatives à la situation des suivis Celex sont communiquées par l'administration pénitentiaire au Tribunal d'Application des Peines (TAP) conformément aux prescrits de la loi du 17 mai 2006 relative au statut juridique externe des personnes condamnées[172] pour qu'il puisse se prononcer en toute connaissance de cause sur les éventuelles demandes de sortie ou mises en liberté du détenu. Cependant, il semble qu'à propos du radicalisme supposé ou avéré de la personne concernée, ce partage d'informations ne soit pas encore optimum à l'heure actuelle[173]. En effet, les avis divergent quant à savoir qui doit fournir cette information au TAP : le parquet ou la direction de la prison ?

[170] Le nombre de suivis Celex aurait ainsi grâce à ce screening, chuté de 203 (en 2018) à 150 (2020). Correspondance électronique avec un membre de la Celex, 3 février 2021.
[171] Note de service n°2019/01 de l'Administration Générale des Maisons de justice du 5 mars 2019 relative aux flux d'informations dans le cadre des dossiers terrorisme ou concernés par une problématique d'extrémisme violent.
[172] Loi du 17 mai 2006 relative au statut juridique externe des personnes condamnées à une peine privative de liberté et aux droits reconnus à la victime dans le cadre des modalités d'exécution de la peine.
[173] Rapport Comité T (2020), p. 80.

Conclusion

Dans ce rapport, nous nous sommes principalement intéressés, au niveau fédéral, à deux bases de données dans lesquelles les (premières) suspicions d'évolution vers une radicalisation (violente) sont enregistrées. Il s'agit des bases de données de la police administrative (BEPAD) et judiciaire (BNG) et de la base de données de l'OCAM (BDC). Nous décrivons leur mise sur pied et leur évolution au fur et à mesure de l'émergence de la problématique de la radicalisation. Nous passons également en revue mais plus brièvement, les autres bases de données du système d'administration de la justice pénale (TPI, PJG, CJC, SIDIS) dans lesquelles sont enregistrées les suites des procédures judiciaires éventuellement lancées à l'égard des personnes suspectées de radicalisation.

Deux constats prédominent dans les évolutions constatées : d'une part, l'ambition de parvenir à un partage de l'information et des données entre un grand nombre de services (police, renseignement, judiciaire, mais également locaux et socio préventifs, etc.) ainsi qu'à une coordination de leurs actions sur la base du modèle de 'multiagency', et d'autre part, une volonté de repérage et d'enregistrement de plus en plus précoce des suspicions de toute forme de radicalité.

La lutte contre le terrorisme qui, autrefois, était plutôt l'apanage des services de renseignement, a muté, au fur et à mesure de l'évolution de la menace et de ses manifestations, vers le développement de dispositifs de prévention impliquant l'ensemble des services belges concernés. Pour évaluer la menace et coordonner les actions de prévention, les services (et plus particulièrement l'OCAM) doivent pouvoir disposer de l'information disponible aux différents niveaux de compétence. À cette fin, de nombreuses plateformes de discussion et de concertation ont été mises en place tant au niveau local qu'au niveau fédéral (CSIL-R, TFL, TFN, Joint Decision Centers, etc.). Parallèlement, l'échange et le partage d'informations que chaque service enregistre pour assurer ses propres missions s'est développé. Cet objectif s'est traduit d'une part, par la mise en place de banques de données communes dans lesquelles chaque service réenregistre les données dont il dispose à l'égard des entités considérées comme présentant des signes de radicalisation (violente) et d'autre part, par l'élargissement des accès aux (banques de) données propres à certains acteurs.

Ce système, assurément utile pour les services de renseignement, pose néanmoins question à plusieurs niveaux. On peut y voir notamment les risques que chacun, quelle que soit sa mission initiale, devienne (ou soit perçu comme) un informateur (des services de renseignement); que les frontières entre les missions et les finalités des différents services soient oblitérées ; que la donnée collectée soit utilisée à d'autres fins et avec d'autres conséquences que celles pour lesquelles elle avait été initialement et légalement enregistrée, etc.

Ces questions se révèlent avec d'autant plus d'acuité que la palette des comportements considérés par les différents acteurs comme indicateurs d'un risque dans le cadre de la prévention du terrorisme et de l'extrémisme pouvant mener au terrorisme est large et variée. Au niveau de la police administrative, les informations relatives aux personnes impliquées dans les activités d'un groupement ou un phénomène, politiquement épinglé comme représentant potentiellement un risque pour l'ordre public, sont enregistrées. Au niveau de l'OCAM, toute personne qui a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme mode d'action en Belgique est dorénavant enregistrée dès lors que, selon les critères établis (par l'OCAM), elle présente un risque accru de violence. Au niveau des établissements pénitentiaires, les détenus sont observés dans leur quotidien pour détecter d'éventuels signes de radicalisation ou de prosélytisme. Et si le législateur s'est abstenu, dans le respect de la convention européenne des droits humains, de condamner la radicalisation en tant que telle, il n'en demeure pas moins qu'à ce niveau également, la formulation des infractions terroristes dans le Code pénal, réfère de plus en plus à des comportements bien en amont d'un passage à l'acte.

À l'instar de ce qui se fait en matière de prévention en santé publique vis-à-vis de la pandémie de la Covid-19, les politiques publiques sont soumises à un travail d'équilibriste délicat dans la mise en place de mesures de traçage et de partage d'informations entre d'une part, l'intérêt de tous de prévenir le (l'extension du) phénomène, et d'autre part, l'intérêt de chacun de sauvegarder ses libertés de pensée, d'expression et de mouvement.

Bibliographie

Brion F. (2019), *Evaluation du plan d'action contre la radicalisation dans les prisons tiré des résultats de la recherche BELSPO*, AFFECT, research paper, http://www.belspo.be/belspo/brain-be/projects/FinalReports/AFFECT-RP1-2019-BRION-Evaluation%20du%20plan%20P.pdf.;

De La Serna I. (2020), « La montée en puissance de la répression administrative : recul ou progrès d'une société ? » , *J.T.*, 5, pp. 77-80 ;

Drossens P. (2008), *Archives des services extérieurs de la direction générale des établissements pénitentiaires. Dossier d'étude et de préparation du tableau de tri*, Archives générales du Royaume et archives de l'Etat dans les provinces, Bruxelles, 28 p. ;

Detry I, Mine B., Jeuniaux P. (2021), « Les Banques de Données Communes dans la lutte contre le terrorisme et l'extrémisme (potentiellement) violent », *RDTI*, 80, pp. 47-75 ;

De Valkeneer C. (2017), « Les réponses face au terrorisme: les glissements du judiciaire vers l'administratif » , *J.T.*, 36, pp. 707-711 ;

Dumortier F. (2016), « La Banque de données Nationale Générale : l'œil de Sauron ? » , *Kairos*, 24, pp. 10-11 ;

Dumortier F. et Forget C. (2020), « Le droit d'accès aux banques de données policières » , *J.T.*, 10 : 176-178 ;

Forget C. (2018), « Protection des données dans le secteur de la « police » et de la « justice » », *in Le règlement général sur la protection des données (RGPD/GDPR): analyse approfondie*, Cahiers du CRIDS, Larcier, 44, pp. 865-900 ;

Goedseels E., Ravier I. (2020), « Les évolutions récentes du droit de la jeunesse », *JSJV*, 15 disponible sur https://nicc.fgov.be/upload/publicaties/jsjv15_fr.pdf;

Jonckeere A., Mine B., Detry I., Jeuniaux P., « Travail social en justice et terrorisme, La gestion de l'information par les services de probation », (article soumis) ;

Jonckheere, A. & Maes, E. (2017), « Actualités autour des alternatives à la détention préventive », *in* Y. Cartuyvels, C. Guillain & T. Slingeneyer (Eds.), *Les alternatives à la détention en Belgique: un état des lieux, à l'aune du Conseil de l'Europe*, Coll. Les dossiers de la Revue de Droit Pénal et de Criminologie, n°25, Bruxelles: la Charte, pp. 145-162.

Kaiser V. (2010), « La Banque de données nationale générale et le droit d'accès indirect du citoyen aux données à caractère personnel qu'elle contient », *RDTI*, 43, pp. 5-33 ;

Keuterickx V., Lanaouche M-A., Liners A. (2019), *La loi sur la fonction de police : le manuel de la fonction de police*, Bruxelles, Éditions Politeia ;

Liégeois Y. (2020), *Na een schijnhuwelijk en een schijnscheiding thans een gedwonge opname ? Of de (uitoefeningen van de) rechten van de natuurlijke persoon bij de verwerking van diens persoonsgegevens in het strafproces*, Mercuriale, Anvers, 92 p.;

Leeman S. (2018), *De oprichting van de Belgische databank voor Foreign Terrorist Fighters : een proportionele maatregel ?*, Mémoire déposé dans le cadre de l'obtention d'un master en droit, Gand, 134 p.;

Maes E. (2002), « Studie van de evolutie van de gedetineerdenpopulatie naar misdrijfcategorie (1980-1998) », *Panopticon*, XXIII, 2002, 4, pp. 340-341;

Mine B., Jeuniaux P. et Detry I., « Une exploration de PGP, la base de données policière administrative des personnes, groupements et phénomènes à suivre », *Revue de droit pénal et de criminologie* (à paraitre) ;

Mine B. et Vanneste C. (dir.) (2011), *Recherche relative aux conditions de faisabilité d'une articulation des bases de données statistiques sous la forme d'un « datawarehouse »,* Rapport final, Bruxelles, Institut National de Criminalistique et de Criminologie, Direction Opérationnelle de Criminologie, 220 p., disponible sur https://nicc.fgov.be/upload/publicaties/rapport_25_0.pdf;

Moreau C. (2018), *Comment penser la prestation préventive du droit pénal face au terrorisme de manière ajustée aux droits de l'Homme ? Réflexions à propos des articles 140sexies et 140septies du Code pénal*, Faculté de droit et de criminologie, Université catholique de Louvain, Prom. : Flore, Daniel, 76 p., disponible sur http://hdl.handle.net/2078.1/thesis:15132 ;

Nederlandt O. (2020), « Actualités en droit de l'exécution des peines privatives de liberté: Un état de crise permanent ? », *in* K.Franklin et C. Guillain, *Actualités en droit pénal et exécution des peines*, Larcier, pp. 127-247 ;

Cour des comptes (2011), *Mesures de lutte contre la surpopulation carcérale,* Rapport de la Cour des comptes transmis à la Chambre des représentants, 183 p. ;

Rapports concernant le contrôle conjoint de la banque de données commune Terrorist Fighters et Prédicateurs de Haine par le comité permanent R et l'organe de contrôle de l' information policière (à diffusion restreinte), 2017, 2018 et 2019 ;

Rapports d'activités du Comité permanent de Contrôle des services de renseignements et de sécurité, 2016 à 2019 ;

Rapports d'activités de l'Organe de contrôle de la gestion de l'information policière, 2016 à 2019 ;

Rapport intermédiaire sur le volet « Architecture de la sécurité » de la Commission d'Enquête Parlementaire charge 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 Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste (2017) *Doc. Parl*. 54 1752/008, 584 p. ;

Rapport du Comité de vigilance en matière de lutte contre le terrorisme (Comité T) (2020), 124 p., disponible sur http://comitet.be/wp-content/uploads/2020/03/Rapport-COMITE-T_2020-final.pdf.;

Rapport du comité de concertation sur la création d'une banque-carrefour de la sécurité, 18 mai 2019 (confidentiel), 28 p. ;

Remacle C. (2019), « Le gel administratif des avoirs dans la lutte contre le financement du terrorisme », *Revue de droit pénal et de criminologie,* 2, pp. 123-134 ;

Seron V. (2010), *Le casier judiciaire. L'après-peine entre mémoire et oubli*, Bruxelles, *La Charte,* 415 p. ;

Thomas C. (2020), *L'organisation fédérale de la lutte antiterroriste en Belgique*, *CRISP*, Courrier hebdomadaire, 2463-2464, 63 p ;

Van Hoey M. (2020), « De Belgische gecoördineerde analyse van de dreiging, van de actie en van de informatieflux: van AGG over OCAD naar (de toekomst van) het 'Actieplan Radicalisme' », *Panopticon*, 41 (3), pp. 266-297;

Vanneste C. , Deltenre S., Detry I., Goedseels E, Jonckheere A., Maes E. (2014), « De la production à l'exploitation statistique : l'intervention scientifique dans tous ses états », *in* VESENTINI F. (dir.), *Les chiffres du crime en débat. Regards croisés sur la statistique pénale en Belgique* (1830-2005), Académia-Bruylant, pp. 193-217 ;

Willems M. (2007), *Quelle validité et quelle fiabilité pour les statistiques pénales du Service de la politique criminelle ?*, Ministère de la Fonction publique (I.F.A.) – Ministère de la Justice (S.P.C.), Mémoire de stage, 50 p. ;

Xavier F. (2019), « le développement d'une politique publique fédérale de prévention et de répression administratives de la radicalisation », *in* F. Brion, C. De Valkeneer et V. Francis, *L'effet radicalisation et le terrorisme: Etat des pratiques et des recherches*, Coll. Les Cahiers du GEPS, Tome 1, Bruxelles, Politea, pp. 171-200.