



UNIL | Université de Lausanne

Ecole des sciences criminelles

# La recherche et la gestion des liens dans l'investigation criminelle : le cas de la criminalité organisée.

Thèse de doctorat

Présentée à

l'Institut de Police Scientifique  
de l'Ecole des Sciences Criminelles  
de l'Université de Lausanne

Par

Julien Cartier  
Licencié en sciences forensiques

2009

Série Criminalistique N°46

ISBN 2-940098-50-6



UNIL | Université de Lausanne  
Ecole des sciences criminelles  
bâtiment Batochime  
CH-1015 Lausanne

## IMPRIMATUR

A l'issue de la soutenance de thèse, le Jury autorise l'impression de la thèse de  
M. Julien Cartier, candidat au doctorat en sciences forensiques, intitulée

« La recherche et la gestion des liens dans l'investigation criminelle : le cas de  
la criminalité organisée »

Le Président du Jury



Professeur Pierre Margot

Lausanne, le 30 octobre 2009





## Remerciements

Je tiens ici à remercier toutes les personnes qui ont toutes contribué à la réalisation de cette recherche. Je ne peux toutes les citer ici, mais j'adresse des remerciements particuliers aux personnes suivantes :

En premier lieu, le Prof. Olivier Ribaux, mon directeur de thèse, qui m'a soutenu et fourni de précieuses recommandations et pistes de réflexions tout au long de ce travail ;

Le Prof. Pierre Margot, directeur de l'Ecole des sciences criminelles, président du jury et mon premier directeur de thèse, pour m'avoir aiguillé sur cette voie au sortir de mes études ;

Le Prof. Jean-Luc Bacher, le Dr. Frank Crispino et le commissaire Philippe Gitz, tous trois membres du jury de thèse, qui m'ont fait part de leurs très nombreuses remarques et critiques constructives lors de l'évaluation du manuscrit ;

Messieurs les commandants de la Police cantonale vaudoise, Monsieur Jacques-François Pradervand, Chef de la Police de Sûreté vaudoise, et mes chefs de brigade successifs (Daniel, Christian et Paolo) qui m'ont permis d'aménager mon temps de travail, afin que je puisse efficacement avancer dans cette recherche personnelle ;

Monsieur le Dr. Olivier Guéniat, Chef de la police judiciaire du canton de Neuchâtel, pour son soutien actif lors de mes premières expériences en milieu policier et pour m'avoir communiqué de nombreuses informations au sujet du cas du sadique zoophile ;

Les membres du groupe de référence JANUS et en particulier Jürg Wüthrich, chef de projet informatique, Kurt Iseli et Christian Vogt, chefs de projet utilisateur et Sabine Kalbermatter qui m'a fourni de précieuses statistiques ;

Mes collègues du groupe analyse criminelle de l'ESC, spécialement Sébastien Capt, Quentin Rossy, Stéphane Birrer, Anne-Laure Terrettaz-Zufferey, Sylvain Ioset et Damien Dessimoz, avec qui j'ai pu discuter à de nombreuses reprises d'analyse criminelle ; mes collègues de la police de sûreté vaudoise avec qui j'ai pu acquérir de l'expérience pratique, chronologiquement au sein de la division criminalité organisée de la brigade financière (Pascal, Alain, Karim, les Marcel), puis de la division d'appui opérationnel de la brigade d'appui, d'analyse et de coordination (Nicolas, Gaël, Carine), mais aussi ceux de la brigade des stupéfiants (Frank, Luc, Louis) et tous les autres que je ne peux nommer ici, avec une mention spéciale au Dr. Frédéric Gisler avec qui nous avons pu échanger nos points de vue sur le sujet de la criminalité organisée ;

Mes parents Jacques et Anne-Marie Adam, qui m'ont soutenu moralement et sur un plan logistique durant ces longues années ;

Enfin, ma femme Anne qui a toujours cru en moi et qui m'a apporté un soutien sans faille, ne posant pas trop de questions dans les moments de doute et m'écoutant attentivement lors d'envolées parfois trop enthousiastes, et mes deux magnifiques filles Lucie et Agathe, à qui je demande de m'excuser de leur avoir volé trop de mon temps libre ;

En dernier lieu, je tiens à remercier tout spécialement Jean-Daniel Héritier qui a été mon premier relecteur et avec qui j'ai pu confronter mes premiers manuscrits à un esprit érudit, mais qui ne pourra plus lire ces quelques lignes puisqu'il en a décidé autrement.

*A Jean-Daniel*

*A Anne, Lucie et Agathe*



**Puzzle**, n. m. mot anglais « embarras », de *to puzzle* « laisser perplexe ; essayer de résoudre »

1. Jeu de patience, composé d'éléments à assembler pour reconstituer une image.
2. Multiplicité d'éléments qu'un raisonnement logique doit assembler pour reconstituer la réalité des faits.

*Les pièces du puzzle commençaient à s'ordonner dans sa tête.*

Dictionnaire « Le Robert pour tous », 1994



## TABLE DES MATIERES :

INTRODUCTION.....	1
<b>1 ETAT DES LIEUX .....</b>	<b>11</b>
1.1 CRIMINALITE ORGANISEE.....	11
1.1.1 <i>Notions (en Suisse)</i> .....	12
1.1.1.1 Crime organisé .....	13
1.1.1.2 Criminalité organisée .....	14
1.1.1.3 Organisation criminelle .....	16
1.1.2 <i>Champ d'application de cette recherche</i> .....	17
1.1.3 <i>Caractéristiques de la criminalité organisée</i> .....	18
1.1.3.1 Différents paradigmes .....	19
1.1.3.2 La superpuissance des organisations criminelles : un mythe qui s'effondre .....	20
1.1.3.3 Criminalité mobile et itinérante.....	21
1.1.3.4 Criminalité secrète, qualifiée dans sa forme la plus intégrée de « mafia » .....	22
1.1.3.5 Criminalité avec un fort pouvoir d'adaptation.....	22
1.1.3.6 Caractéristiques récurrentes .....	23
1.1.4 <i>Survol de l'état de la lutte contre la criminalité organisée en Suisse</i> .....	24
1.1.4.1 Au plan législatif .....	24
1.1.4.2 Au plan de la procédure.....	28
1.1.5 <i>Synthèse</i> .....	30
1.2 L'ENQUETE CRIMINELLE .....	33
1.2.1 <i>Retour aux notions de base</i> .....	35
1.2.2 <i>Les principes</i> .....	35
1.2.2.1 Le but de l'enquête.....	35
1.2.2.2 Les dimensions de l'enquête .....	37
1.2.2.3 La méthodologie de l'enquête .....	37
1.2.3 <i>Le contexte</i> .....	38
1.2.3.1 L'enquête proactive versus réactive .....	39
1.2.4 <i>Les étapes du processus d'enquête</i> .....	41
1.2.4.1 Les phases de l'enquête proactive .....	43
1.2.5 <i>L'organisation du système de poursuite pénale</i> .....	46
1.2.5.1 Les différents modèles organisationnels.....	47
1.2.5.2 De l'avant-projet au code de procédure pénale suisse .....	49
1.2.5.3 L'organisation de la police judiciaire .....	50
1.2.5.4 Organisation pratique de l'enquête judiciaire.....	58
1.2.6 <i>Synthèse</i> .....	60
1.3 LES BASES DE DONNEES DE POLICE .....	63
1.3.1 <i>Notion de base de données</i> .....	63
1.3.2 <i>Evolution des fichiers aux bases de données</i> .....	63
1.3.2.1 Fichiers.....	63
1.3.2.2 Bases de données.....	65
1.3.3 <i>Survol historique des bases de données de police en Suisse</i> .....	73
1.3.3.1 Au niveau cantonal.....	73
1.3.3.2 Au niveau fédéral .....	75
1.3.4 <i>Les bases de données centralisées de police judiciaire</i> .....	77
1.3.4.1 Les bases de données centralisées JANUS .....	78
1.3.5 <i>Les bases de données utiles à l'enquête</i> .....	81

1.3.6	<i>Synthèse</i> .....	82
1.4	L'ANALYSE CRIMINELLE .....	84
1.4.1	<i>Définitions</i> .....	85
1.4.2	<i>Origines de l'analyse criminelle</i> .....	85
1.4.3	<i>Cadre de l'analyse criminelle</i> .....	86
1.4.4	<i>Champ d'application de l'analyse criminelle</i> .....	87
1.4.5	<i>Méthodes de travail</i> .....	90
1.4.5.1	Le cycle du renseignement .....	90
1.4.5.2	Raisonnements .....	91
1.4.5.3	Décomposition et interprétation des informations.....	96
1.4.6	<i>Techniques proposées dans le cadre de la criminalité organisée</i> .....	101
1.4.6.1	Diagrammes relationnels.....	102
1.4.6.2	Les analyses de contrôles techniques .....	108
1.4.6.3	Schémas relationnels et analyse de réseaux sociaux.....	115
1.4.6.4	Diagrammes chronologiques .....	125
1.4.7	<i>Synthèse</i> .....	131
<b>2</b>	<b>LE PROJET</b> .....	<b>133</b>
2.1	POSTULAT 1 – BESOIN DE PARTAGER LES INFORMATIONS .....	136
2.1.1	<i>Parabole du puzzle</i> .....	136
2.1.1.1	Base de données commune.....	136
2.1.1.2	Base de données structurée.....	136
2.1.2	<i>Situation actuelle</i> .....	137
2.2	POSTULAT 2 – BESOIN DE RECONSTRUIRE UNE SITUATION .....	139
2.2.1	<i>Parabole du puzzle</i> .....	139
2.2.1.1	Besoin de mettre des personnes en relation.....	139
2.2.1.2	Besoin de disposer d'éléments factuels .....	140
2.2.2	<i>Situation actuelle</i> .....	140
2.3	POSTULAT 3 – BESOIN D'ANALYSER LA SITUATION .....	142
2.3.1	<i>Parabole du puzzle</i> .....	142
2.3.1.1	Besoin d'un outil de représentation (visualisation graphique).....	142
2.3.1.2	Besoin d'un outil évolutif (base de données) .....	142
2.3.1.3	Besoin d'un système d'analyse dynamique (base de données d'analyse).....	143
2.3.2	<i>Situation actuelle</i> .....	144
2.4	DESCRIPTION DU PROJET .....	145
2.4.1	<i>Besoins de chaque intervenant</i> .....	145
2.4.1.1	Besoins de l'enquêteur .....	145
2.4.1.2	Besoins de l'analyste.....	148
2.4.1.3	Compromis.....	149
2.4.2	<i>Concept</i> .....	150
2.4.3	<i>Système basé sur deux composants</i> .....	151
2.4.3.1	Base de données d'enquête centralisée (JANUS PV 2.0).....	151
2.4.3.2	Bases de données d'analyse .....	152
2.4.4	<i>Composants interconnectés</i> .....	154
2.4.4.1	Possibilités de flux de données descendant pour l'analyse.....	154
2.4.4.2	Possibilités de flux de données montant pour alimenter la mémoire à long terme .....	155
2.4.5	<i>Synthèse</i> .....	155
2.5	HYPOTHESE 1 – FAISABILITE DU PROJET.....	157
2.5.1	<i>Bases de données d'enquête centralisées</i> .....	157



2.5.1.1	JANUS PV (Personnes et antécédents) .....	158
2.5.1.2	JANUS JO .....	161
2.5.1.3	Synthèse .....	163
2.5.2	<i>Structure détaillée de JANUS PV</i> .....	163
2.5.2.1	Modèle conceptuel : personnes et antécédents (Personen und Vorgänge – PV).....	163
2.5.2.2	IDENTITE .....	165
2.5.2.3	REL>, REL>adr (relations interpersonnelles).....	167
2.5.2.4	SOC> (société).....	169
2.5.2.5	ADR>, HOT> (adresse, hôtel) .....	169
2.5.2.6	AUT>, DET> (automobile, détenteur) .....	171
2.5.2.7	CPT> (comptes).....	171
2.5.2.8	TEL>, ABO> (téléphone, abonnement) .....	172
2.5.2.9	URL> (adresse Internet).....	174
2.5.2.10	OBJ> (objet).....	175
2.5.2.11	PAS> (passeport) .....	175
2.5.2.12	VER> (arrestation).....	176
2.5.3	<i>Organisation détaillée de JANUS PV</i> .....	177
2.5.3.1	Situation illustrative .....	178
2.5.4	<i>Synthèse</i> .....	184
2.5.4.1	Potentialités des systèmes centralisés de la Confédération.....	186
2.5.4.2	Développements possibles .....	187
2.6	HYPOTHESE 2 – UTILITE DU PROJET .....	188
2.6.1	<i>Méthodologie de test</i> .....	189
2.6.1.1	Test du gain d'information .....	189
2.6.1.2	Test du gain de temps.....	190
2.6.1.3	Test du gain de capacité d'analyse .....	191
2.6.1.4	Recherche des problèmes persistants ou nouveaux .....	192
<b>3</b>	<b>REALISATION</b> .....	<b>193</b>
3.1	MODELE METHODOLOGIQUE .....	193
3.1.1	<i>Entités</i> .....	194
3.1.1.1	Type .....	194
3.1.1.2	Identifiant .....	200
3.1.1.3	Représentation graphique des entités .....	201
3.1.2	<i>Connexions</i> .....	202
3.1.2.1	Types.....	202
3.1.2.2	Représentation graphique des connexions.....	206
3.1.3	<i>Niveau de détail</i> .....	208
3.1.3.1	Matrice relationnelle .....	209
3.1.3.2	Adéquation du niveau de détail à la situation.....	212
3.1.3.3	Possibilités de navigation (niveaux d'agrégation) .....	214
3.1.4	<i>Synthèse</i> .....	217
3.2	JANUS PV 2.0 (BASE DE DONNÉES D'ENQUÊTE CENTRALISÉE) .....	218
3.2.1	<i>Introduction</i> .....	219
3.2.2	<i>Structure et organisation</i> .....	221
3.2.3	<i>Entités : « sous-champs » et « attributs »</i> .....	223
3.2.3.1	Objets de JANUS PV 2.0 .....	224
3.2.4	<i>Système d'interconnexion : importation et exportation</i> .....	233
3.2.4.1	Importation des « sous-champs » .....	233
3.2.4.2	Importation et exportation des données souches .....	233

3.2.5	<i>Synthèse</i> .....	234
3.3	PROTOTYPE $\beta$ (BASE DE DONNÉES D'ANALYSE).....	235
3.3.1	<i>Introduction</i> .....	235
3.3.2	<i>Structure et organisation</i> .....	236
3.3.2.1	Structure .....	236
3.3.2.2	Organisation.....	242
3.3.3	<i>Valeurs standardisées : selon le standard ISO de JANUS PV 2.0</i> .....	246
3.3.4	<i>Système de visualisation : relationnel et chronologique</i> .....	248
3.3.4.1	Représentations relationnelles .....	249
3.3.4.2	Représentations chronologiques.....	254
3.3.5	<i>Autres fonctions d'analyse propres à iBase™ et utiles au prototype <math>\beta</math></i> .....	256
3.3.5.1	Recherches visuelles et pondérées.....	256
3.3.5.2	Sélections (Sets).....	258
3.3.5.3	Exploration et recherche « texte » .....	259
3.3.6	<i>Synthèse</i> .....	260
3.4	INTERCONNEXION DES DEUX COMPOSANTS DU SYSTÈME .....	262
3.4.1	<i>Exportation de JANUS PV 2.0</i> .....	264
3.4.1.1	Visualisation de JANUS PV 2.0.....	266
3.4.1.2	Relation avec d'autres systèmes d'information.....	272
3.4.2	<i>Importation XML dans iBase™</i> .....	273
3.4.3	<i>Traitements XML</i> .....	275
3.5	RÉSULTATS DE LA MISE EN ŒUVRE .....	276
3.5.1	<i>Composant mémoire à long terme</i> .....	276
3.5.1.1	Enquête B&W .....	276
3.5.2	<i>Composant analyse</i> .....	279
3.5.2.1	Opération DK.....	281
3.5.3	<i>Système interconnecté</i> .....	283
3.5.3.1	Affaire VO .....	283
<b>4</b>	<b>EVALUATION DES RESULTATS ET DISCUSSION.....</b>	<b>285</b>
4.1	FAISABILITE DU PROJET.....	287
4.2	UTILITE DU PROJET.....	291
4.2.1	<i>Gain d'information ?</i> .....	291
4.2.1.1	Système plus facile d'accès → Plus d'adhérents ? .....	291
4.2.1.2	Système plus performant → Plus d'intérêt ? .....	292
4.2.1.3	Système plus convivial → Plus de participants ? .....	293
4.2.1.4	Système plus précis → Plus de données structurées ? .....	296
4.2.1.5	Synthèse .....	298
4.2.2	<i>Gain de temps ?</i> .....	299
4.2.2.1	Système plus simple → Moins de saisies intermédiaires ? .....	299
4.2.2.2	Système plus ouvert → Moins de double saisie ? .....	300
4.2.2.3	Système plus intégré → Moins de manipulations ? .....	300
4.2.2.4	Système plus précis → Moins de formatage ? .....	301
4.2.2.5	Synthèse .....	301
4.2.3	<i>Gain de capacité d'analyse ?</i> .....	302
4.2.3.1	Gain d'intégration → L'analyse est meilleure ? .....	302
4.2.3.2	Gain de précision → L'analyse est meilleure ? .....	303
4.2.3.3	Gain de décomposition → L'analyse est plus fine ? .....	303
4.2.3.4	Gain de structuration → L'analyse est plus standardisée ? .....	304

4.2.3.5	Synthèse .....	304
4.2.4	<i>Problèmes nouveaux ou récurrents</i> .....	304
4.2.4.1	Problème récurrent : la place des analystes.....	305
4.2.4.2	Problème nouveau : une collaboration durable.....	306
4.3	PERSPECTIVES POUR L'ANALYSE CRIMINELLE OPERATIONNELLE.....	309
4.3.1	<i>Encadrement de l'étape d'analyse</i> .....	310
4.3.1.1	Limites et biais de la cognition.....	314
4.3.1.2	Limites du processus d'analyse.....	314
4.3.1.3	Effets de contexte.....	315
4.3.1.4	Procédure de production et de test d'hypothèses.....	318
4.3.1.5	Matrice d'analyse bayésienne d'hypothèses concurrentes.....	325
4.3.2	<i>Perspectives de l'automatisation</i> .....	328
4.3.2.1	Concurrence ou complémentarité ?.....	331
4.3.2.2	Outils informatisés d'analyse d'hypothèse concurrentes.....	335
4.3.2.3	Synthèse .....	339
<b>5</b>	<b>CONCLUSION</b> .....	<b>341</b>
<b>6</b>	<b>BIBLIOGRAPHIE</b> .....	<b>349</b>
6.1	ARTICLES ET OUVRAGES .....	349
6.2	TEXTES LEGAUX.....	356
<b>7</b>	<b>ANNEXES</b> .....	<b>363</b>



## Avant-propos

Cette thèse s'inscrit dans le prolongement de précédents travaux de doctorat qui ont eu pour sujet d'étude la recherche et la gestion des liens dans l'investigation<sup>1</sup>, mais qui se sont focalisés sur des cas particuliers différents.

Au départ, nous pensions que cette recherche devait se concentrer sur la lutte contre le trafic illicite de stupéfiants. L'Institut de Police Scientifique (IPS) de l'École des Sciences Criminelles de l'Université de Lausanne a en effet été très actif, depuis le début des années 1990, notamment dans le développement du profilage des stupéfiants, ce qui a débouché sur la publication de nombreuses thèses et d'un ouvrage de référence dans ce domaine<sup>2</sup>. Ces recherches ont ainsi permis le traitement systématique des signatures chimiques<sup>3</sup> de certains produits stupéfiants. Ces travaux ont permis à l'IPS d'apporter un nouvel éclairage aux services de police chargés de mener les investigations en matière de lutte contre le trafic illicite de stupéfiants, par le lien physico-chimique qu'il est désormais possible d'établir entre les différentes saisies effectuées par la police.

L'amorce de cette recherche a été la question de l'intégration de cette information au processus d'enquête, afin de rendre son utilisation optimale.

N'ayant alors que peu de connaissances des processus d'enquête dans le cadre de la lutte contre le trafic illicite de stupéfiants, cette recherche a débuté par un travail d'exploration, de réflexion et d'analyse de fonctionnements plus souvent coutumiers que basés sur des règles écrites et soumis à des perpétuels changements dus aux évolutions d'ordre législatif, procédural, structurel, financier, technologique ou encore simplement humain.

Différents stages ont été organisés dès 1998 dans les services spécialisés de différents cantons romands. Ces immersions temporaires ont débouché en 2000 par une plongée en profondeur de l'auteur de cette présente recherche au sein du groupe de lutte contre la criminalité organisée de la brigade financière de la police de sûreté vaudoise, puis au sein d'une unité nouvelle spécialisée dans l'analyse et l'appui opérationnel à l'enquête.

La délimitation de la recherche à la seule lutte contre le trafic illicite de stupéfiants est dès lors rapidement apparue comme trop restrictive, tant les mécanismes et stratégies mis en place dans ce cadre précis étaient extensibles à la lutte contre tout type de criminalité agissant de manière plus ou moins organisée.

---

<sup>1</sup> TARONI, 1997 ; RIBAUX, 1997

<sup>2</sup> GOLDMANN, 2000 ; GUENIAT, 2001 ; ESSEIVA, 2004 ; LOCK, 2005 ; ZINGG, 2005 ; BAER, 2007 ; LOCICIRO, 2007 ; GUENIAT, ESSEIVA, *Le profilage de l'héroïne et de la cocaïne, une méthodologie moderne de lutte contre le trafic illicite*, 2005

<sup>3</sup> ESSEIVA, *et al.*, *Les signatures chimiques à partir des saisies de produits stupéfiants : Utilité et gestion de l'information*, 2002



## Introduction

Le travail qui vous est proposé ici s'inscrit dans le contexte judiciaire, plus particulièrement policier et précisément sur *ce que fait la police*. CUSSON<sup>4</sup> définit son action, connue en anglais sous le terme de *policing*, en « action de sécurité », ce qui lui permet d'élargir le propos au secteur privé. Cet auteur distingue quatre fonctions dans l'action de sécurité qu'il retrouve dans les services de police d'une certaine importance. Il définit ces fonctions et schématise les rapports qui les nouent de la manière suivante :

« Une fonction est une catégorie d'activités qui apportent une contribution essentielle à un organisme. Une fonction de sécurité serait donc une catégorie d'opérations nécessaires pour sécuriser un ensemble de personnes et de biens. Quatre fonctions sont remplies dans la plupart des grands services de sécurité non spécialisés : 1) le renseignement qui est un processus de cueillette et d'analyse d'informations en vue de connaître les problèmes et de guider l'action ; 2) la prévention, c'est-à-dire les mesures non coercitives pour empêcher les attentats, destructions, vols ou crises ; 3) la répression, c'est-à-dire le recours à la force et à la sanction pour dissuader et mettre hors d'état de nuire les malfaiteurs ; et 4) la gestion de crise, qui est l'intervention d'urgence lors d'événements qui tournent mal. » (p. 45)

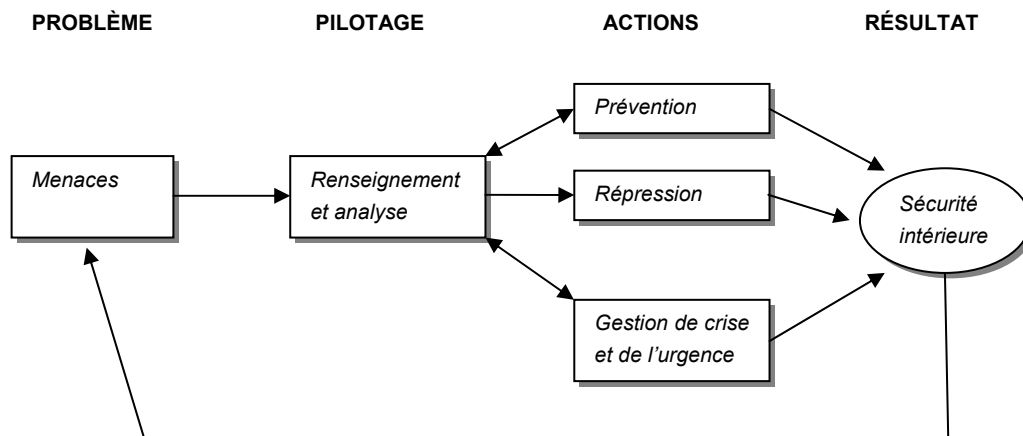


fig. 1 : Rapports qui se nouent entre les quatre fonctions de l'action de sécurité<sup>5</sup>

Cette figure montre que les policiers, et par extension les autres acteurs de la sécurité publique et / ou privée, ne doivent plus se borner à une approche purement réactive, qui consiste à appliquer servilement la loi ou des procédures prédéfinies sans même se poser la question du problème sécuritaire auquel ils font face. Il est aujourd'hui nécessaire pour ces acteurs de vouloir comprendre

<sup>4</sup> CUSSON, De l'action de sécurité, in CUSSON, DUPONT, LEMIEUX, Traité de sécurité intérieure, 2008, p.43

<sup>5</sup> Figure tirée de CUSSON, *op. cit.*, p.47

les problèmes, de les analyser et de tenter d'y apporter des réponses (répressives ou préventives) dont ils devraient s'efforcer de mesurer les effets.<sup>6</sup>

Ce travail de doctorat qui s'intéresse à la problématique de la lutte contre la criminalité organisée a voulu suivre une démarche holistique et pragmatique. Celle-ci a eu pour but de proposer un système d'aide aux investigations criminelles reposant sur une méthode basée sur une organisation du flux de données et une architecture fondée sur deux composants informatiques. Nous avons cherché à valider cette méthode par le développement d'outils informatisés faisant partie de ce système. Ces moyens, nouveaux en Suisse, s'inscrivent dans la fonction répressive de l'investigation de police judiciaire et se basent sur des méthodes d'analyse criminelle<sup>7</sup>, fonction devant permettre le pilotage de l'action de sécurité.

Cette recherche se concentre donc sur l'enquête judiciaire et en particulier sur le cadre de la lutte contre la criminalité organisée, ainsi que des méthodes de travail et des moyens qui y sont mis en œuvre. Ce contexte reste aujourd'hui encore très mal formalisé. Il existe, en effet, très peu de recherches sur l'application de systématiques « scientifiques » dans l'investigation criminelle<sup>8</sup>, que ce soit sur les méthodologies adoptées, sur les processus mis en place ou encore sur les raisonnements apparaissant dans toute enquête. De plus, ces pratiques évoluent sans cesse en fonction de diverses contraintes et des affaires rencontrées.

La situation actuelle présente donc de nombreuses faiblesses qui, si elles sont souvent ressenties par les praticiens, sont difficilement identifiées précisément et rarement traitées de manière systémique.

En regard de certaines faiblesses, des besoins se font également clairement sentir. Par exemple, il paraît nécessaire de pouvoir poser un cadre plus structuré à l'enquête judiciaire dans le contexte de la lutte contre la criminalité organisée. Il semble aussi que les développements méthodologiques proposés par l'analyse criminelle opérationnelle peuvent apporter une réponse appropriée à ce type de problème. Ainsi, il pourrait être envisageable de fournir dans des délais raisonnables de nouveaux outils aux policiers.

En l'absence d'une formalisation scientifique préexistante suffisante, ce travail a donc dû s'appuyer sur des bonnes pratiques identifiées et usitées de manière récurrente dans le monde judiciaire à

---

<sup>6</sup> Cette approche stratégique (*Problem-oriented policing*) apparue dans les années 1990 aux Etats-Unis et associée au nom d'Herman GOLDSTEIN. BRODEUR la traduit par *police d'expertise* ou *police par résolution de problèmes*. Voir notamment : BRODEUR, *Tailor Made Policing: a Conceptual Investigation*. in BRODEUR, *How to Recognize Good Policing*, 1998 ou DUPONT, *Police communautaire ou de résolution de problèmes*, in CUSSON, DUPONT, LEMIEUX, *Traité de sécurité intérieure*, 2008, p.98

<sup>7</sup> *Criminal Intelligence* en anglais, dans le sens du renseignement criminel. Voir chapitre 1.4 – L'analyse criminelle

<sup>8</sup> On peut notamment citer : KIND, *The Scientific Investigation of Crime*, 1987



plusieurs niveaux : légal, structurel ou organisationnel, méthodologique, technique<sup>9</sup>. En parallèle, il a été possible de mettre à jour des blocages, ou des fonctionnements peu satisfaisants.

Il aura souvent fallu décrire ces dysfonctionnements, car ils ne sont que très rarement formalisés et n'apparaissent pas clairement aux yeux des personnes qui les subissent pourtant quotidiennement.

Pour que le nouveau moyen d'aide aux investigations criminelles dans le contexte de la lutte contre la criminalité organisée proposé par cette recherche puisse avoir une chance d'être un jour réellement mis en œuvre, il devait pouvoir s'inscrire dans un processus global qui prenne en compte les différentes contraintes inhérentes à chaque niveau (tel que défini ci-dessus). Sans prendre en compte dès le départ l'intégration future d'un tel moyen dans ce contexte pluridisciplinaire, il aurait été illusoire d'espérer arriver finalement à un processus du traitement de l'information qui amène aux enquêteurs *in fine* un moyen fonctionnel plus efficient. Le système projeté devait permettre aux investigateurs de pouvoir bénéficier d'outils faits sur mesure, en adéquation avec la légalité des moyens engagés, les limites structurelles des organisations et les méthodes systématiques du traitement de l'information. Ce n'est qu'à cette condition que les investigateurs pourront à l'avenir évoluer dans un environnement favorable à l'analyse des données qu'ils collectent dans leurs enquêtes, ce qui leur permettrait de dégager enfin le temps qui fait toujours défaut et qui est nécessaire à l'analyse et à la réflexion.

Ce projet propose une méthode de travail basée sur un modèle d'organisation du flux de données dans l'enquête judiciaire. L'architecture de ce modèle est fondée sur deux composants interconnectés et informatisés constituant un système d'aide aux investigations criminelles.

Le premier composant (banque de données nationale JANUS) est alimenté et essentiellement partagé par l'ensemble des polices Suisses. Il répertorie des informations sur les personnes et des événements qui relèvent de la criminalité organisée. Le second composant est temporaire et est sollicité lorsque des affaires particulières nécessitent l'intégration d'un extrait d'informations provenant de JANUS, ainsi que l'absorption rapide d'informations spécifiques éventuellement pas encore confirmées (par exemple provenant d'informateurs) et qui ne présentent pas un intérêt général immédiat.

Par exemple, dans les enquêtes sur les réseaux de distribution illégale de produits stupéfiants, les données concernant les trafiquants sont systématiquement répertoriées dans la base de données JANUS. Lorsqu'une nouvelle information nécessitant des investigations est portée à la connaissance de la police, cette information est évaluée à l'aide des données déjà présentes dans JANUS, et si cela est nécessaire, une affaire particulière est déclenchée. Un extrait des données connexes à cette affaire présentes dans JANUS est réalisé et il initialise le fonctionnement du second composant qui, lui-même, est alors alimenté par d'autres données spécifiques d'enquête.

---

<sup>9</sup> Voir 1.4.3 – Les cadres de l'analyse criminelle

Le système proposé se base sur deux composants pour les raisons suivantes<sup>10</sup> :

- les données générales relatives aux enquêtes criminelles en matière de criminalité organisée doivent être partagées. Ce type de criminalité dépasse presque assurément les frontières cantonales, régionales et même nationales, celles-ci définissant des juridictions différentes, et participant ainsi généralement au cloisonnement des données qui s’y rapportent (JANUS).
- la complexité des données recueillies, notamment par leur nombre, leurs types, leur qualité, nécessite de disposer d’un moyen d’analyse dynamique. Le second composant externe et ponctuel répond spécifiquement à ce besoin (base d’analyse iBase™).
- L’enquête criminelle cherche à reconstruire une situation passée ou à comprendre une situation courante selon trois dimensions: *les entités et leurs relations* (personnes ou choses), *le temps et les lieux*. Dans le cadre des investigations sur la criminalité organisée, il est primordial de pouvoir apprécier le rôle joué par les protagonistes au sein du groupement criminel, notamment en se basant sur les relations déterminées par des liens factuels. Ce système définit pour les deux composants un modèle conceptuel générique qui permet de répertorier ces faits et les met en perspective pour faciliter leur analyse selon ces trois dimensions (cherche à reproduire le réel)

Toutefois, il faut être réaliste, construire un système global en fonction de problèmes encore mal formalisés tient de la gageure. Les difficultés récurrentes rencontrées depuis des dizaines d’années dans le développement des bases de données policières ne sont donc pas surprenantes. Le tout est sans conteste très ambitieux.

En parallèle au développement du système imaginé dans cette recherche, une réflexion a été entreprise sur la criminalité organisée, en particulier sur les bases de données qui sont dédiées aux enquêtes relatives à des groupements criminels (JANUS)<sup>11</sup>. Par des redéfinitions de leur structure de données et de quelques principes d’utilisation, ce travail permet de mettre aujourd’hui en évidence une série de notions utilisées dans le cadre de l’investigation de la criminalité organisée et qui aideront à définir à l’avenir des modèles plus complets dont pourront ensuite découler des méthodes et structures d’analyse. Ces modèles pourront alors à leur tour avoir un impact sur les nouveaux développements, des changements de bases légales, de nouvelles organisations au sein des autorités de poursuite ou encore de l’intégration de l’analyse criminelle opérationnelle en Suisse, et *in fine* à la mise à disposition d’un système cohérent.

\* \* \*

---

<sup>10</sup> Ces raisons seront évidemment reprises en détail dans le deuxième chapitre.

<sup>11</sup> Voir chapitre 1.3.4

Cette thèse est divisée en quatre chapitres principaux : L'état des lieux de la situation actuelle dans le contexte de la lutte contre la criminalité organisée, la description du projet de recherche, les résultats obtenus, et l'évaluation et la discussion de ces derniers.

Le premier chapitre est donc consacré à la description de la situation dans des domaines directement concernés par le sujet de cette recherche.

Ainsi, la première partie va délimiter le champ d'application de cette recherche, notamment en éclaircissant la différence que nous donnons aux notions de *criminalité organisée* et de *crime organisé*, qui se retrouvent tant dans les contextes criminologique que juridique. La situation actuelle de la lutte contre la *criminalité organisée* en Suisse au plan de la loi et de la procédure pénale sera également abordée ici. On verra ainsi que les nouvelles normes pénales spécifiques introduites dans les années 1990 peinent à trouver une mise en application satisfaisante.

La deuxième partie s'attache à décrire *l'enquête judiciaire* : ses principes, ses dimensions, le contexte dans lequel les acteurs évoluent et les phases du processus qui se succèdent, allant de la première information, constat ou élément rapporté à sa conclusion. La description du processus d'investigation et de ses contraintes servira de base à la méthode de travail choisie pour l'élaboration du système d'aide à l'enquête. Deux différents modèles organisationnels de la poursuite pénale, qui ont toujours cours en Suisse seront sommairement exposés, bien qu'ils seront unifiés d'ici peu de temps en un seul code de procédure pénale. Les structures et organisations qui en découleront seront celles dans lesquelles le système proposé dans ce projet de recherche devra s'inscrire.

La troisième partie traite des *bases de données*. On dit souvent que la police peut se reposer sur deux de ses atouts : le temps et la mémoire. Or, comment aujourd'hui conserver de la mémoire au fil du temps ? Le recours à des bases de données informatisées est actuellement un bon moyen technique d'y arriver. Les modèles des bases de données ont beaucoup évolué au fil de ces quarante dernières années. Ils évoluent encore et ils influencent souvent grandement les solutions envisagées *a priori*, qui sont utilisées et dont les systèmes suivants hériteront par la suite. Une description de certains fondamentaux sera donc nécessaire. En outre, un historique de l'utilisation des bases de données dans le cadre judiciaire permettra de constater que de nombreuses difficultés ont été rencontrées jusqu'ici et que la situation actuelle compose avec un lourd héritage. Cependant, il demeure encore une ouverture importante, car une base de données centralisée au niveau suisse et dédiée aux enquêtes sur les groupements criminels organisés existe. Elle dispose déjà d'un cadre légal qui peut permettre d'intégrer le système proposé par cette recherche. Elle souffrait toutefois avant 2005 de lacunes dues à la technologie désuète utilisée lors de sa conception quinze ans plus tôt.

La dernière partie du premier chapitre est réservée à l'*analyse criminelle* et en premier lieu à la description de sa méthodologie sous-jacente. Celle-ci s'exprimant par un processus systémique du traitement de l'information, lui-même influencé par chacun des cadres qui l'entourent (légal, structurel, organisationnel, méthodologique ou technique). Ce processus fondamental itératif peut être assimilé à une assurance qualité du traitement de l'information qui décrit les étapes fondamentales du traitement de toute information. L'étape de l'analyse constitue la réelle mise en valeur de l'information par le développement systématique d'hypothèses. Entrent en jeu à ce stade des raisonnements analytiques (aussi qualifiés suivant les auteurs de régressifs ou de « non-démonstratifs »).

Les origines de l'analyse criminelle, son cadre et son champ d'application, ainsi que des méthodes de travail et des techniques utilisées dans la lutte contre la criminalité organisée y seront aussi décrits, puisqu'ils feront partie du système proposé par cette recherche. On pourra constater encore que des vides méthodologiques importants sont encore bien présents dans cette discipline.

\* \*

Le deuxième chapitre présente les éléments qui ont mené au projet de cette recherche, par une critique constructive de la situation du début des années 2000. Ainsi, trois postulats illustrés par la parabole du jeu du puzzle y sont formulés. Suivent ensuite la description du projet et les hypothèses de travail que sont sa faisabilité et son utilité.

Le premier postulat<sup>12</sup> met en évidence que l'un de moyens pour résoudre un puzzle est de disposer de toutes les pièces, ou du moins le but doit être d'en recueillir un maximum. Il en est de même dans l'investigation criminelle. Différents facteurs, apparaissant à tous niveaux, peuvent empêcher les acteurs de disposer des pièces d'information et de pouvoir ainsi résoudre l'enquête. Cette inhabilité à faire des liens a été formalisée dans les années 1980 par EGGER par la notion de *linkage blindness*<sup>13</sup>.

Le deuxième postulat<sup>14</sup> traite de la mise en relation des pièces du puzzle. Les questions que les joueurs se posent en tentant de résoudre le puzzle sont : *qui ?*, *quand ?*, *quoi ?*, *où ?*, *comment ?* (et

---

<sup>12</sup> *En matière d'investigation sur la criminalité organisée, le partage d'informations est devenu impératif. A l'heure actuelle, il doit notamment se faire grâce à des outils à haut potentiel qualitatif et quantitatif, comme une base de données commune aux unités d'enquête et structurée en fonction du but recherché.*

<sup>13</sup> « The nearly total lack of sharing or coordinating investigative information and the lack of adequate networking by law enforcement agencies » (p. 164-165) in EGGER, *Serial Murder: An Elusive Phenomenon*, 1990

<sup>14</sup> *Dans toute enquête criminelle, on cherche à reconstruire une situation passée ou présente, selon les trois dimensions de l'enquête (entités, temps et lieux). Dans le cas particulier de la criminalité organisée, la stratégie d'enquête passe*

éventuellement *pourquoi* ?). Ces questions permettent de remettre un élément dans son contexte et de l'interpréter correctement. Ces questions sont les mêmes dans l'investigation criminelle<sup>15</sup> et s'organisent selon les trois dimensions principales de la reconstruction de la réalité : les entités (*qui et quoi* ?), le temps (*quand* ?), et le lieu (*où* ?).

Tout comme pour un puzzle qui est subdivisé en pièces, les enquêtes reposent sur des faits qu'il faut assembler pour pouvoir reconstruire la réalité. Ces éléments factuels de base doivent être individualisables, bien que de types différents (personnes ou choses, lieux, événements), pour pouvoir générer des liens et permettre d'obtenir une image de la situation à un temps donné.

Le troisième postulat<sup>16</sup> s'intéresse aux moyens qui pourraient être utilisés par des joueurs lorsqu'ils s'appliquent à reconstruire un puzzle pour lequel ils disposent du maximum de pièces et dont les possibilités de mise en relation (découpe des pièces) sont existantes, mais sans qu'ils aient réellement visuellement accès aux pièces du puzzle (comme c'est aujourd'hui le cas pour les enquêteurs).

Dans le cadre de la lutte contre la criminalité organisée, si peu de résultats spectaculaires ont été obtenus jusqu'ici, souvent à cause de certains dysfonctionnements légaux ou de procédure, il apparaît aussi clairement que la complexité des affaires traitées, par le nombre d'informations à disposition des enquêteurs, ne leur permettait plus d'obtenir une image satisfaisante des faits, et que le recours à des moyens d'analyse restait encore largement sous-développé. Ces moyens auxiliaires doivent être graphiques et évolutifs, afin de permettre l'analyse itérative des informations nouvelles permettant de reconstruire la réalité des faits.

La troisième partie de ce chapitre traite du projet pratique de la recherche qui consiste en la réalisation d'un prototype de système d'aide aux investigations criminelles dans le cadre de la lutte contre la criminalité organisée. Ce système prévoit une gestion du renseignement criminel transversale et itérative basée sur deux composants principaux interconnectés de manière bidirectionnelle : la base de données de police centralisée, réglementée et jouant le rôle de mémoire à long terme, et la base de données d'analyse, jouant celui de mémoire à court terme, en jouissant de plus de précision, de liberté d'action et de flexibilité dans le traitement d'informations encore incertaines en cours d'enquête.

---

*par la détermination du rôle et de l'implication de chacun des protagonistes dans le groupement criminel apparaissant lors des investigations.*

<sup>15</sup> Un vers de QUINTILIEN, rhéteur et pédagogue latin du Ier siècle apr. J.-C., resté célèbre, résume à lui seul la démarche de toute investigation criminelle : *Quis, quid, ubi, quibus auxiliis, cur, quomodo, quando* : Qui (a commis l'acte criminel), quoi (de quoi s'agit-il ?), où, avec quels moyens, pourquoi, comment, quand ?

<sup>16</sup> *Le nombre et la complexité des relations en rapport avec une affaire particulière, ou par extension à plusieurs cas, nécessitent la mise en place d'un système d'analyse dynamique qui permette dans un premier temps d'apprécier une situation de départ et dans un second temps d'adapter son appréciation en fonction des nouveaux éléments.*

Ce système bi-composant permet de proposer un prototype fonctionnel en évitant de vouloir construire directement un système global reposant sur des fondations trop mal formalisées. Il permet aussi de trouver plus facilement un compromis qui tienne compte des besoins souvent antagonistes des différents utilisateurs du système que sont les « policiers » et les « analystes », sans trop alourdir l'ensemble. Les premiers nommés ayant besoin en priorité de *rapidité*, de *simplicité*, de *centralisation* et d'*exhaustivité* ; alors que les analystes réclament la *précision*, la *structuration*, la *décomposition* et l'*individualisation* des données.

La première hypothèse de travail<sup>17</sup> étudie ensuite la faisabilité de l'intégration du système d'analyse des relations complexes avec la base de données centralisée préexistante (JANUS PV). Sont abordés ici principalement les aspects juridiques, structurels et organisationnels de la base de données de police centralisée JANUS en fonction au début des années 2000. Il en ressort que des développements devaient être envisagés afin qu'un processus transversal d'analyse puisse y être intégré. De tels développements étaient justement projetés dès 2002.

La seconde hypothèse de travail<sup>18</sup> traite de l'utilité d'un tel système multi-composant. Pour y répondre, trois axes de test sont proposés par rapport au gain global d'information, au gain de temps et au gain de capacité d'analyse.

\* \*

Le troisième chapitre traite de la réalisation de la partie pratique de la recherche. Elle est composée de cinq parties.

La première partie de ce chapitre présente le modèle méthodologique qui a été élaboré pour la mise en pratique de ce projet de recherche. Ce modèle a été façonné par un certain nombre de choix, eux-mêmes basés sur des hypothèses empiriques qu'il n'était ni possible, ni raisonnable de tester dans cette présente recherche, et principalement dictés par des bonnes pratiques rencontrées jusqu'ici. Par exemple, lors du choix entre l'élaboration de plusieurs modèles spécifiques à chaque situation spéciale ou d'un modèle seul générique « réaliste » utilisable dans de très nombreux cas, nous avons préféré la seconde possibilité comme base de départ, afin que le modèle permette de répondre à un maximum de situations, même de manière imparfaite. Ce choix initial influence directement la définition des entités qui seront présentes dans le modèle méthodologique qui sera repris dans les composants du système proposé : bases de données centralisées et d'analyse.

---

<sup>17</sup> Il est possible de coupler aux bases de données centralisées un composant d'analyse externe évolutif qui intègre des systèmes de représentation graphique, dans le but d'analyser les relations complexes de la criminalité organisée.

<sup>18</sup> L'intégration d'un composant d'analyse externe couplé aux bases de données d'enquête centralisées et par conséquent compatible avec la structure des informations qui y sont contenues, est utile à l'investigation dans le cadre de la lutte contre la criminalité organisée.

De même, lorsqu'il s'est agi de choisir le degré de détail (niveau d'agrégation) avec lequel les entités doivent être représentées, notre choix s'est porté vers le niveau d'agrégation le plus faible, permettant l'expression de tous les éléments factuels présents. Là encore, ce choix, évidemment discutable, est guidé par le but visé par notre système, soit la résolution des investigations criminelles, plus particulièrement dans le cadre de la lutte contre la criminalité organisée, alors qu'il serait certainement inadéquat si le but recherché était par exemple de permettre l'étude plus stratégique ou criminologique de ce même contexte.

Cette partie est primordiale, car le modèle méthodologique défini va directement influencer tant le composant centralisé que le composant d'analyse à proprement parler. Les différents types d'entités (éléments ou faits identifiables), la manière de les lier et avec quel degré de détail, y sont décrits et expliqués.

La deuxième partie décrit de manière critique la structure et l'organisation de la nouvelle version de la base de données d'enquête centralisée (JANUS PV 2.0), composant de mémoire à long terme du système proposé, telle qu'elle a été réalisée et mise en service en été 2005.

La troisième partie traite de la base de données d'analyse (*prototype  $\beta$* ), second composant du système proposé, réalisé à l'aide du logiciel *iBase*<sup>TM</sup>. Sa structure et son organisation découlent du modèle générique décrit auparavant et des contraintes liées à la compatibilité nécessaire avec JANUS PV. Les autres fonctions d'analyse prévues par le logiciel *iBase*<sup>TM</sup> et qui font partie de la plus-value analytique du composant sont également présentées dans cette troisième partie.

La quatrième partie du chapitre de la réalisation du projet traite de l'interconnexion des deux composants, des difficultés structurelles et techniques rencontrées et des possibilités futures.

Enfin, la cinquième partie présente quelques expériences pratiques réalisées avec le nouveau composant de base de données centralisé JANUS PV 2.0, puis avec des bases de données d'analyse réalisées avec le modèle structurel et fonctionnel du *prototype  $\beta$*  et enfin ce qui aurait pu être une utilisation des deux composants interconnectés.

\* \*

Le quatrième chapitre de cette recherche, qui est divisé en trois parties, comprend l'évaluation des résultats et une discussion.

La première partie reviendra sur la faisabilité du projet et les problèmes qui ont été rencontrés lors de sa réalisation. Les raisons de l'inachèvement de la réalisation pratique du système tel qu'il a été imaginé dans cette recherche sont décrites.

La deuxième partie discutera de l'efficacité du processus imaginé et qui n'a pu être réalisé qu'en partie durant cette recherche. Le gain d'information, de temps et de capacité d'analyse seront mesurés ou évalués tant au niveau du composant centralisé qu'au niveau de la base de données d'analyse. Puis, des problèmes persistants seront décrits, ainsi que l'identification des problèmes nouveaux qui ont pu ou qui pourraient apparaître consécutivement à la réalisation complète du système.

La dernière partie de la discussion se concentrera sur quelques perspectives actuelles concernant l'analyse criminelle. L'une concerne l'encadrement de l'étape d'analyse à proprement parler. Elle abordera succinctement la problématique des limites de la cognition, et de ses pièges.

Puis, des procédures de production et surtout de test d'hypothèses seront présentées et une méthode originale par l'utilisation d'une « *matrice d'analyse bayésienne d'hypothèses concurrentes* » sera proposée et illustrée.

Enfin, les perspectives liées à l'automatisation des processus qualifiés d'analytiques seront discutées, qu'il s'agisse du cycle du renseignement dans son ensemble ou de l'étape d'analyse prise isolément.

\* \* \*

Enfin, nous nous permettons une mise en garde. Cette thèse touche à plusieurs disciplines que ce soit le droit pénal et sa procédure, la criminologie, l'enquête criminelle, l'informatique, la logique, les sciences cognitives, les questions de modélisation, et bien d'autres encore qui mériteraient toutes d'être traitées plus en profondeur et qui sont des domaines d'études à part entière pour chacune d'entre-elles.

Cette recherche est un projet pluridisciplinaire et voulait dès le départ essayer de proposer un système qu'il aurait été possible de mettre rapidement en pratique dans les structures d'enquêtes actuelles qui traitent de la *criminalité organisée*.

Il est clair que nous ne pouvons qu'effleurer certains sujets qui auraient mérité plus de temps et d'attention aux yeux de chaque spécialiste de l'une ou de l'autre des disciplines abordées. Nous ne cherchons dans cette thèse ni à être exhaustif, ni à prétendre couvrir et maîtriser toutes ces disciplines. Nous n'avons fait qu'y prendre les éléments qui nous semblent utiles à l'étude de cette problématique et à la construction de ce système transversal d'aide aux investigations criminelles dans le cadre de la lutte contre la criminalité organisée.



# 1 Etat des lieux

Ce premier chapitre est destiné à présenter le contexte de cette recherche, qui touche différents domaines qui sont directement concernés par le projet de cette thèse. Ce chapitre doit permettre de dépeindre l'image de la situation actuelle et de disposer des éléments contextuels et méthodologiques qui vont sous-tendre la définition d'un modèle méthodologique qui va servir de base à la réalisation pratique du système d'aide aux investigations criminelles dans le cadre de la lutte contre la criminalité organisée qui est proposé dans cette recherche.

Quatre problématiques importantes à nos yeux doivent être abordées ici : la criminalité organisée, l'enquête criminelle, les bases de données de police et l'analyse criminelle ; sans toutefois avoir la prétention de les traiter complètement, chacune d'elles pouvant être le sujet principal de recherches académiques.

## 1.1 Criminalité organisée

Avant tout, il convient de tenter de définir la notion de *criminalité organisée* plus précisément, tant elle est floue par son emploi fréquent dans divers contextes : policier, juridique, criminologique ou encore journalistique. Est-ce un synonyme de *crime organisé*, ou d'*organisation criminelle* qui figure dans le code pénal suisse ? Ces trois termes se recouvrent, se chevauchent et se mélangent.

S'il y a un point qui rassemble la plupart des auteurs ayant traité de la question, c'est qu'il n'existe pas de définition qui fasse consensus<sup>19</sup>. Un recueil récent en langue française qui est consacré aux « organisations criminelles » est d'ailleurs révélateur. Pour paraphraser ALBANESE<sup>20</sup>, on peut dire qu'il y a quasiment autant de définitions qu'il y a d'auteurs qui adoptent généralement une approche descriptive, MAROTTA<sup>21</sup> s'y exprime ainsi :

« (...) C'est pour cela qu'au delà des caractéristiques communes (...), la criminalité organisée ne peut se laisser enfermer dans une définition statique, mais est à appréhender dans ses transformations qui accompagnent les mutations de la société. En somme, nous devons nous placer dans une optique de *work in progress*, dans une tentative continue de falsification, pour reprendre les mots de Popper, sans prétendre trouver un jour une définition définitive. » (p. 239).

---

<sup>19</sup> Voir entre autres BRODEUR J.-P., Le crime organisé, in MUCHIELLI L., ROBERT PH., Crimes et sécurité. L'État des savoirs, 2002, p.242 ; MORSELLI C., *et al.*, Le crime organisé et les contre-mesures, in CUSSON, DUPONT, LEMIEUX, Traité de sécurité intérieure, 2008, p.185 ; ou encore AUDA G., Le crime organisé, une perception variable, un concept polémique, 2009, pp.16-23

<sup>20</sup> ALBANESE J.S., Organized Crime in America, 1989, p.4

<sup>21</sup> MAROTTA G., Réflexions criminologiques sur le thème de la criminalité organisée, 2009

GISLER<sup>22</sup> identifie trois raisons aux difficultés d'appréhension de cette notion. Il constate des confusions terminologiques, une terminologie imprécise et une difficulté de définition accrue par la nature protéiforme et évolutive du phénomène de la *criminalité organisée* :

« (...) A la lecture des divers ouvrages et études qui y sont spécialement consacrés, trois constatations d'ordre général s'imposent au regard de la définition de ce phénomène criminel.

Première constatation, la notion de « *criminalité organisée* » fait en général l'objet de **confusions terminologiques** au point que son débat est fréquemment marqué par des divergences conceptuelles. En effet, les termes de « *criminalité organisée* », de « *crime organisé* », d'« *organisation criminelle* », de « *mafia* », d'« *association de malfaiteurs* » et bien d'autres encore, sont fréquemment employés indistinctement l'un de l'autre comme synonymes. (...)

Deuxième constatation : la notion de criminalité organisée est liée à une **terminologie imprécise**. Sur le plan étymologique, le concept de criminalité organisée tire son origine littérale de la notion anglo-américaine d'« *organized crime* », expression longtemps traduite en français par « *crime organisé* » et en allemand par « *organisierte Verbrechen* ». Cependant, dans la langue française, le concept de « *crime* » s'entend essentiellement d'un acte criminel, soit un comportement humain individuel punissable, alors que celui de « *criminalité* » fait plus spécifiquement référence à un ensemble de crimes. (...)

Troisième et dernière constatation : la criminalité organisée est une **notion difficile à définir**. Pendant de nombreuses années, il n'existait en effet guère de consensus sur le contenu et la portée de ce concept en raison notamment du caractère obscur et protéiforme de ce phénomène, mais aussi de la disparité des législations nationales censées l'appréhender. (...) » (p. 9-11)

### 1.1.1 Notions (en Suisse)

Nous tenterons toutefois le difficile exercice de synthétiser et de schématiser les quelques définitions qui ont cours dans notre pays et qui sont de nature essentiellement policières et juridiques. Ceci devant nous permettre de définir le champ d'application de cette recherche, soit de la manière dont nous entendons la notion de *criminalité organisée*. Nous reviendrons ensuite sur certaines notions criminologiques issues de la littérature internationale.

---

<sup>22</sup> GISLER F., La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée - *Concepts, état des lieux, évaluation et perspectives*, 2009, p. 9-11. L'auteur applique ensuite une grille d'analyse des définitions existantes basée sur leur origine : policière, criminologique ou juridique, au plan suisse et international. Nous ne pouvons que conseiller au lecteur de s'y référer, celle-ci nous paraissant particulièrement précise et abondamment documentée.

### 1.1.1.1 Crime organisé

Une définition du *crime organisé*, tel qu'il était perçu en Suisse à la fin du siècle dernier, apparaît dans les directives de la mise en application de la protection de l'Etat du 9 septembre 1992<sup>23</sup> :

« *Crime organisé* : Commission méthodique d'actes délictueux, caractérisée par la convoitise du gain ou la recherche de puissance et qui, considérés isolément ou globalement sont d'une lourde gravité; leur préparation et leur réalisation impliquent plus de deux personnes qui agissent en commun pendant une période plus ou moins longue ou indéterminée et qui, pour parvenir à leurs fins :

- a. utilisent des structures professionnelles ou analogues;
- b. recourent à la violence ou à d'autres moyens d'intimidation, ou
- c. s'efforcent d'exercer une influence sur la politique, les médias, l'administration publique, la justice ou l'économie. » (p.151)

Selon GISLER<sup>24</sup>, il s'agit d'une définition policière de la notion de *crime organisé*, elle sera reprise et complétée dans le règlement de traitement JANUS (voir *supra* chapitre 1.3.4). D'autres définitions juridiques se faisaient toutefois simultanément jour, par exemple par le Conseil fédéral, dans le message du 30 juin 1993 concernant la modification du code pénal suisse et du code pénal militaire devant amener l'introduction de l'art 260<sup>ter</sup> sur l'*organisation criminelle*<sup>25</sup> :

« Il y a crime organisé lorsqu'une organisation, dont le fonctionnement est proche de celui d'une entreprise internationale, pratique une division très poussée des tâches, dispose de structures hermétiquement cloisonnées, conçues de façon méthodique et durable et qu'elle s'efforce de réaliser des profits aussi élevés que possible en commettant des infractions et en participant à l'économie légale. Pour ce faire, l'organisation a recours à la violence, à l'intimidation et cherche à exercer son influence sur la politique et l'économie. Elle présente généralement une structure fortement hiérarchisée et dispose de mécanismes efficaces pour imposer ses règles internes. Ses protagonistes sont en outre fortement interchangeables. » (p.273)

Les organisations répondant aux caractéristiques du *crime organisé*, telles que décrites par nos autorités fédérales, s'apparentent donc plus à des multinationales du crime qu'à des PME<sup>26</sup> locales.

La plupart des éléments contenus dans ces définitions juridiques ou policières se retrouvent déjà dans un texte datant de 1973, le Traité entre la Confédération Suisse et les Etats-Unis d'Amérique

<sup>23</sup> FF 1992 VI 150 et Rapport sur la sécurité intérieure 1994

<sup>24</sup> GISLER, *op. cit.*, 2009

<sup>25</sup> FF 1993 III 269

<sup>26</sup> PME : acronyme de Petites et Moyennes Entreprises

sur l'entraide judiciaire en matière pénale du 25 mai 1973 (TEJUS), et plus particulièrement dans les dispositions particulières sur le *crime organisé* :

**« Art. 6 Conditions générales**

(...)

3. Par « groupe de criminels organisés », au sens du présent chapitre, il faut entendre une association ou un groupe de personnes constitué pour une période relativement longue ou indéterminée, afin de se procurer ou de procurer à autrui des revenus ou d'autres avantages financiers ou économiques par des moyens partiellement ou totalement illégaux et de mettre ses activités illicites à l'abri de poursuites pénales, et qui, systématiquement et méthodiquement, cherche à parvenir à ses fins:

- a. En commettant ou en menaçant de commettre, pour une partie de son activité tout au moins, des actes de violence ou d'intimidation punissables dans les deux Etats
- b. Et
  - (1) en s'efforçant d'exercer une influence sur la politique ou l'économie, notamment sur les institutions ou les organisations politiques, les administrations publiques, la justice, les entreprises commerciales, les syndicats patronaux ou ouvriers ou d'autres associations d'employés, ou
  - (2) en se joignant, sous quelque forme que ce soit, à une ou plusieurs associations ou groupes du même genre, dont l'un tout au moins exerce une des activités mentionnées au chiffre 1 ci—dessus. » (p. 6-7)

**1.1.1.2 Criminalité organisée**

La notion de *criminalité organisée* n'a pas spécifiquement définie en Suisse sur le plan juridico-policier. On retrouve une définition d'IINTERPOL qui a été adoptée lors du premier colloque international sur la criminalité organisée qui a eu lieu à Saint-Cloud (France) en mai 1988 :

« Toute association ou tout groupement de personnes se livrant à une activité illicite continue, dont le premier but est de réaliser des profits sans souci des frontières nationales. »

Cette définition cherche par sa concision à fournir un dénominateur commun aux Etats représentés au sein d'Interpol. Le phénomène criminel décrit englobe le *crime organisé* au sens strict tel que défini ci-avant, mais ne s'arrête manifestement pas aux seules multinationales du crime. La pratique nous montre bien que la criminalité – à l'instar de l'économie licite – est avant tout composée d'organisations de plus petite taille, souvent regroupées par origine ethnique ou nationale, formant un tissu criminel complexe et varié, comme le mentionnent RAUFER & QUÉRÉ<sup>27</sup> :

---

<sup>27</sup> RAUFER X., QUÉRÉ S., *Le crime organisé*, 2005

« Mais, d'évidence, la société criminelle est aussi diverse que la société légitime : tout s'y trouve, de l'épicerie de quartier à la multinationale mondialisée. Et l'individu criminel est comme le citoyen honnête : l'un accepte un rang modeste, ou s'y résigne, l'autre est dévoré d'ambition. Or dans la société criminelle, observance de grandes règles et initiative personnelle se conjuguent bien. » (p.13)

Ces mêmes auteurs mentionnent encore l'Union européenne<sup>28</sup>, qui définit le *crime organisé* selon que le groupe visé répond à au moins six des onze critères suivants (les critères 1, 5 et 11 [en gras dans le texte] sont obligatoires) :

- « 1. **collaboration de plus de deux personnes** ;
2. tâches spécifiques attribuées à chacune d'entre elles ;
3. sur une période de temps assez longue ou indéterminée ;
4. avec une forme de discipline et de contrôle ;
5. **dont les membres sont suspectés d'avoir commis des infractions pénales graves** ;
6. agissant au niveau international ;
7. recourant à la violence ou à d'autres moyens d'intimidation ;
8. utilisant des structures commerciales ou de type commercial ;
9. se livrant au blanchiment d'argent ;
10. exerçant une influence sur les milieux politiques, les médias, l'administration publique, le pouvoir judiciaire ou économique ;
11. **agissant pour le profit et/ou pour le pouvoir.**

Ne prenez que les critères 1, 5 et 11 : c'est une bande criminelle structurée. Prenez-les tous et vous avez une mafia. » (p.20)

Le terme de *criminalité organisée*<sup>29</sup> est donc plus général. Il englobe bien sûr les multinationales du crime, mais aussi un tissu fait de criminels qui commettent divers délits qui dépendent de la collaboration de personnes bien précises, mais pour lesquelles la pérennité du groupe dans le temps ne constitue pas un but en soi. Ces auteurs sont souvent condamnés pour la commission de ces divers délits, assortis des circonstances aggravantes du code pénal suisse de commission d'infractions *en bande ou par métier*.

Le schéma suivant résume cette différenciation juridique d'un continuum réel que forme la *criminalité organisée* au sens large.

<sup>28</sup> EUROPOL 161/1994, annexe C.

<sup>29</sup> Bien que défini par l'UE sous le synonyme de *crime organisé*, la notion de *criminalité et de délinquance organisée* a été introduite en 2003 dans le droit pénal français (articles 706-73 et 706-74).

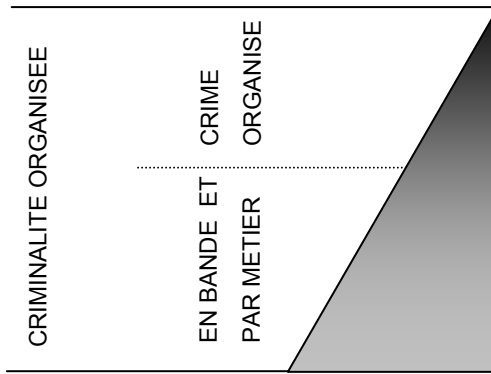


fig. 2 : Continuum criminalité organisée

### 1.1.1.3 Organisation criminelle

L'*organisation criminelle* est, en Suisse, avant tout une notion connotée juridiquement. La Suisse a entrepris, au début des années 1990, les démarches législatives afin de répondre spécifiquement au vide juridique qui devait profiter à des personnages haut-placés, qui semblaient diriger une part importante de la criminalité transnationale. En août 1994, un nouvel article du code pénal suisse (art. 260<sup>ter</sup>) était introduit précisément dans le but de réprimer l'appartenance ou le soutien à une *organisation criminelle*.

#### Art. 260<sup>ter</sup>

1. Celui qui aura participé à une organisation qui tient sa structure et son effectif secrets et qui poursuit le but de commettre des actes de violence criminels ou de se procurer des revenus par des moyens criminels, celui qui aura soutenu une telle organisation dans son activité criminelle, sera puni de la réclusion pour cinq ans au plus ou de l'emprisonnement.
2. Le juge pourra atténuer librement la peine (art. 66) à l'égard de celui qui se sera efforcé d'empêcher la poursuite de l'activité criminelle de l'organisation.
3. Est également punissable celui qui aura commis l'infraction à l'étranger si l'organisation exerce ou doit exercer son activité criminelle en tout ou en partie en Suisse. L'article 3, chiffre 1, 2<sup>e</sup> alinéa, est applicable.

La notion d'*organisation criminelle* n'est, dans sa définition légale, pas restreinte aux seuls membres du *crime organisé* ; mais également à l'ensemble du phénomène de la *criminalité organisée*, pour autant que le groupement tienne sa structure et son effectif secrets et qu'il poursuive des buts criminels.

Le schéma suivant schématise la notion d'*organisation criminelle* qui recouvre l'ensemble de la *criminalité organisée* en passant par tous les degrés d'organisation, du plus simple au plus complexe.

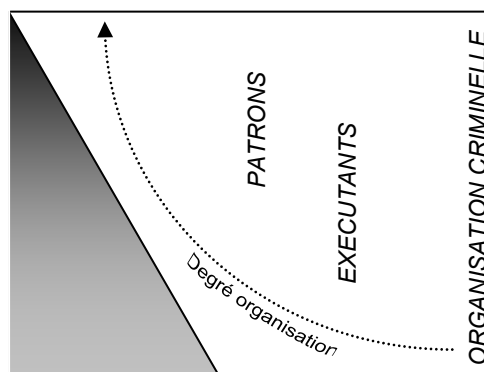


fig. 3 : Continuum des organisations criminelles

Nous verrons toutefois plus loin si cette notion semble plus s'approcher *juridiquement* de la notion plus restrictive de *crime organisé* et s'éloigner des qualifications aggravantes de la commission d'infractions *en bande et par métier*. Ce qui semble être au cœur du débat est la nature existentielle et explicite de l'organisation elle-même. Faut-il que l'organisation soit notoirement reconnue comme criminelle pour que cette disposition légale puisse s'appliquer ?

### 1.1.2 Champ d'application de cette recherche

Les méthodes et les outils proposés dans ce travail s'appliqueront à la recherche et à la gestion des liens d'une *organisation criminelle au sens large*, soit de « toute association ou tout groupement de personnes se livrant à une activité illicite continue, dont le premier but est de réaliser des profits »<sup>30</sup>, sans distinction *a priori* de son degré d'organisation, poursuivie pour des infractions décrites au livre deuxième du code pénal ou de différentes lois fédérales.

Schématiquement, l'ensemble de ces groupements ou *organisations criminelles* constituent la *criminalité organisée* en tant que phénomène criminel, dont le *crime organisé* représente la pointe.

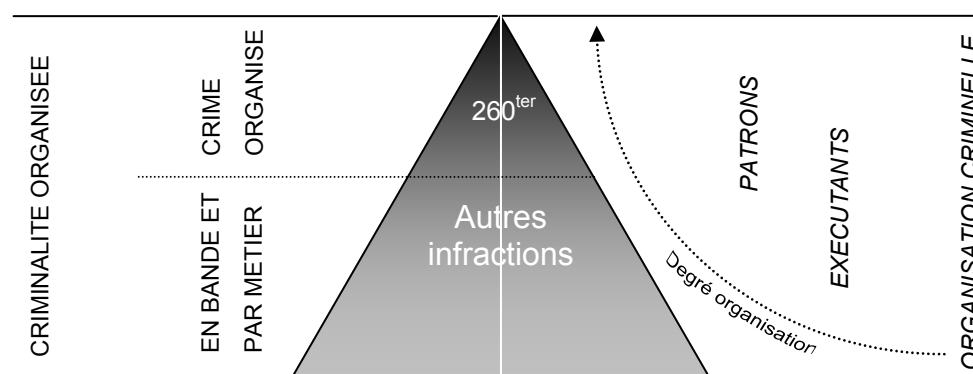


fig. 4 : Criminalité organisée, crime organisé et organisations criminelles

<sup>30</sup> Définition donnée par Interpol en 1998

Les activités déployées par ces délinquants organisés allant du trafic de stupéfiants<sup>31</sup>, au blanchiment d'argent<sup>32</sup> en passant bien sûr par diverses infractions, qu'elles soient contre la vie et l'intégrité corporelle (homicide, agressions, etc.), contre le patrimoine (vol, brigandage, escroqueries, etc.), ou encore contre l'intégrité sexuelle (encouragement à la prostitution, traite d'êtres humains) ou même contre les devoirs de fonction et les devoirs professionnels (corruption active et passive) et comme il se doit en lien avec une organisation criminelle (appartenance ou soutien au sens de l'art 260<sup>ter</sup>).

Le besoin de pouvoir apprécier le degré de participation des différents membres d'*organisations criminelles* plus ou moins structurées est donc indispensable aux autorités pénales, malgré la complexité croissant avec la taille et les moyens de tels organismes.

Le champ d'application de cette thèse dépasse donc une conception juridique afin de pouvoir aborder un phénomène criminel plus large.

### **1.1.3 Caractéristiques de la criminalité organisée**

L'étude criminologique des caractéristiques de la criminalité organisée a alimenté de très nombreuses recherches et constitue sans aucun doute un sujet d'étude à part entière, que nous ne pouvons que survoler.

Relevons que comme dit MAROTTA<sup>33</sup> les multiples études criminologiques sont restées très descriptives ou explicatives, ce qui s'est d'ailleurs ressenti dans les tentatives de définition du phénomène :

« (...) la criminologie a très vite dû admettre qu'elle n'était pas préparée à affronter ce phénomène. La preuve en est que, jusqu'au début des années 1990, les recherches relatives à la criminalité organisée étaient très insuffisantes et la littérature sur ce sujet était le plus souvent l'œuvre de journalistes et, de fait, fruit d'enquêtes journalistiques. Les études socio-criminologiques, qu'elles soient descriptives ou explicatives, n'ont pu proposer qu'une définition de la criminalité codivisible, c'est-à-dire qui n'était pas limitée au niveau spatio-temporel ou au niveau interprétatif. » (p.237)

Nous nous en tiendrons donc ici à aborder succinctement les différentes grilles de lecture qui sont proposées par certains auteurs pour décrire ce phénomène. Nous constaterons que son ampleur et sa nature ont sans doute été à un moment surévaluées et nous reviendrons finalement à la description concrète de certaines caractéristiques constatées par l'auteur dans sa pratique policière dans le canton de Vaud ces dix dernières années.

---

<sup>31</sup> LStup, RS 812.121, Loi fédérale du 3 octobre 1951 sur les stupéfiants et les substances psychotropes

<sup>32</sup> LBA, RS 955.0, Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier

<sup>33</sup> MAROTTA, *op. cit.*, 2009



### 1.1.3.1 Différents paradigmes

Depuis le milieu du XX<sup>e</sup> siècle, la vision que les spécialistes ont eue sur le phénomène a évolué, sans doute aussi bien que la criminalité elle-même.

Comme le rappellent LEMIEUX<sup>34</sup> et KLERKS<sup>35</sup>, le premier de ces paradigmes a été dominant jusque dans les années 1960 – 1970, sans doute en raison de la visibilité du phénomène. Il repose sur un modèle commun du *crime organisé* qui est l'organisation mafieuse hiérarchique. La *mafia traditionnelle* s'est développée dans l'Italie du Sud au XIX<sup>e</sup> siècle. CARTIER-BRESSON<sup>36</sup> décrit le comportement mafioso traditionnel « *par le phénomène de compétition pour l'honneur. Etre un mafioso signifiait alors se faire respecter, être un homme d'honneur, capable de venger avec ses propres forces n'importe quelle offense faite à sa personne, ou à ses proches.* » (p.4).

Contrairement aux systèmes de protection « *Seigneur – vassaux* » du Moyen-âge, il s'agit ici d'un modèle d'ascension sociale « ouvert », chacun pouvant être concurrent. Cette concurrence justifie ses devoirs de protection et de s'imposer par rapport aux autres, créant un système complet de légitimation. Ces activités de protection contre une rétribution étant devenues dans nos démocraties modernes des activités régaliennes, le système de taxation publique parallèle à celui de l'Etat s'apparentait à un racket et constituait le financement de base de la *mafia*.

Le deuxième paradigme, qui reprend les termes de « *nouvelle mafia* » ou de « *mafia contemporaine* », considère que la légitimation de base, qui était traditionnellement la protection de proches et l'honneur a été corrompue par l'argent, et seule la méthode a persisté. « *Le projet d'accumulation du capital devient le projet existentiel du groupe.* » (p.4).<sup>37</sup>

C'est le modèle qui voit dans les organisations criminelles les notions d'échange et de clientélisme. Elles agissent comme des entreprises. Ce deuxième paradigme a fait son apparition depuis les années 1980 et perdure jusqu'à nos jours.

Cependant, la mondialisation du modèle économique peut nous faire penser qu'un nouveau paradigme fait son apparition : les organisations criminelles peuvent être vues comme des réseaux. Selon LEMIEUX<sup>38</sup>, ce modèle ne peut toutefois pas se dissocier complètement du deuxième paradigme. « *Autrement dit, les organisations criminelles se présenteraient comme des entreprises ou des réseaux, selon que l'on s'intéresse principalement aux transactions de ces organisations dans leur environnement externe ou aux liens qui existent dans leur milieu interne.* » (p.3).

---

<sup>34</sup> LEMIEUX, Les réseaux criminels, 2003

<sup>35</sup> KLERKS, The network paradigm applied to criminal organisations, 2001

<sup>36</sup> CARTIER-BRESSON, États, marchés, réseaux et organisations criminelles entrepreneuriales, 1997

<sup>37</sup> CARTIER-BRESSON, *op. cit.*, 1997

<sup>38</sup> LEMIEUX, *op. cit.*, 2003

Ces paradigmes sont nuancés par MORSELLI<sup>39</sup> qui distingue la thèse des *interstices criminogènes*, nécessaire à l'émergence de la criminalité organisée, de celle du *marché criminel* qui se rapproche du second paradigme. Selon lui, ces paradigmes ne sont pas concurrents, puisqu'ils ne tentent pas de répondre aux mêmes questions :

« A l'origine, la thèse selon laquelle le crime organisé s'apparente à une entreprise offrant un bien ou un service sur le marché a été élaborée en réaction à l'image traditionnelle de la mafia, vue comme une organisation bureaucratique. Cette thèse, souvent considérée comme l'antithèse du modèle inspiré de la mafia, ne s'attache cependant pas aux mêmes problèmes. Alors que la thèse des interstices criminogènes vise à expliquer la possibilité que des organisations criminelles émergent et prospèrent du fait des faiblesses gouvernementales, la thèse du marché criminel s'intéresse, elle, à la place que se font les entreprises criminelles dans les secteurs prohibés. » (p.187)

En conclusion, la manière dont on décrit la criminalité organisée dépend finalement beaucoup du référentiel dans lequel l'observateur se place. Un sociologue verra sans doute plus l'aspect relationnel du tissu criminel, alors que l'économiste axera son étude sur l'esprit entrepreneurial du crime. Mais, l'évolution des organisations criminelles tout au long du XX<sup>e</sup> siècle a suivi le développement économique et technologique. Sur ce point, de nombreux spécialistes convergent<sup>40</sup>.

### 1.1.3.2 La superpuissance des organisations criminelles : un mythe qui s'effondre

Avant de poursuivre dans la description de certaines caractéristiques de la *criminalité organisée*, nous tenons à rappeler que cette notion est prise ici au sens large et que le lecteur doit sortir du mythe des « seigneurs du crime » tel qu'il a été perçu et décrit dans les années 1990 et jusqu'à un certain 11 septembre 2001. CHOQUET<sup>41</sup> nous livre une analyse géopolitique assez univoque :

« Il faudra attendre la fin du XX<sup>e</sup> siècle et la mauvaise farce que fit le Pacte de Varsovie à l'Occident en le privant soudain d'ennemi pour que la géopolitique et la stratégie se résolvent à porter leur regard sur les phénomènes criminels. (...)

Les « nouvelles menaces » connurent ainsi leur heure de gloire dans le courant des années 1990, permirent à quelques auteurs de se reconvertir et à quelques services de lutter contre l'érosion budgétaire que d'aucuns qualifiaient de « dividendes de la paix ». Ceux qui avaient aimé la menace rouge et n'avaient pas la patience d'attendre la menace verte trompèrent leur ennui en développant des théories parfois argumentées, parfois séduisantes, mais rarement pertinentes sur l'émergence d'une nouvelle catégorie d'acteurs des relations internationales : les « seigneurs du crime » « les superpuissances du crime » le « directoire mondial du crime » donnaient un peu de substance et d'actualité au mythe

---

<sup>39</sup> MORSELLI, *op. cit.*, 2007

<sup>40</sup> Voir notamment AUDA, *op. cit.*, 2009

<sup>41</sup> CHOQUET Ch., *La Criminalité organisée dans la réflexion géopolitique*, 2009

fascinant du mafieux omnipotent dictant sa loi aux puissants en attendant de devenir maître du monde. (...)

Que reste-t-il aujourd'hui de la « nouvelle menace » du crime organisé ? En réalité, peu de chose. Les phénomènes mafieux, analysés avec rigueur, ont révélé leur véritable nature: une nature essentiellement criminelle, sans doute spécifique dans la mesure où la responsabilité d'un groupe, parfois pérenne, se substitue à celle de l'individu qui jusqu'alors était au centre des systèmes policiers et judiciaires ; mais cette nature est néanmoins distincte de celle des phénomènes nécessitant la mise en œuvre de stratégies militaires. (...)

L'émergence de l'autre « nouvelle menace », à savoir le terrorisme, érigée en priorité absolue dans le domaine de la sécurité internationale après le 11 septembre 2001, donna un coup d'arrêt sévère à la vogue de la menace mafieuse. (...)

La criminalité organisée se trouve donc reléguée, depuis quelques années, au rang des phénomènes de basse police qu'en fin de compte elle n'a jamais cessé d'être. » (p.2)

Nous quittons la géopolitique mondiale et revenons donc aux tâches de *basse police* et allons aborder ensuite quelques composantes qui caractérisent le phénomène criminel au sens large de la (ou des) criminalité(s) organisée(s) et qui rendent la lutte contre les groupements criminels justement difficile et coûteuse en ressources matérielles et humaines.

### 1.1.3.3 Criminalité mobile et itinérante

L'évolution de nos sociétés depuis la seconde moitié du siècle dernier a facilité grandement la mobilité des êtres humains, a accéléré les moyens de transport et de communication et, dans notre environnement direct, a éliminé les frontières entre les Etats membres de l'Union européenne. La chute du mur de Berlin et les conflits armés dans les Balkans et en Afrique occidentale ont provoqué de nouveaux flux migratoires relativement importants vers la Suisse.

Cette évolution a également influencé la criminalité en Suisse et dans le canton de Vaud<sup>42</sup>. Celle-ci perd de plus en plus de son caractère local pour devenir le fait de bandes ou d'organisations œuvrant sur un territoire beaucoup plus vaste que les frontières communales, cantonales et même nationales qui délimitent les compétences de nos autorités de poursuite pénale régies par le principe de la territorialité.

Nos autorités s'exposent donc actuellement d'autant plus au cruel cloisonnement de leurs informations. Ce cloisonnement, connu sous la dénomination anglophone de « *Linkage blindness* »<sup>43</sup>, illustre bien ce phénomène qui consiste en l'incapacité de faire une relation entre

---

<sup>42</sup> Voir entre autres TARONI, La recherche et la gestion des liens dans l'investigation des cambriolages : une étape vers l'exploitation systématique des données de police, 1997 ; et RIBAUUX, La recherche et la gestion des liens dans l'investigation criminelle : le cas particulier du cambriolage, 1997

<sup>43</sup> Littéralement *relation invisible*, voir EGGER, Working Definition of Serial Murder and the Reduction of Linkage Blindness, 1984

deux éléments, ceux-ci étant connus des autorités, mais compartimentés dans des structures organisationnelles, légales, territoriales ou technologiques différentes.

#### **1.1.3.4 Criminalité secrète, qualifiée dans sa forme la plus intégrée de « mafia »**

Comme beaucoup l'ont constaté, la particularité de la criminalité organisée est sa diversité. Elle prend de multiples formes, les structures et les organisations dépendent souvent des coutumes et de l'origine des membres qui la composent. CHOQUET<sup>44</sup> la décrit ainsi :

« Débarrassée des oripeaux dont l'avaient parée des études journalistiques ou pseudo-stratégiques, la criminalité organisée a pu être appréhendée à partir de ses caractéristiques fondamentales : il s'agit d'un phénomène social, d'un mode particulier d'activité criminelle fréquemment pratiqué sur la base de solidarités communautaires, parfois familiales ou claniques, parfois ethniques. Dans ses formes traditionnelles, elle est profondément attachée à un territoire sur lequel elle exerce ce qui a pu être qualifié en Italie de « souveraineté parallèle » ». (p.4)

Cependant, en plus du but économique recherché, le principe du secret semble être un point commun à toutes ces organisations. Il s'agit d'ailleurs d'une réaction de protection naturelle face à tout adversaire représentant un danger. Le fonctionnement qualifié habituellement de « mafieux », se rapporte donc plus aux activités de corruption et de menace ou de racket, qu'à de la dissimulation pure et simple. Ces activités peuvent devenir courantes, mais seulement une fois qu'une organisation criminelle a pris suffisamment d'importance et de confiance dans son environnement sociopolitique immédiat. Les activités logistiques s'efforcent d'être les plus discrètes possibles et tous les moyens de camouflage imaginables sont utilisés à tous les niveaux de l'organisation.

Une fois interpellés, les membres de ces organisations ne sont souvent pas enclins à donner des renseignements<sup>45</sup>, que ce soit par loyauté ou par crainte de représailles importe peu. Cet état de fait oblige les autorités de poursuite pénale à devoir reconstituer discrètement la structure de l'organisation avant de passer à la phase active de l'enquête par des interpellations et des perquisitions. Les liens et relations qui pourront être faits par la suite ne dépendront souvent que de la rigueur des protagonistes dans la dissimulation ou la destruction des traces compromettantes.

#### **1.1.3.5 Criminalité avec un fort pouvoir d'adaptation**

Sans même parler de la *mafia* qui tel le phœnix semble toujours renaître de ses cendres et « *qui est en perpétuelle évolution surtout en ce qui concerne le choix des marchés illicites* »<sup>46</sup>, les professionnels du crime ont un formidable pouvoir d'adaptation, comme le relève encore AUDA<sup>47</sup> :

---

<sup>44</sup> CHOQUET, *op. cit.*, 2009

<sup>45</sup> Qui connaît son paroxysme par la notion bien connue d'*omerta* de la mafia sicilienne.

<sup>46</sup> ANTINORI, L'activité des forces de police dans la lutte contre la criminalité organisée de type mafieux en Italie, 2009, p.71

« Une autre difficulté réside dans le fait que le monde du crime organisé est en mouvement et recouvre un panel d'activités, de comportements individuels extrêmement divers et multiformes. Opportuniste, il sait dénicher de nouveaux secteurs et débouchés. Structuré, il s'adapte aux contraintes que lui oppose la société dans laquelle il évolue. »  
(p.23)

On le remarque d'autant plus avec les nouvelles technologies de l'information et des communications (NTIC)<sup>48</sup>. La criminalité organisée est au fait de toutes les nouveautés et les maîtrise avec une telle rapidité que les lésés et les autorités de poursuite pénale peinent à suivre le rythme imposé<sup>49</sup>. Les nouvelles possibilités offertes par les moyens de paiement sans argent liquide (cartes bancaires ou de crédit) ont par exemple été très rapidement exploitées par des bandes venues principalement de pays voisins de la Suisse. Il en est de même avec les nouveaux systèmes de télécommunication fixes ou mobiles et les escroqueries téléphoniques ou commises par le biais d'Internet, qui créent de nouvelles opportunités criminelles<sup>50</sup>.

#### 1.1.3.6 Caractéristiques récurrentes

Cependant, bien que la criminalité organisée soit protéiforme, mobile, qu'elle évolue et s'adapte rapidement tout en cultivant son secret, les processus plus élémentaires ne changent que très peu. Les *modus operandi* évoluent, mais le fondement de l'acte, soit l'enrichissement illégitime par le vol, la tromperie, l'astuce, le recel, le trafic, ne varie pas. Il s'agit donc pour les autorités de poursuite pénale d'identifier et de démontrer ces processus invariants en focalisant leurs efforts sur ces derniers. Il en est de même dans la structure et l'organisation des bandes ou des organisations de plus grande taille. Afin d'assurer la cohésion de l'ensemble de l'organisme, deux autres fondements sont communs : les relations interpersonnelles et les communications qui en découlent. Celles-ci pouvant nécessiter pour leur interception des moyens sophistiqués ou rudimentaires<sup>51</sup> ! Même si les moyens changent, les auteurs laisseront malgré tout des traces exploitables derrière eux.

---

<sup>47</sup> AUDA, *op. cit.*, 2009

<sup>48</sup> Voir entre autres HERNU, *Le Web et les organisations mafieuses : mythes et réalités*, 2008

<sup>49</sup> RIBAUX, *Comprendre l'influence des NTIC sur l'évolution de la criminalité et des moyens de lutte : un champ d'étude pour les sciences criminelles*, 2005

<sup>50</sup> Voir par exemple un cas de fraude professionnelle à la téléphonie : BERGIER & CARTIER, *Les fraudes GSM: détection et contre-mesures – Collaboration entre les organisations et les instances de justice et police* (Première partie), 2007 ; et CARTIER & BERGIER, *Les fraudes GSM: analyse criminelle et poursuite pénale – Collaboration entre les organisations et les instances de justice et police* (Seconde partie), 2008.

<sup>51</sup> Comme le rappelle CHOQUET, *op. cit.*, 2009 : « *Quant au légendaire et mystérieux Bernardo Provenzano, son successeur au rang de capo dei capi, il vivait dans une cabane de berger et communiquait avec ses collaborateurs en faisant glisser des petits papiers dans les fentes des murs* ». (p.3)

Afin de lutter efficacement contre ce phénomène, il s'agit donc de suivre ces caractéristiques récurrentes, en recherchant l'enrichissement illégal, quel que soit le moyen finalement utilisé, ainsi que les relations qui unissent les membres d'une organisation et leurs moyens de communication, permettant de démontrer ces liens. Les autorités doivent donc s'intéresser tant aux *processus* qu'aux *structures* et à l'*organisation* des criminels, en traitant ce contexte particulier selon une approche systémique pour obtenir une image de l'organisation criminelle. ZINCANI<sup>52</sup>, procureur de Modène en Italie, l'exprime ainsi :

« Élaborer un plan stratégique apte à contrecarrer un phénomène extrêmement complexe diffus et en évolution continue comme le crime organisé, présuppose, d'une part, une profonde connaissance des mécanismes qui sont constamment remis à jour et à travers lesquels il s'articule dans les segments productifs. Et, d'autre part, il requiert une profonde connaissance de sa nature protéiforme, d'où découle une extraordinaire capacité d'adaptation de reproduction et de mimétisme. » (p. 79)

C'est donc par une remise à jour permanente des connaissances disponibles que la lutte peut être efficace que ce soit bien évidemment sur un plan opérationnel, mais également au plan stratégique, ce qui présuppose de mettre en place les moyens de disposer des bonnes informations en temps voulu.

#### **1.1.4 Survol de l'état de la lutte contre la criminalité organisée en Suisse**

Un premier bilan des efforts consentis après une décennie est désormais possible, bien que le recul manque encore, les premières jurisprudences fédérales datant de ces dernières années seulement. Nous verrons, tant au point de vue de la norme pénale que de la procédure, que la lutte contre la *criminalité organisée* a été à ses débuts dans une phase incertaine, tant les normes ont évolué depuis un peu plus de 10 ans. Les problèmes de transfert de compétences entre les cantons et la Confédération, ainsi que l'application de la nouvelle norme pénale ont été au centre de beaucoup de préoccupations. Des difficultés peuvent encore apparaître au niveau des structures de poursuite pénale mises en place et de leur organisation<sup>53</sup>, mais ce point sera abordé dans la partie suivante.

##### **1.1.4.1 Au plan législatif**

Le rapport de situation 2000 de l'Office fédéral de la police<sup>54</sup> nous présente un bilan intermédiaire de la mise en application de l'art. 260<sup>ter</sup> CP et conclut en ces termes :

« ...

1. L'essentiel des mises en accusation ne touchent pas encore les ténors des organisations criminelles, ceux qui s'enrichissent, mais bien plus les exécutants

---

<sup>52</sup> ZINCANI, Les stratégies d'opposition à la criminalité organisée, 2009

<sup>53</sup> Cette problématique est abordée en détail dans le Rapport Uster, « La poursuite pénale au niveau fédéral », 2006.

<sup>54</sup> Rapport de situation 2000, SAP, Office fédéral de la police

dont la participation à une organisation criminelle est souvent masquée par la participation à un délit concret.

2. Dans la pratique judiciaire, l'art. 260<sup>ter</sup> CP n'a pas encore été appliqué spécifiquement à des groupements dont la structure organisationnelle exclut la possibilité d'imputer les actes criminels aux différents protagonistes. On se trouve presque toujours en présence d'actes criminels qui peuvent être imputés à une personne bien précise et qui sont de toute manière poursuivis par le code pénal.
3. On ne trouve pratiquement aucune affaire dans la pratique judiciaire dans laquelle les autorités de poursuite pénale et les services de renseignements n'ont été confrontés à des organisations criminelles, sans qu'on se trouve également en présence de délits concrets. Pour l'instant, le travail de police judiciaire traditionnel appliqué aux affaires individuelles n'a encore que rarement été combiné aux méthodes d'analyse criminelle – ces dernières consistent à réunir des données criminelles dans un cadre plus large et, en utilisant des procédés propres aux services de renseignements, à mettre au jour des relations entre des délits sans lien apparent, pour finalement aboutir aux personnes qui tirent les ficelles – ou, si tel a été le cas, cette association de méthodes n'a pas permis jusqu'ici de fournir des preuves utilisables devant les tribunaux. » (p.81)

Que ressort-il de ce constat de demi-échec ? La mise en application de l'art. 260<sup>ter</sup> CP semble poser un problème au système judiciaire.

Cet article avait pour but, aux yeux du législateur, de pouvoir poursuivre pénalement les patrons, qui ne commettent pas eux-mêmes les infractions, mais qui en vivent. Or, pour que cet article soit appliqué dans ce cas de figure, il faut prouver qu'il y a eu participation ou tout du moins soutien à une organisation qui poursuit des buts criminels. Il s'agit d'être en mesure de remonter – ou redescendre – niveau par niveau la hiérarchie de l'organisation, ce qui est extrêmement difficile lorsque l'on désire s'attaquer justement à des multinationales du crime, qui peuvent, par exemple, influencer sur la justice du pays où les actes criminels violents sont commis.

La pratique nous montrait que jusqu'au 31 décembre 2000, sur 63 affaires pénales visant l'art. 260<sup>ter</sup> CP, 48 avaient débouché sur des acquittements. Dans seulement 4 cas, cet article ne portait pas sur des activités de participation et de soutien à d'autres délits. La moitié des acquittements (24) était due à la subsidiarité de l'art. 260<sup>ter</sup>, lorsqu'il s'agissait d'infractions à la loi sur les stupéfiants, où la personne agissait en tant que membre d'une bande (art. 19, ch. 2, let. b, LStup), ou de délits de blanchiment d'argent, où la personne agissait en tant que membre d'une organisation criminelle (art. 305<sup>bis</sup>, ch. 2., let. a, CP) . Il n'y avait concours réel entre l'art. 260<sup>ter</sup> et les dispositions

concernant les délits précis que lorsque la participation ou le soutien dépassait le cadre de ces infractions précises ; l'un et l'autre article pouvaient alors s'appliquer<sup>55</sup>.

Pourquoi alors les instances d'instruction utilisent-elles quand même cet article, dont l'application est dans la moitié des cas utilisée à titre subsidiaire et n'apporte en définitive pas de condamnation à des peines plus longues ? La raison pourrait se trouver à l'art 59 al. 3 CP :

**Art. 59**

(...)

3. Le juge prononcera la confiscation de toutes les valeurs sur lesquelles une organisation criminelle exerce un pouvoir de disposition. Les valeurs appartenant à une personne qui a participé ou apporté son soutien à une organisation criminelle (art. 260<sup>ter</sup>) sont présumées soumises, jusqu'à preuve du contraire, au pouvoir de disposition de l'organisation.

L'application de cet article permet de renverser le fardeau de la preuve. Les magistrats instructeurs sont alors en mesure de s'attaquer non seulement aux criminels personnellement, mais surtout au produit de leur activité illicite par la confiscation des biens sur lesquels une organisation criminelle a un pouvoir de disposition. La tâche incombant désormais aux suspects de prouver l'origine licite des fonds bloqués.

Ce principe de combattre le crime en confisquant les profits est décrit en détail par CASSANI<sup>56</sup>. Il faut rappeler toutefois qu'une condamnation au sens de l'art 260<sup>ter</sup> CP est une condition nécessaire à son utilisation. En 2004, un jugement en cassation vaudois avait confirmé le renversement du fardeau de la preuve. Cependant, le Tribunal Fédéral<sup>57</sup> a cassé cette décision en février 2005, et a renvoyé la cause pour un nouveau jugement. Cet arrêt rappelle que pour pouvoir invoquer l'art. 59 CP, il faut que le bénéficiaire des fonds soit préalablement condamné au sens de l'art 260<sup>ter</sup> CP. Or, dans ce cas vaudois, seule une mesure de confiscation au sens de l'art 59 CP avait été prononcée par le Juge d'instruction, l'appartenance à une organisation criminelle de deux des bénéficiaires des fonds étant principalement basée sur le témoignage sous le couvert de l'anonymat d'un commissaire de la police fédérale.

L'application de l'art 260<sup>ter</sup> semble poser bien des problèmes. On est en droit de se poser la question si les autorités de poursuite pénale sont capables de manière récurrente d'apporter les éléments de preuve ou si cet article est en adéquation avec la réalité du tissu criminel suisse.

---

<sup>55</sup> Message du 30 juin 1993, FF 1993 III ; et ATF 6S.229/2005, *op. cit.*

<sup>56</sup> CASSANI, Combattre le crime en confisquant les profits: Nouvelles perspectives d'une justice transnationale, 1999

<sup>57</sup> Arrêt du 7 février 2005, Cour de cassation pénale. Réf : 6P.142/2004 et 6S.389/2004/rod



Dans une contribution sur l'échec de l'application de l'art 260<sup>ter</sup>, DE VRIES REILINGH<sup>58</sup>, conclut en proposant la création d'une nouvelle norme pénale permettant de lutter contre les PME du crime qui semblent actuellement échapper à des condamnations au sens de la participation ou du soutien à une organisation criminelle, ce dernier article semblant être réservé aux multinationales du crime. Le continuum de la criminalité organisée présenté à la figure 4 est en effet segmenté, en droit, par des circonstances aggravantes qui ne s'appliquent qu'à certaines infractions, et le 260<sup>ter</sup> qui sanctionne le niveau supérieur des organisations criminelles. La catégorie intermédiaire n'est pas touchée par une norme collective idoine.

« Une solution pourrait résider dans l'incrimination autonome de la constitution de bande (à l'image de ce qu'ont fait nos voisins autrichiens et liechtensteinois), ou encore dans la création d'une infraction intermédiaire entre l'organisation criminelle et la circonstance aggravante de la bande, soit une sorte de catégorie hybride inspirée de la «bande organisée» déjà entrée dans le langage courant. Cet emploi linguistique d'une notion qui n'existe pas encore en droit mais qui qualifie les faits prouve, si besoin était, que le temps presse. » (p. 315)

Dans une autre publication qui traite aussi de la question, AUGSBURGER et PERRIN<sup>59</sup> concluent dans ces termes :

« Les moyens importants dont s'est dotée la Confédération pour lutter contre le crime international organisé ne doivent cependant pas masquer les problèmes d'application de l'art. 260<sup>ter</sup> CP. Cette disposition rend finalement surtout des services dans le cadre des procédures internationales d'entraide et d'extradition. Elle est également utile pour la discussion politique et pour justifier les mesures policières prises, en particulier les bases de données mises sur pied.

Les craintes exprimées par une grande majorité de la doctrine quant aux effets d'une application extensive de cette norme et par conséquent du non-respect de principes fondamentaux, comme le principe de la légalité ou celui de la présomption d'innocence, sont à ce jour infondées, tant les tribunaux sont restrictifs dans l'application de l'art. 260<sup>ter</sup> CP qui reste confinée aux organisations de type mafieux ou terroristes. L'application correcte de la présomption d'innocence conduit en effet souvent à écarter l'application de l'art. 260<sup>ter</sup> CP au profit d'une incrimination moins grave comme la constitution d'une bande.

Avec J. DE VRIES REILINGH, nous constatons que l'élaboration d'une nouvelle catégorie d'infractions serait nécessaire pour appréhender juridiquement une réalité qui existe dans les faits. On peut penser par exemple à l'incrimination autonome de la constitution d'une bande, «soit une catégorie hybride inspirée de la «bande organisée» déjà entrée dans le

<sup>58</sup> DE VRIES REILINGH, La répression des infractions collectives et les problèmes liés à l'application de l'article 260<sup>ter</sup>CP relatif à l'organisation criminelle, notamment du point de vue de la présomption d'innocence, 2002

<sup>59</sup> AUGSBURGER-BUCHELI et PERRIN, Les règles de fond sur la lutte contre le crime organisé, 2006

langage courant». Une autre possibilité consisterait à reformuler l'art. 260<sup>ter</sup> CP en s'inspirant des définitions policières. » (p.267)

#### 1.1.4.2 Au plan de la procédure

Le 1<sup>er</sup> janvier 2002, le nouvel article 340<sup>bis</sup> CP<sup>60</sup> est entré en vigueur. Il redéfinit les compétences de poursuite du crime organisé, du financement du terrorisme<sup>61</sup> et de la criminalité économique, en attribuant de nouvelles compétences à la Confédération aux conditions suivantes :

##### **Art. 340<sup>bis</sup>**

1. Sont également soumis à la juridiction fédérale les infractions aux art. 260<sup>ter</sup>, 260<sup>quinquies</sup>, 305<sup>bis</sup>, 305<sup>ter</sup> et 322<sup>ter</sup> à 322<sup>septies</sup> ainsi que les crimes qui sont le fait d'une organisation criminelle au sens de l'art. 260<sup>ter</sup>:
  - a. si les actes punissables ont été commis pour une part prépondérante à l'étranger;
  - b. si les actes punissables ont été commis dans plusieurs cantons sans qu'il y ait de prédominance évidente dans l'un d'entre eux.
2. Pour les crimes prévus aux deuxième et onzième titres, le ministère public de la Confédération peut ouvrir une procédure d'investigation:
  - a. si les conditions prévues à l'al. 1 sont réalisées;
  - b. et si aucune autorité cantonale de poursuite pénale n'est saisie de l'affaire ou que l'autorité cantonale de poursuite pénale compétente sollicite du ministère public de la Confédération la reprise de la procédure.
3. L'ouverture de la procédure d'investigation prévue à l'al. 2 fonde la compétence fédérale.

Dans le même temps, l'Office Fédéral de la Police (OFP), subissait une nouvelle mue, afin de se donner les moyens d'absorber le travail engendré par ces nouvelles compétences. Le projet « ProjEff »<sup>62</sup>, adopté en 1999 par les Chambres fédérales, devait permettre de grossir les rangs de plusieurs centaines de collaborateurs.

Les années 2002 à 2004 furent naturellement assez floues sur la manière d'appliquer ce nouvel article du code pénal. Les autorités de poursuite pénale cantonales envoyaient les dossiers pour détermination au Ministère Public de la Confédération (MPC) lorsqu'elles devaient ouvrir des enquêtes liées à l'art 260<sup>ter</sup>, notamment. Le temps nécessaire aux déterminations freinait

---

<sup>60</sup> Cette disposition se trouve aujourd'hui à l'art. 337 CP depuis la révision du 1<sup>er</sup> juin 2007. Nous conservons ici l'ancienne numérotation plus rependue dans la littérature

<sup>61</sup> Nouvelle teneur selon le ch. I 1 de la LF du 21 mars 2003 (Financement du terrorisme), en vigueur depuis le 1er oct. 2003 (RO 2003 3043 3047; FF 2002 5014)

<sup>62</sup> Ou communément nommé « f4 », phonétiquement à l'anglaise « effort »

malheureusement les enquêtes de police et les rendaient même parfois tactiquement caduques par manque de célérité<sup>63</sup>.

Ce d'autant plus que le *crime organisé* n'était enfin plus considéré uniquement focalisé sur les organisations multinationales de type mafieux, mais aussi sur d'autres formes de criminalité organisée. Ce revirement est déjà sensible dans le rapport 2002 sur la sécurité intérieure de la Suisse<sup>64</sup> :

**« Hier: focalisation sur les organisations mafieuses**

La définition et l'ampleur du crime organisé en Suisse ont fait l'objet de débats publics en 2002, notamment au lendemain de la publication des résultats du Programme national de recherche 40 (PNR 40) «Violence au quotidien et crime organisé». Dans l'opinion publique, le crime organisé est généralement assimilé aux activités mafieuses. Les experts en revanche s'accordent à dire que les organisations dont la structure est calquée sur celle de la mafia ne représentent qu'une partie du phénomène. Le crime organisé axé sur le profit va des réseaux de malfaiteurs organisés professionnellement aux groupes criminels apparentés dont la structure est très hiérarchisée.

**Aujourd'hui: nouvelle compréhension du phénomène**

La définition du crime organisé met l'accent soit sur les structures d'un groupe criminel considéré comme organisé, soit sur les actes ou les séries d'actes commis de manière organisée. En l'état actuel des connaissances, postulons que le crime organisé revêt des formes de criminalité transnationales particulièrement complexes. A cet égard, de petits groupes fonctionnant comme des entreprises modernes, mais au demeurant très cloisonnés, concluent des alliances à court ou long terme et commettent des actes criminels en se répartissant le travail phase par phase, avec un grand professionnalisme, dans le but d'en retirer un gain aussi élevé que possible. Parmi les domaines caractéristiques du crime organisé figurent le trafic de drogue, le trafic de migrants et la traite d'êtres humains, le trafic d'armes et le trafic de cigarettes. Vu sous cet angle, le crime organisé demeure, en Suisse également, un problème qui doit être pris au sérieux et ne doit en aucun cas être minimisé. Si une grande partie de cette criminalité est organisée, elle ne repose pas systématiquement sur des organisations au sens strict de l'art. 260<sup>ter</sup> CP. » (p.54)

Ce changement de conception de la part de la Confédération semblait reconnaître le rôle des autorités cantonales dans la lutte contre la criminalité organisée. Les cantons ne pouvaient que ressentir un certain dépit face à un transfert de compétence incohérent en regard du tissu criminel présent et visiblement difficile à mettre en œuvre dans la pratique.

<sup>63</sup> Comme ce fut le cas pour une affaire de Nigerian Connection, voir à ce sujet SCHIFFER, CARTIER *et al.*, 2004

<sup>64</sup> Rapport sur la sécurité intérieure 2002, FEDPOL.CH

Plus tard, la chambre d'accusation du Tribunal Fédéral faisait quelque peu le point sur l'application du 340<sup>bis</sup> dans une affaire de blanchiment d'argent (305<sup>bis</sup>)<sup>65</sup>. Elle concluait en ces termes :

« ...

1. La question de savoir si l'une ou l'autre des infractions visées à l'art. 340<sup>bis</sup> al 1 CP a été commise « pour une part prépondérante à l'étranger » doit être résolue en termes qualitatifs et non quantitatifs ou comptables.
2. S'agissant plus particulièrement de l'infraction de blanchiment d'argent, ce sont les actes punissables au regard de l'art. 305<sup>bis</sup> CP – et non pas ceux qui relèvent du crime précurseur – qui entrent en considération pour cette appréciation. » (p. 378)

Le partage des tâches semblait alors être plus clair et les autorités cantonales pensaient retrouver une certaine sérénité.

Enfin, un arrêt du tribunal fédéral<sup>66</sup> sur ces questions de compétences a conclu que le tribunal appelé à statuer ne pouvait remettre en question les accords passés entre le MPC et une autorité cantonale de justice, quant au for, que lorsque l'accord constituait un abus de la liberté d'appréciation.

Cet arrêt permet désormais une application assez pragmatique de cette norme, mais il ne supprime pas les délais nécessaires à l'établissement du for par les autorités cantonales et fédérales, chaque nouveau cas devant systématiquement passer par le MPC pour détermination, avec des conséquences opérationnelles parfois fâcheuses.

### 1.1.5 Synthèse

La politique criminelle de la fin du XXe siècle a été fortement marquée, parfois avec excès, par le « nouveau risque » que pouvait représenter la *criminalité organisée* et plus spécifiquement le *crime organisé*, entendu comme *mafia*, véritable « multinationale du crime ». La difficulté à produire une définition qui fasse consensus que se soit sur les plans juridique, policier ou criminologique, en est le meilleur reflet.

S'il s'est avéré que cette menace a été largement surévaluée, au sortir d'une période de guerre froide, la prise de conscience aura au moins eu le mérite de modifier les paysages juridico-policiers de nombreux pays. En Suisse, de nouvelles normes pénales ont été édictées et de nouvelles règles de procédures sont apparues dans le but de centraliser la lutte contre le crime organisé au sein d'autorités de poursuite fédérales. Des crédits ont été accordés par les autorités politiques pour se donner les moyens de répondre à cette nouvelle menace. Des changements se sont donc produits au niveau de la politique criminelle, des moyens économiques disponibles, des cadres légaux et de la procédure. Malheureusement, l'application de ces nouvelles règles ne s'est pas faite sans difficultés. Des problèmes spécifiques au niveau de la loi et de la procédure sont rapidement apparus.

---

<sup>65</sup> ATF 130 IV 68

<sup>66</sup> ATF 132 IV 89

Par exemple, lorsqu'un des membres « supérieurs » du crime organisé a été personnellement visé, on a buté sur d'énormes difficultés pratiques à rassembler suffisamment de preuves, sur le manque de ressources nécessaires aux autorités de poursuite pénale et sur l'insuffisance de la coopération policière et judiciaire intercantonale ou avec l'étranger. Des succès n'ont même que rarement été enregistrés lorsqu'on s'en est seulement tenu au produit du crime. Mais, il ne faut pas se focaliser uniquement sur le contenu de ces nouvelles normes. Elles ne sont pas la seule cause de certaines déconvenues.

La représentation des *organisations criminelles* qui avait cours dans les années 1990 a ainsi pu évoluer et elles sont désormais et à nouveau considérées comme le définissait Interpol en 1988, soit des associations ou groupements de personnes se livrant à une activité illicite continue, dont le premier but est de réaliser des profits sans souci des frontières nationales. Ce tissu criminel constituant un phénomène au sens large : la *criminalité organisée*.

On constate que la lutte contre la *criminalité organisée* est difficile, tant ce phénomène criminel est complexe, par sa nature protéiforme, mobile, évolutive, et le flou qui entoure sa perception par les nombreux acteurs qui y participent. Elle nécessite une approche différente qui déroge à différents principes que ce soit sur le plan légal ou policier, comme le relève CHOQUET<sup>67</sup> :

« La reconnaissance d'organisations criminelles communautaires est en effet difficile à concilier avec l'un des piliers des systèmes judiciaires occidentaux qui est la responsabilité individuelle. Pourtant, elle ne la remet pas en cause car il n'y a pas substitution de responsabilité : l'existence de l'organisation ne constitue pas une cause d'atténuation de la responsabilité de ses membres. A l'inverse, c'est dans la plupart des droits nationaux un motif d'aggravation des peines, voire d'une infraction *sui generis*. En revanche, la reconnaissance d'entités criminelles distinctes de leurs membres remet en question la méthode inductive traditionnellement utilisée dans l'enquête judiciaire, qui part de la constatation d'un fait pour parvenir à l'identification d'un auteur.

L'observation continue des phénomènes terroristes et mafieux reposant sur une base communautaire justifie donc une analyse stratégique réactualisée en permanence et l'utilisation optimisée des renseignements disponibles sur l'organisation et ses structures, ses objectifs et ses activités. » (pp. 269-270)

Si des modifications au niveau du code pénal suisse n'apportent pas les résultats escomptés, différentes lois qui régissent notamment les systèmes d'information de l'Office Fédéral de la Police ont permis des développements très intéressants, comme les parties suivantes vont le démontrer. Ceux-ci s'inscrivent parfaitement dans ce que CHOQUET préconise, soit l'utilisation optimale des renseignements disponibles dans le but de pouvoir conduire une analyse constamment réactualisée

---

<sup>67</sup> CHOQUET, Terrorisme et criminalité organisée, 2003

des structures et des activités des organisations criminelles. Ce processus de renseignement criminel s'inscrit très exactement dans le concept présenté dans cette recherche.

La partie suivante décrit donc plus en détail l'enquête criminelle, ses principes et son déroulement, ainsi que les structures en place depuis longtemps à un niveau cantonal et ce qui a été récemment mis en place au niveau fédéral pour mener à bien la nouvelle politique criminelle.

Plus loin, de plus amples détails seront donnés sur ce que sont les bases de données, outils incontournables au XXI<sup>e</sup> siècle et particulièrement sur les bases de données de police. Puis, la partie suivante traitera de l'analyse criminelle, méthode de travail apparue justement dans les années 1960 aux Etats-Unis d'Amérique en réponse à ce type de criminalité.

## 1.2 L'enquête criminelle

S'il est un sujet que chacun d'entre-nous croît connaître, tant il fait l'objet de nombreuses fictions, romans policiers ou thrillers cinématographiques, c'est bien l'enquête criminelle. Toutefois, la littérature scientifique souffre de cette situation et ne s'attache que rarement à l'activité d'enquêter. Par exemple, BRODEUR<sup>68</sup> constate, que, souvent, les ouvrages de référence « *se penchent sur tout le processus qui prend en charge un suspect et qui le conduit de façon ultime devant le tribunal : [alors que] les enquêteurs n'ont qu'une part restreinte à ce processus* ». Le contexte particulier dans lequel se déroule l'enquête prend souvent plus d'importance que la discussion et la description de l'activité d'enquêter, activité essentiellement régaliennne qui assigne à la police la mission de *sauvegarder la sécurité, la tranquillité, la santé et la moralité publiques, à préserver d'un danger ou à l'écarter*<sup>69</sup>. BRODEUR classe par ailleurs les écrits portant sur l'enquête policière en cinq catégories<sup>70</sup> selon l'éclairage contextuel qui a été choisi par l'auteur de l'étude.

Comme le marin qui observe un iceberg, les auteurs discutent souvent de l'enquête criminelle par sa partie visible, sa finalité qui est le jugement, alors qu'elle est un enchaînement de tâches qui se doit *de constater les infractions, d'en rassembler les preuves et d'en rechercher les auteurs pour les livrer à la justice, afin de permettre aux autorités compétentes de les poursuivre et de les juger*<sup>71</sup>.

Que ce soit dans les manuels, les revues de techniques spécialisées, certaines monographies, les études d'évaluation et en particulier les études du processus judiciaire, la majorité de ces ouvrages sont influencés par la seule étape du processus qui est vraiment publique et qui déterminera ou non la « réussite » d'une enquête : le procès et la condamnation de l'accusé<sup>72</sup>.

Ainsi, la description de l'activité effectuée par les enquêteurs, qu'ils soient policiers, magistrats, analystes ou experts, est souvent noyée dans la description de l'ensemble du processus judiciaire, dans la discussion de l'application des règles de procédure pouvant pourvoir, par exemple, à la

---

<sup>68</sup> BRODEUR, L'enquête criminelle, 2008. Voir aussi à ce sujet LEVY, Du suspect au coupable : le travail de la police judiciaire, 1987 (p.541).

<sup>69</sup> P.ex. ATF 116 (1990) Ia 355 ss (356)

<sup>70</sup> « 1. Les manuels destinés à la formation des enquêteurs, où la police scientifique occupe une part prépondérante ; 2. Les techniques spécialisées qui sont des manuels portant sur l'étude d'une technique d'enquête déterminée ; 3. Les monographies sur l'enquête qui portent sur l'enquête judiciaire en général ou qui prennent pour objet un type spécialisé d'enquête ou d'enquêteur et qui sont de nature plus universitaire ; 4. Les études du processus judiciaire qui insistent particulièrement sur la description de la séquence des étapes que parcourt un suspect avant de passer en jugement ; 5. Les études d'évaluation qui ont pour but de mesurer l'efficacité de l'enquête criminelle. » Extraits de BRODEUR, *op.cit.*, 2008, p. 542

<sup>71</sup> P. ex. PIQUEREZ, Traité de procédure pénale, 2006

<sup>72</sup> Entre autre : PRÉVOST, Enquête criminelle, 2000 ou LUSHBAUCH & WESTON, Criminal Investigation – Basic Perspectives, 2009

nullité de la preuve et de la multitude des auxiliaires et techniques spécialisées qui ont apparu dès le début du XX<sup>e</sup> siècle avec les sciences forensiques.

On se demande bien finalement ce que fait réellement l'enquêteur lorsqu'il enquête. Est-il un « travailleur du savoir »<sup>73</sup> ? BRODEUR en doute. Selon lui « *l'enquête s'éloigne de la production d'un savoir pour se rapprocher du transfert des connaissances, le policier étant celui qui est en situation passive d'apprentissage par rapport à ses sources d'informations* » et « *l'enquêteur est surtout investi dans la préparation et la structuration de la preuve qui doit être présentée au tribunal* », cette démarche est plus « *caractéristique d'une quête d'information ou d'enseignement typique de la démarche d'un journaliste ou d'un élève plutôt qu'un parcours scientifique.* » (p.556)

On peut comprendre le scepticisme de BRODEUR. En effet, ses constatations se basent sur un travail empirique de plusieurs années dans les archives d'un grand corps de police québécois. Or, il n'y a rien d'étonnant à retrouver dans les archives uniquement ce qui va être nécessaire à la poursuite du processus judiciaire, principalement démontrer la culpabilité d'un prévenu, et qui est transmis au magistrat. L'activité d'enquêter qui a été réellement déployée par l'enquêteur lors de la première phase de l'investigation n'est nullement évoquée de manière explicite et exhaustive dans les rapports de police. Seuls les éléments factuels utiles à la structuration de la preuve qui doit en finalité être présentée au juge y sont effectivement mentionnés. Il fait d'ailleurs lui-même le constat de l'absence d'éléments qui, selon lui, devraient faire partie intégrante de l'action d'enquête, alors qu'ils ont certainement joué un rôle, sans être mentionnés textuellement : « *Je remarquerai en outre que l'expertise scientifique, le renseignement criminel et la consultation des banques de données, qui correspondent de plus près à la conception qu'on se fait du savoir, ne jouent qu'un rôle marginal dans l'élucidation des affaires* » (p.555).

On constate donc qu'à part des manuels monographiques ou spécifiques la plupart du temps destinés à des pairs afin de leur transmettre les meilleures pratiques déterminées en général empiriquement, l'enquête de police reste obscure, même aux yeux des spécialistes. La faute en revient toutefois entièrement à la police et à sa culture traditionnellement discrète, surtout sur ses propres méthodes de travail, d'ailleurs malheureusement rarement explicitées et reconnues comme telles.

Ainsi, comme le dit BRODEUR<sup>74</sup> en conclusion, cette thèse du policier comme travailleur du savoir doit faire l'objet d'une élaboration beaucoup plus explicite pour s'appliquer de façon féconde à l'activité de la police. Et c'est ce que nous allons nous efforcer de faire dans ce chapitre en revenant

---

<sup>73</sup> BRODEUR, *op. cit.*, 2008, p. 555, attribue à HABERMAS le concept de policier comme « travailleur du savoir ». HABERMAS Jürg (1929 - ) est un philosophe et sociologue allemand.

<sup>74</sup> BRODEUR, *op.cit.*, 2008, p.556



aux notions de base, en explicitant le déroulement et les phases de l'enquête avant de décrire succinctement l'organisation du système de poursuite pénale suisse.

### 1.2.1 Retour aux notions de base

L'*enquête*<sup>75</sup> de police reste donc dans l'imagerie populaire et pour nombre de spécialistes une activité basée sur la récolte d'informations auprès de personnes, témoins d'un acte punissable ou ayant connaissance de faits répréhensibles.

Aujourd'hui, bien que cette vision reste vraie et extrêmement valable, pour certains cas où la police agit en réaction lorsque des crimes sont commis et découverts, on parle désormais aussi volontiers d'*investigation*<sup>76</sup> policière, ce terme est moins axé sur les *témoignages de personnes* que le précédent, et il met en valeur la systématique de la recherche.

Nous préférons donc aujourd'hui le terme d'*investigation criminelle*. Celui-ci plus général permet de prendre en compte toutes les activités « annexes » qui font désormais partie des instructions judiciaires, telles que les constatations scientifiques, les contrôles techniques, les expertises techniques, économiques, ou encore médico-légales, etc.

### 1.2.2 Les principes

La notion d'*enquête* ou d'*investigation criminelle*<sup>77</sup> étant décrite, il est encore nécessaire d'en définir le but et certains principes fondamentaux qui régissent toute activité de ce type dans le contexte policier.

#### 1.2.2.1 Le but de l'enquête

Il faut relever que les auteurs du début du XX<sup>e</sup> siècle, à l'instar de GROSS<sup>78</sup>, relèvent que chaque enquête a pour but de reconstruire la réalité sur des éléments passés ou présents en étant aussi près que possible de la vérité :

« Criminal investigation is a lawful search for people and things useful reconstructing an illegal act or omission and analysis of the mental state accompanying it. It is a probing from the known to the unknown, backward in time. The objective of criminal investigation is to determine truth as far as it can be discovered in any inquiry. Successful investigations are based on fidelity, accuracy, and sincerity in lawfully searching for the facts, and on equal faithfulness, exactness and probity in reporting the results. » (p.4)

<sup>75</sup> **Enquête**, *enquête* déb XIIIe ; lat pop *inquaesita*, class. *Inquista*. 1. Mesure d'instruction permettant au juge de recevoir des tiers des déclarations de nature à l'éclairer sur des faits litigieux dont ils ont personnellement connaissance. 2. Recherche méthodique reposant notamment sur des questions et des témoignages. (Le Robert, 1994)

<sup>76</sup> **Investigation**, XIVe ; lat. *investigatio*. Recherche suivie, systématique sur quelque objet. (Le Robert, 1994)

<sup>77</sup> Nous utiliserons désormais ces deux notions comme synonymes, malgré la différence sémantique énoncée ci-dessus.

<sup>78</sup> GROSS, *Criminal Investigation. A practical Textbook for Magistrates, Police Officers and Lawers*, Jackson's fifth edition of 1962, cité dans LUSHBAUCH & WESTON, *op. cit.*, 2009

Mais, la reconstruction d'une situation n'est qu'une représentation, un modèle de ce qui a été ou de ce qui est. Il est illusoire de vouloir reconstruire la réalité matérielle dans son ensemble et dans sa complexité. Il faut donc modéliser (et par conséquent simplifier) la réalité pour en former une qui se doit de tendre vers la *vérité*<sup>79</sup>. Cette connaissance qui se doit conforme au réel, se base sur des *faits*<sup>80</sup>.

Or, ces faits, éléments intimes de l'enquête, doivent être vérifiables ou, pour le moins, leur qualité doit être mesurable, afin qu'ils puissent être appréciés à leur juste valeur. Les faits connus deviennent alors dans l'enquête des *indices*<sup>81</sup>. Par exemple, on parle de trace indiciare pour un élément matériel tel qu'une trace digitale retrouvée sur le lieu d'un délit ou sur un objet, d'un témoignage sur le déroulement d'un événement criminel, ou encore d'un faisceau d'indices pour une série d'éléments factuels concordants et soutenant une hypothèse.

Toujours dans le vocabulaire judiciaire, lorsque des indices permettent l'établissement de la vérité, on parle de *preuves*<sup>82</sup>. Les preuves sont principalement des faits vérifiables, si possible irréfutables et dont certains sont à défaut quantifiables<sup>83</sup>. Ces faits permettent de fixer certains éléments de sa représentation de la réalité et d'en démontrer par un raisonnement les éléments qui les entourent ou qui en découlent.

L'investigation criminelle reconstruit donc un modèle de la réalité aussi fidèle que possible. Celui-ci sera repris et confronté aux arguments des parties au procès à l'issue duquel la *vérité judiciaire*<sup>84</sup> sera établie par le ou les juges, par un processus décisionnel. La vérité judiciaire est donc une vérité fabriquée, construite, ou plutôt reconstruite. Elle ne peut et ne doit pas naître de l'imagination de l'un ou l'autre des acteurs, mais doit avoir des fondements solides.

---

<sup>79</sup> **Vérité**, XIIe ; a remplacé la forme francisée *verté*, *vertet* ; lat. *veritas*, de *verus* « vrai ». Connaissance conforme au réel ; son expression ; les faits qui lui correspondent en tant qu'ils sont exprimés, connus ou à connaître. (Le Robert, 1994)

<sup>80</sup> **Fait**, XIIe ; lat. *factum* de *facere* « faire ». 1. Ce qui est arrivé, ce qui a eu lieu. 2. Ce qui existe réellement, ce qui est du domaine du réel. (Le Robert, 1994)

<sup>81</sup> **Indice**, 1488 ; *endice* XIIe ; lat. *indicium* de *index*. 1. Signe apparent qui indique avec probabilité. 2. DR. Fait connu qui sert à constituer la preuve par présomption, début de preuve. (Le Robert, 1994)

<sup>82</sup> **Preuve**, v.1200 « témoin » ; *prouve* 1175 ; de *prouver*. Ce qui sert à établir qu'une chose est vraie. (Le Robert, 1994)

<sup>83</sup> Par exemple, dans le domaine forensique, la quantification de la valeur probante peut se calculer par un « *Likelihood Ratio* ». Voir chapitre 4.3 – Perspectives pour l'analyse criminelle opérationnelle

<sup>84</sup> Cette *vérité* fait bien entendu l'objet d'un questionnement légitime. Voir notamment FLÜCKIGER, La preuve juridique à l'épreuve du principe de précaution, 2003 et KERCHOVE (VAN DE), La vérité judiciaire: quelle vérité, rien que la vérité, toute la vérité?, 2000

### 1.2.2.2 Les dimensions de l'enquête

Comme le préconisait déjà un vers de QUINTILIEN<sup>85</sup>, resté célèbre, qui résume à lui seul la démarche de toute instruction criminelle : *Quis, quid, ubi, quibus auxiliis, cur, quomodo, quando*, toute reconstruction de la réalité se doit de pouvoir répondre à ces questions, soit :

- Qui ?
- Quoi ?
- Où ?
- Avec quels moyens ?
- Comment ?
- Pourquoi ?
- Quand ?

Ces questions s'articulent selon trois dimensions principales : Les éléments matériels (personnes et choses), le temps et les lieux.

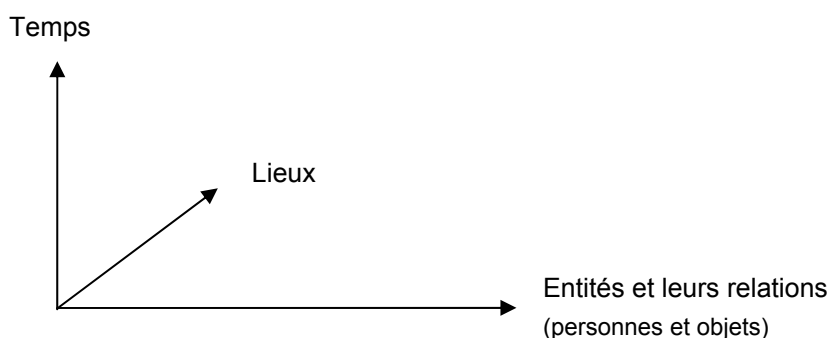


fig. 5 : Modèle universel des trois dimensions d'une enquête

Le « pourquoi » (le mobile) est une question importante et qui est souvent la clé qui mène aux réponses aux autres questions.

### 1.2.2.3 La méthodologie de l'enquête

Les grands criminalistes du début du XX<sup>e</sup> siècle ont été parmi les premiers à formaliser la méthodologie de l'enquête, principalement dans le but de faire bonne place à l'indice matériel, art en plein essor. Ainsi, LOCARD<sup>86</sup> l'exprime ainsi :

« Mais pour n'être qu'un art, la technique de l'enquête criminelle n'en comporte pas moins une méthode, comme les sciences sur quoi elle se base. Et c'est des méthodes de ces sciences que participera celle de l'art qui en découle. (...) Et c'est donc à la méthodologie des sciences naturelles et des sciences physiques que la police technique

<sup>85</sup> QUINTILIEN (en latin *Marcus Fabius Quintilianus*) est un rhéteur et pédagogue latin du I<sup>er</sup> siècle apr. J.-C.

<sup>86</sup> LOCARD E., *L'enquête criminelle et les méthodes scientifiques*, 1933

emprunte les temps de son processus : observation, hypothèse, expérimentation, raisonnement.

**I. Observation.** – L'observation, premier temps de la méthode des sciences physiques comme des sciences naturelles, est représentée ici par les constatations faites sur les lieux. (...)

**II. Hypothèse.** – L'imagination, qui joue dans la méthode même des mathématiques un rôle essentiel, ne saurait être exclue de l'enquête criminelle. Bien au contraire, la hardiesse des hypothèses est un des signes à quoi l'on reconnaît l'excellence du policier. (...)

**III. Expérimentation.** – Prise dans le sens le plus large, l'expérimentation consiste à rechercher si telle cause admise par l'hypothèse est réellement capable de produire tel effet constaté par l'observation. (...)

**IV. Raisonnement.** – Chaque groupe de sciences a son mode propre de raisonnement : les mathématiques ont la déduction, les sciences physiques l'induction, les sciences naturelles l'analogie. (...) Dans la réalité, et qu'il s'agisse d'arithmétique, de géométrie ou d'infinitésimales, il en est tout autrement, parce que les sciences exactes utilisent encore une toute autre façon de raisonner qui est l'induction mathématique, c'est-à-dire le raisonnement par construction suivi du raisonnement par récurrence. (...) D'un mot, le policier idéal serait celui qui construit et imagine un système par l'induction, puis le contrôle par le syllogisme pour aboutir à l'équation finale de l'analyse : inculpé = coupable. » (p. 237 à 256)

LOCARD jetait alors les prémisses d'une méthodologie d'enquête basée sur un modèle inspiré de la démarche scientifique et du raisonnement hypothéticodéductif, basé sur l'abduction, qu'il mentionne sous le nom de *l'induction mathématique*. Cette méthodologie est également reprise par l'analyse criminelle, dans son processus de production de renseignement, mais cette fois de manière beaucoup plus explicite<sup>87</sup>.

### 1.2.3 Le contexte

La plupart des activités de la Justice et par conséquent de la police judiciaire sont réactives. Il s'agit d'un système répressif qui vise à identifier et à punir ceux qui, pour diverses raisons, enfreignent les règles que la société s'est fixées pour son bon fonctionnement communautaire.

Chronologiquement, bien qu'il se passe sauf exception en premier l'acte réprimé par la loi, il n'y a pas toujours l'ouverture d'une enquête judiciaire sur le plan de la procédure<sup>88</sup>. Ce qui permet aux

---

<sup>87</sup> Voir chapitre 1.4.5.2 – Les raisonnements

<sup>88</sup> Voir plus loin la distinction entre « l'enquête préliminaire » et « l'enquête ouverte ». Formellement, l'opportunité de poursuite, qui est une prérogative des magistrats, et la qualification pénale de l'infraction sont rédhitoires à l'ouverture d'une enquête.

autorités de poursuite d'enquêter, c'est la connaissance des faits répréhensibles qu'elles peuvent avoir à un moment donné.

Qui sont les personnes qui renseignent traditionnellement la police ou les juges d'instruction ? En premier lieu, les victimes des infractions elles-mêmes, qui demandent réparation du tort subi ; ensuite les témoins des actes punissables. Or, dans les cas où les actes délictueux sont dissimulés et où il n'y a pas de victime directe, il est par conséquent difficile pour les autorités de poursuite d'ouvrir une enquête, à moins qu'elles ne se donnent les moyens de rechercher elles-mêmes ces actes délictueux, de manière proactive.

### 1.2.3.1 L'enquête proactive *versus* réactive

Dans le schéma traditionnel, la commission d'un acte répréhensible provoque, dès sa découverte, l'ouverture d'une enquête, si les infractions sont poursuivies d'office ou après le dépôt d'une plainte, si elle est nécessaire. Les actes d'enquête découlent de son ouverture (auditions de témoins et/ou de prévenus, recherches diverses) et amènent dans le meilleur des cas à l'identification et à la déférence du (ou des) suspect(s) devant le magistrat instructeur.

Enquête réactive (ou classique) :

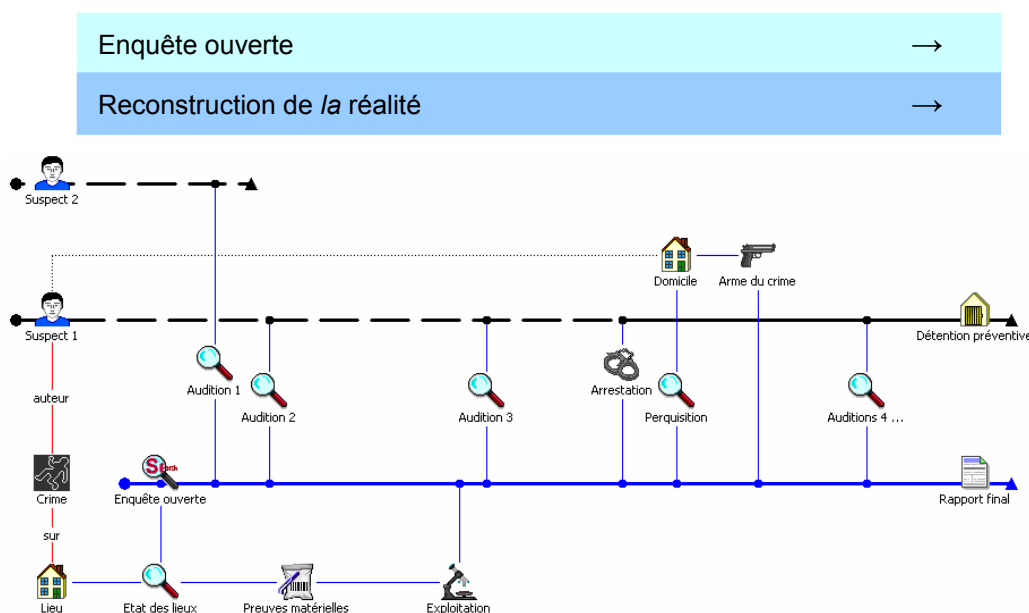


fig. 6 : Représentation du déroulement chronologique d'une enquête classique<sup>89</sup>

Or, nous avons vu que c'est justement une des caractéristiques de la criminalité organisée que de tenir ses activités secrètes. Souvent, qu'il s'agisse de trafics divers, d'escroqueries, de blanchiment,

<sup>89</sup> Cette illustration et la suivante sont faites à l'aide du logiciel *Analyst's Notebook™* de la société *i2 inc.* (voir chapitre sur l'analyse criminelle).

ou même de vols<sup>90</sup>, les auteurs font en sorte de prendre le plus de distance possible avec les victimes réelles des infractions qu'ils commettent, afin de diminuer le risque de mise à jour de leur activité délictueuse régulière et par conséquent de sa poursuite par les autorités compétentes. Ainsi, la vision ordinairement réactive de l'enquête, que l'on peut qualifier aujourd'hui de traditionnelle, n'est plus adaptée à certains phénomènes criminels, comme le relève, par exemple, VAN CAMP<sup>91</sup> :

« Pendant des siècles, tant en Europe qu'ailleurs, les services de police ne vont “ réagir ” qu'en fonction d'infractions commises ou tentées et cela suite à des renseignements, des dénonciations, des plaintes, des constatations et des traces. Ils se focalisaient sur des recherches à l'encontre d'une personne ou de plusieurs délinquants connus ou à identifier. Mais aujourd'hui, de nouveaux types de criminalité apparaissent. Ce sont d'abord les infractions dites “ consensuelles ” dans lesquelles les participants s'accordent entre eux de sorte que la victime n'ira pas dénoncer le délinquant puisqu'elle tire avantage à le fréquenter et est même aussi un délinquant.

Ce sont ensuite les infractions pour lesquelles “ les victimes sont si dépendantes des auteurs qu'elles n'osent pas renseigner la police. Ainsi en est-il des entreprises mafieuses dont les membres utilisent souvent la force d'intimidation, du lien associatif et de la condition d'assujettissement et de la loi du silence qui en dérive, pour commettre des crimes ” ». (p.6)

Ici, il s'agit de répondre à un continuum d'actes répréhensibles<sup>92</sup>, plutôt qu'à un seul acte isolé. La difficulté de l'enquête est d'obtenir les moyens à mettre en œuvre pour recueillir des faits. Ceux-ci devant préférentiellement être obtenus durant l'enquête préliminaire et avant les arrestations et durant les perquisitions. Les auditions n'étant pas toujours très instructives.

Notons au passage que BRODEUR<sup>93</sup> reconnaît ce type d'enquête, qu'il qualifie d'*enquête préventive*, et qu'il réserve aux infractions contre la sécurité de l'Etat. Il accorde que « à cause de sa complexité, elle réclame un traitement indépendant, qui dépasse de beaucoup le cadre de cet

---

<sup>90</sup> Les criminels ont aujourd'hui bien compris qu'il est beaucoup moins risqué de commettre un plus grand nombre de petits délits qu'un seul plus important arrivant au même résultat. On peut prendre l'exemple du vol des cartes bancaires et les retraits subséquents permettant d'obtenir des montants équivalents à l'attaque d'un bureau postal, dont la violence nécessaire et le risque encouru sont comparativement beaucoup plus grands.

<sup>91</sup> VAN CAMP, La lutte contre la criminalité organisée au niveau européen : nouvelles technologies, 2001. Egalement relevé par GISLER, *op.cit.*, 2009

<sup>92</sup> Les nouvelles technologies permettent aussi à des criminels d'automatiser la commission d'infractions en masse sur de tout petits montants, mettant en pratique l'adage *c'est avec de petits ruisseaux que se forment les grandes rivières*. Ces *modus operandi* sont des modèles du genre de la dissimulation et de la dilution des responsabilités de la commission d'infractions.

Cela pose la question de la stratégie qui permet de détecter ces activités. L'analyse des « petits délits » peut amener à comprendre des mécanismes qui relèvent de la criminalité organisée

<sup>93</sup> BRODEUR, *op. cit.*, 2008

article. Nous n'en traiterons donc pas. » (p.547). Il faut pourtant bien admettre que les enquêtes criminelles contre la criminalité organisée ont avantage à utiliser des méthodes proactives, inspirées du renseignement, comme le relève VAN CAMP.

### Enquête proactive (ou d'initiative) :

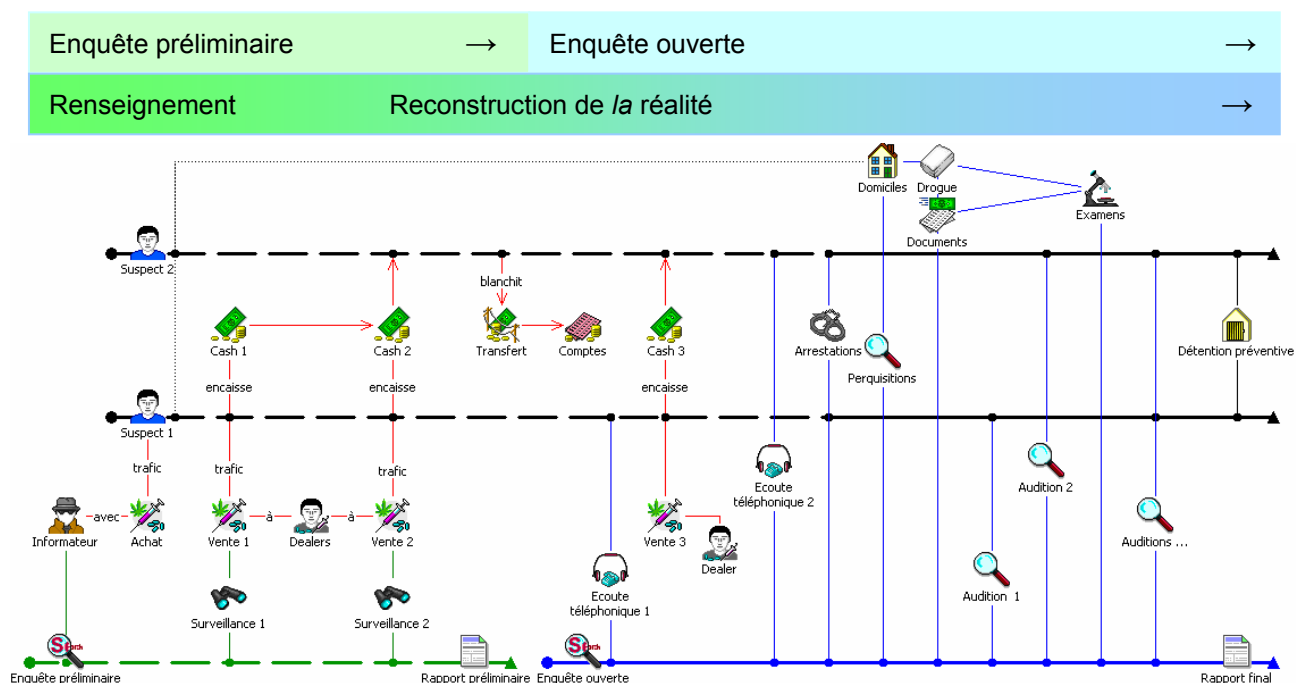


fig. 7 : Représentation du déroulement chronologique d'une enquête d'initiative

## 1.2.4 Les étapes du processus d'enquête

RIBAUX et MARGOT<sup>94</sup> schématisent le déroulement d'une enquête « du suspect au tribunal » en se référant au paradigme de KIND<sup>95</sup> qui voit l'investigation criminelle comme un livre en trois chapitres, que sont : le *problème de trouver*, la *décision d'accuser* et le *problème de prouver* :

« Si on se réfère au paradigme en trois chapitre de Kind (1994) pour expliquer le processus de l'enquête criminelle, le « problème de trouver » consisterait à rassembler toutes les pièces d'information accessibles pour aboutir à la découverte du criminel. Si

<sup>94</sup> RIBAUX & MARGOT, La trace matérielle, vecteur d'information au service du renseignement, 2008

<sup>95</sup> « The investigation of a crime and the consequent criminal trial are best considered, conceptually, as a book of three chapters: The problem to Find, The Decision of Charge and The Problem to Prove. All three chapters contain element of induction and deduction. Induction consists of reasoning from the particular to the general. Deduction consists of reasoning from the general to the particular. However, the first chapter, the investigation requires predominantly inductive reasoning in that it considers how various pieces of evidence combine to point out a particular culprit. The second chapter is something of a hybrid and it represents the fundamental change in mental attitude which is required in the change from a mainly inductive, to a mainly deductive, reasoning approach to evidence. The third chapter, the criminal trial is mainly deductive in character in that it considers each piece of evidence in the light of the hypothesis (i.e. the criminal charge) that a named accused person is guilty of the offence. (...) » (Abstract), KIND, Crime Investigation and the Criminal Trial: A Three Chapter Paradigm of Evidence, 1994.

cette étape aboutit, un suspect est identifié et sous contrôle (éventuellement détenu). Le dossier peut se constituer. Il contiendra les éléments de preuve solides mis en relation avec des infractions bien définies. Au procès, la présentation de ces éléments de preuve contribue à mettre en valeur et discuter la force probante de l'ensemble des éléments du dossier ainsi constitué. Dans beaucoup de situations, le processus de recherche n'est évidemment pas appliqué, car un suspect peut être directement arrêté en flagrant délit ou au cours d'une patrouille de routine.

Chacun des trois chapitres de Kind fait appel à une logique propre. La taxinomie de l'enquête proposée par Brodeur (2005) complète ce modèle en distinguant l'enquête d'identification, de localisation et la structuration de la preuve. » (p. 309-310)

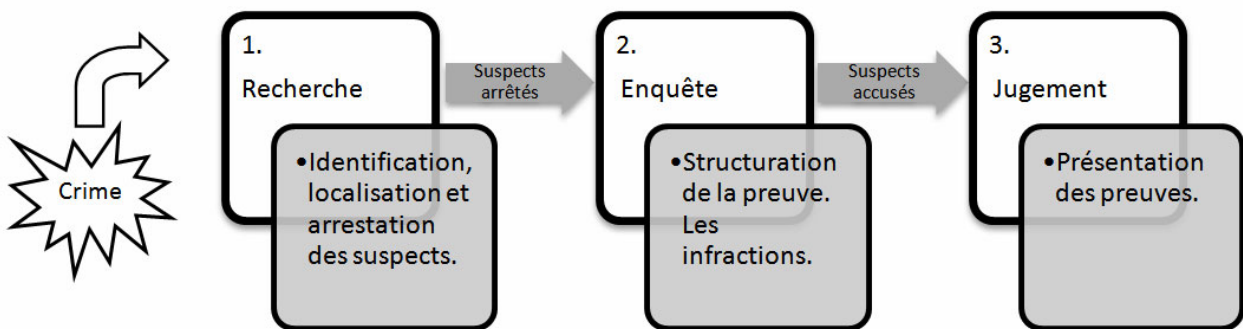


fig. 8 : Schématisation des trois chapitres de l'enquête selon KIND<sup>96</sup>

Ce modèle comporte l'avantage de mettre en évidence que le processus d'enquête passe par une succession d'étapes (les chapitres de KIND) qui sont, sauf exception, nécessaires pour passer à l'étape suivante<sup>97</sup>, mais qui visent des buts différents. L'enquête repose donc sur plusieurs stratégies définies par l'exploitation des informations accessibles à chaque stade et du but recherché : identifier et trouver, ou structurer le dossier (et juger, ce qui n'est plus le rôle de la police). Ce paradigme<sup>98</sup> est universel, car il correspond aussi à ce qui peut se faire dans le cadre des enquêtes proactives, l'événement « crime » devant être ici remplacé par une recherche active ou idéalement par une stratégie de renseignement criminel<sup>99</sup>.

<sup>96</sup> Tiré de RIBAUX & MARGOT, *op.cit.*, 2008

<sup>97</sup> Il n'est par exemple pas absolument nécessaire que le suspect identifié soit arrêté pour que le dossier puisse être constitué, ni même que l'accusé soit jugé.

<sup>98</sup> « I omit in this treatment any consideration of what might be called the “preface” to the three chapters which is the problem of deciding if a crime has been committed. This problem is often more difficult than imagined by those professionally unconnected with crime investigation but it is not part of the enterprise that I wish to deal with here. » (p.156), KIND, *op.cit.*, 1994

<sup>99</sup> Ce sujet sera abordé spécifiquement au chapitre 1.4 – L'analyse criminelle



On comprend peut-être ici mieux pourquoi la lecture des rapports de police ne donne pas l'impression que le policier est un véritable « travailleur du savoir » dans le cadre de la lutte contre la criminalité organisée. Les rapports détaillés ne sont établis que lors de la deuxième étape du processus de l'enquête, dans le but de structurer la preuve. Seuls quelques actes de procédures émanant de la phase de recherche peuvent subsister au dossier, mais ils ne reflètent absolument pas l'activité qui y est déployée. Les stratégies mises en œuvre en vue de l'identification et de la localisation d'un suspect, et *a fortiori* dans le cadre d'enquêtes proactives qui recherchent activement des informations en vue de reconstruire une situation présente, ne sont plus utiles au magistrat. Tout au plus un certain nombre d'indices collectés « collatéralement » durant cette étape seront repris dans le dossier.

#### 1.2.4.1 Les phases de l'enquête proactive

Dans le cadre de la lutte contre la criminalité organisée, on se trouve le plus fréquemment dans des situations où il s'agit dans un premier temps de rechercher activement des crimes ou délits qui sont le fait de délinquants d'habitude inconnus et qui, bien souvent, font partie d'une structure qui les reconnaît socialement. Ces recherches proactives ou *enquêtes d'initiative* (ou *enquêtes préliminaires*) selon les appellations cantonales ou fédérales passe par diverses phases. Chacune de ces phases fait appel au traitement d'informations selon des méthodes structurées.

##### L'enquête préliminaire

Dans ce contexte, l'enquêteur ne dispose pas, en règle générale, de tout l'arsenal des mesures de contraintes et de surveillance du juge d'instruction. Il évolue dans un monde relativement flou et recherche des points d'accrochage qui lui permettent de se focaliser sur un auteur, un événement particulier ou une série de crimes ou délits. Dès lors, il devra recueillir des informations lui permettant de vérifier les soupçons de commission d'actes délictueux et d'en mesurer l'importance. Cette phase est souvent difficile, les moyens à disposition étant réduits, les meilleurs criminels peuvent alors sans doute passer entre les mailles du filet. Dans certaines typologies de criminalité, des structures de renseignement permanentes peuvent être profitables.

Fort de ses constatations, l'enquêteur va lui-même rapporter les faits qu'il a pu récolter et les porter à la connaissance d'un juge d'instruction (ou d'un procureur selon les procédures) qui va pouvoir décider de l'opportunité d'ouvrir une enquête pour les faits rapportés.

##### L'enquête ouverte

Une fois l'enquête ouverte, la police judiciaire agit sous la délégation de l'autorité compétente (juge d'instruction ou procureur). Selon la situation, dans le canton de Vaud, le juge peut délivrer une délégation générale, ou spéciale. Ceci est réglé à l'art 170 CPPV :

**Art. 170.** – La délégation peut être générale ou spéciale. La délégation générale autorise la police judiciaire ou un agent de police judiciaire à procéder dans une affaire, au nom

d'un juge déterminé, à l'ensemble des opérations que la police judiciaire est habilitée à faire par délégation.

La délégation spéciale autorise la police judiciaire ou un agent de police judiciaire à procéder dans une affaire, au nom d'un juge déterminé, à une opération que la police judiciaire est habilitée à faire par délégation.

Il s'agit pour les enquêteurs d'étayer leurs soupçons dans un premier temps. Si le ou les auteur(s) des infractions ne sont pas connus, il va s'agir de les identifier, ou du moins de les « connaître » en vue de leur(s) interpellation(s).

*Les moyens discrets :*

Les moyens à disposition sont cette fois plus conséquents. Comme il est évidemment très difficile et très risqué d'obtenir des témoignages de proches ou de « collaborateurs » des personnes visées avant qu'elles soient arrêtées, il faut agir dans l'ombre afin de ne pas prévenir les personnes ciblées qu'une enquête de police à leur encontre est en cours, avec les conséquences que l'on peut imaginer : collusion, fuite, arrêt des activités répréhensibles et destruction des traces permettant de les confondre.

Les outils de prédilection durant cette phase sont les contrôles par l'intermédiaire des organismes de communication, financiers, et évidemment étatiques (fisc, registres du commerce, fonciers ou de la population, etc.).

Les contrôles téléphoniques<sup>100</sup> sont souvent évoqués, et, bien qu'ils soient notoires, ils apportent encore souvent beaucoup d'éléments aux enquêtes. Toutefois, ceux qui ont déjà été pris et condamnés à cause de ces contrôles deviennent beaucoup plus prudents et compliquent radicalement la vie des autorités, s'ils récidivent.

Une fois que suffisamment de faits et de preuves ont été récoltés, la phase opérationnelle durant laquelle les personnes suspectes seront interpellées et des lieux visités, peut enfin avoir lieu. Il va de soi que si un nouvel événement délictueux en préparation a pu être connu, permettant par là un flagrant-délit, l'opération visera à interpellier les suspects « la main dans le sac ».

Une récente loi fédérale concernant l'investigation secrète<sup>101</sup> régleme le recours à des agents infiltrés ou à des informateurs dans le cadre des enquêtes judiciaires. L'infiltration est désormais soumise à la décision d'un magistrat. Peuvent être désignés agents infiltrés, soit des policiers, soit des personnes engagées à titre provisoire. La provocation de la commission de délits par l'agent infiltré est interdite.

---

<sup>100</sup> RS 780.1 Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

<sup>101</sup> RS 312.8 Loi fédérale du 20 juin 2003 sur l'investigation secrète (LFIS). Voir également FF 2003 4009. Cette loi fera intégralement partie du prochain code de procédure pénale unifiée (CPP) et sera alors abrogée.

### Les opérations

Durant cette phase opérationnelle, le but est d'interpeller les personnes et de préserver les lieux et par conséquent les preuves.

#### *Les interpellations :*

Les personnes suspectes, auteurs ou complices, sont interpellées afin de permettre leur audition par l'autorité compétente (juge d'instruction ou procureur) qui décidera de leur inculpation et le cas échéant de leur arrestation et de leur mise en détention préventive, s'ils remplissent les conditions de dangerosité, de risque de fuite ou de collusion (selon le CPP vaudois – art. 59).

Afin de permettre les interpellations, la police doit connaître le lieu de résidence des personnes suspectes ou leurs déplacements, et pouvoir ainsi procéder à leur « capture physique ».

Le juge d'instruction peut en tout temps durant l'enquête, de son propre chef, décerner des mandats d'amener ou d'arrêt, qui seront exécutés par la police.

#### *Les perquisitions et visites domiciliaires :*

Les perquisitions et les visites domiciliaires (dans les lieux privés) ont pour but de retrouver des personnes, des biens ou des preuves utiles à l'enquête. Dans le cas de la visite domiciliaire, hors cas de péril en la demeure, la police agit avec un mandat du juge.

En cas de découverte d'éléments matériels intéressant l'enquête, les agents de police judiciaire peuvent procéder à la saisie de ceux-ci.

#### *Les séquestres :*

Les objets saisis doivent faire l'objet d'un inventaire qui est signé par leur détenteur et par l'agent de police judiciaire.

Le contenu informatif des saisies est ensuite exploité par la police durant la phase suivante de l'enquête.

### La fin de l'enquête proactive

Dans cette dernière phase, qui doit aboutir à la clôture formelle de l'enquête par l'autorité d'instruction, la police va devoir confronter les éléments désormais en sa possession par le biais de l'enquête préliminaire, par l'instruction à proprement parler et par les opérations qui en ont découlé. Il va s'agir pour l'enquêteur de tester ses hypothèses et sa représentation de la réalité cette fois par le biais d'auditions.

#### *Les auditions :*

Les auteurs, leurs complices, les témoins ou toute personne appelée à fournir des renseignements peuvent être auditionnés.

Ces auditions servent à rechercher, à confirmer, ou à vérifier des éléments obtenus précédemment. La qualité de la source de l'information doit être appréciée avec soin.

Il va sans dire que dans un milieu où la loi du silence est la règle, il ne faut pas souvent s'attendre à des déclarations qui facilitent le travail des enquêteurs. La Suisse ne connaît pas les remises de peine pour les personnes collaborant et permettant d'interpeller d'autres auteurs.

Dans l'actuel système vaudois, la police a accès aux prévenus tout au long de l'enquête, ce qui facilite grandement l'élaboration de stratégies d'auditions. Le système français de *garde à vue* demande une approche totalement différente lors des auditions<sup>102</sup>.

Les auditions peuvent être nombreuses et se succéder à un rythme important. Il s'agira alors aussi de comparer les différentes versions intra ou interpersonnelles. Soit par exemple de détecter si A se contredit lui-même entre ses différentes auditions ou si B et C contredisent A.

*Le rapport :*

Par exemple, dans le canton de Vaud, l'agent de police judiciaire qui a été requis pour exécuter la délégation du juge d'instruction doit lui remettre un rapport, comme cela est demandé à l'art 10 de la loi sur la police cantonale vaudoise :

**Art. 10. (...)**

L'agent requis fait rapport directement au magistrat requérant et adresse sans délai un double de son rapport au chef de la police judiciaire.

Par analogie, le même processus de transmission a lieu dans les autres procédures.

Le rapport sert ensuite à l'autorité compétente pour clôturer l'instruction. Dans le canton de Vaud, le juge rédige une ordonnance de clôture pouvant prendre diverses formes, soit le non-lieu, la condamnation (dans certaines conditions) et le renvoi en tribunal pour jugement. Si des actes d'enquête consécutifs sont encore nécessaires, le juge d'instruction peut délivrer à la police judiciaire une nouvelle délégation.

### **1.2.5 L'organisation du système de poursuite pénale**

Comme le démontre le chapitre précédent, les actes du policier judiciaire sont très clairement réglementés par les codes de procédure. Ceux-ci déterminent également l'organisation du système de poursuite pénale. On peut classer grossièrement deux types de procédures : inquisitoire ou accusatoire, respectivement selon deux modèles : celui du juge d'instruction ou celui du ministère public. Ces modèles dépendent de règles d'organisation décrites par la procédure pénale. Ils n'ont pas d'influence sur le but recherché par l'enquête (reconstruction de la réalité), ni sur son processus général (recherche, enquête, jugement), mais ils définissent précisément (codifient) comment les

---

<sup>102</sup> En effet, les officiers de police judiciaire français ne disposent que du délai de garde à vue, soit de 24h ou 48h avec la prolongation, pour interroger les suspects (des exceptions permettent la garde à vue jusqu'à six jours). Le rythme des auditions est très soutenu et demande une infrastructure très importante lors d'opérations où plusieurs suspects sont interpellés. Une fois que le suspect est formellement inculpé (ou mis en examen) par le juge d'instruction, la police n'a plus accès au prévenu, qui ne peut plus être entendu que par le juge. Elle ne peut donc se déterminer que sur les éléments obtenus durant ce laps de temps très court par rapport au temps que durent les investigations. D'expérience, cette procédure est très frustrante, pour des enquêteurs suisses, face à ces criminels déterminés. Ces derniers ne manquent pas de rappeler au policier qui les interroge qu'ils *tiendront* le temps de la garde à vue, pensant ainsi se soustraire à la Justice.

actes d'enquêtes policières doivent être réalisés, dans le respect de la légalité, de l'intérêt public, de la proportionnalité et de l'opportunité<sup>103</sup>.

Actuellement, nous vivons encore en Suisse, pour quelques dizaines de mois, avec 29 codes de procédure pénale, mais un code de procédure pénale unifiée a été élaboré au niveau fédéral<sup>104</sup>. Suite à la publication du message du Conseil fédéral du 21 décembre 2005<sup>105</sup>, des débats législatifs ont eu lieu et le texte a été adopté par les chambres le 5 octobre 2007. L'entrée en vigueur de la nouvelle procédure unifiée aura lieu, sauf retard, en 2010 dans les cantons et plus rapidement au niveau de la Confédération. En effet, le 21 septembre 2007 déjà, le Conseil fédéral a envoyé en consultation l'avant-projet de loi fédérale sur l'organisation des autorités pénales, et décidait ensuite que les juges d'instruction fédéraux devaient disparaître en 2008 déjà.

### 1.2.5.1 Les différents modèles organisationnels

Les différents modèles présents en Suisse qui ont été étudiés par la commission d'experts en charge de l'étude du concept de procédure pénale unifiée de 1994 à 1998 sont au nombre de quatre<sup>106</sup> :

« - Dans le modèle « **juge d'instruction I** », l'information pénale est dirigée par un juge d'instruction indépendant. La police judiciaire lui est subordonnée, ce qui élimine la séparation entre l'enquête préliminaire et l'instruction. Le ministère public, qui n'a pas le pouvoir de donner des instructions au juge d'instruction, n'intervient dans la procédure préliminaire que comme partie. Lorsque l'instruction est close, le ministère public formule ses réquisitions et soutient l'accusation devant les tribunaux. Selon la commission d'experts, six codes de procédure cantonaux sont rattachés à ce modèle (GL, ZG, FR, SO, VD, VS).

- La commission d'experts a dénombré onze codes de procédure cantonaux relevant du modèle « **juge d'instruction II** » (ZH, BE, LU, SZ, OW, NW, BL, SH, AR, GR, TG). La procédure préliminaire fait intervenir et le juge d'instruction et le ministère public. Toutefois, à la différence du modèle « juge d'instruction I », le premier, n'est pas

<sup>103</sup> Voir au sujet des principes d'intervention de la police, notamment REMY, Droit des mesures policières, 2008.

<sup>104</sup> Début 1998, une commission d'experts instituée en 1994 par le Département fédéral de justice et police (DFJP) publie son concept relatif à une procédure pénale unifiée. Sur cette base, un expert extérieur à l'administration élabore sur mandat du DFJP un avant-projet d'un code de procédure pénale suisse. Le 27 juin 2001, le Conseil fédéral autorise le DFJP à organiser une procédure de consultation relative aux avant-projets d'un code de procédure pénale suisse. Le 2 juillet 2003, le Conseil fédéral prend acte des résultats de la procédure de consultation et charge le DFJP d'élaborer un message relatif à l'unification de la procédure pénale suisse. Le 21 décembre 2005, le Conseil fédéral adopte le message relatif à l'unification de la procédure pénale. Source : communication de l'Office Fédéral de la Justice (OFJ) sur l'unification du droit de la procédure pénale ([www.ofj.admin.ch](http://www.ofj.admin.ch))

<sup>105</sup> FF 2006 1057

<sup>106</sup> Documentation de presse du DFJP relatif à l'avant-projet d'un code de procédure pénale suisse (extraits du rapport explicatif) du 27 juin 2001

indépendant du second ; il est soumis, dans une mesure qui, évidemment, varie considérablement d'un canton à l'autre, au pouvoir d'instruction du ministère public. Dans la majorité des cantons, la mise en accusation et la représentation de l'accusation au tribunal incombe exclusivement au ministère public.

- Le modèle « **ministère public I** », issu du droit français, est caractérisé par la bipartition de la phase préliminaire. Avant même l'intervention du juge d'instruction, la police judiciaire mène l'enquête sous la direction du ministère public. Ce n'est qu'ensuite que ce dernier requiert un juge d'instruction (indépendant) d'ouvrir une instruction préparatoire. Ce système est surtout connu en procédure pénale fédérale mais également dans cinq cantons (UR, AG, NE, GE, JU). Lorsque l'information est close, le juge d'instruction communique le dossier au ministère public qui décide de la mise en accusation ou du classement.

- Le modèle « **ministère public II** » a cours dans quatre cantons (BS, TI, SG, AI) et à l'étranger, sous une forme semblable, en Italie, en Allemagne et dans les pays anglo-saxons. Ce système est caractérisé par l'absence totale de juge d'instruction. Le ministère public conduit l'instruction, prononce la mise en accusation et soutient celle-ci devant les tribunaux. Il dirige habituellement la police judiciaire ou dispose tout au moins à son égard d'un pouvoir d'instruction. » (p 4-5)

Les différents modèles de procédure définissent donc quels sont les organes de poursuite pénale (juge d'instruction, ministère public et la police judiciaire) et quels sont leurs rôles respectifs dans le processus judiciaire, du début de l'enquête jusqu'au jugement. Les droits de la défense (droit de recours, droit d'assistance, etc..) figurent dans le code de procédure selon les systèmes inquisitoires ou accusatoires.

Selon certains modèles, la police judiciaire a plus de liberté de manœuvre, comme c'est le cas dans le canton de Vaud, car elle peut recevoir des délégations de compétence générale de la part d'un juge d'instruction. Dans d'autres cas, les délégations doivent être beaucoup plus précises et concises, ce qui reporte le travail de direction de l'enquête sur les épaules du procureur ou du juge d'instruction.

Certains y voient un gage d'indépendance du système judiciaire, d'autres un manque de confiance dans la police judiciaire. Ce qui est probable, c'est que toutes les restrictions de compétences des exécutants occasionnent un surcroît de travail qui entraîne un surcoût humain et temporel.

Mais, finalement, il faut bien admettre que ces différences n'influencent que partiellement le processus de l'enquête judiciaire qui reste globalement le même. Il faut être toutefois attentif à ce que des règles de procédures trop strictes empêchent *de facto* la police d'être suffisamment efficace dans la première étape, où elle est souvent la plus active, à savoir la recherche de délits, d'auteurs et de leur localisation.

### 1.2.5.2 De l'avant-projet au code de procédure pénale suisse

Il fallait bien constater que les disparités de procédures et par conséquent de l'organisation des systèmes judiciaires cantonaux et fédéraux compliquaient le système judiciaire suisse dans son ensemble. Il fallait donc agir et bien que la commission d'expert ait préféré le système « **juge d'instruction I** », l'Office fédéral de la justice a organisé au printemps 1998 une table ronde avec les représentants des principales institutions concernées, qui a préconisé l'unification intégrale de la procédure en s'inspirant en priorité du modèle « **ministère public II** »<sup>107</sup>. Suite à ce choix, le DFJP a chargé, en mars 1999, Niklaus SCHMID, professeur de droit pénal et de procédure pénale à l'université de Zurich, d'élaborer d'ici le mois de mars 2001 un avant-projet de code de procédure pénale unifiée.

En juin 2001, l'avant-projet était publié et mis en consultation<sup>108</sup>. Les avis obtenus suite à cette procédure au sujet du modèle judiciaire démontrent un clivage entre les cantons romands et alémaniques (à l'exception de GE) dû aux coutumes des modèles utilisés jusqu'ici. Le canton qui déplore que son système de poursuite pénale différencié n'ait pas été pris en compte est Bâle-Campagne, qui applique un système de poursuite d'infractions relevant de la criminalité économique et de la criminalité organisée selon le modèle « ministère public II »; et de poursuite des autres infractions selon le modèle « juge d'instruction » assorti d'une procédure d'instruction en deux temps.

Cet exemple particulier bâlois montre que le système « ministère public II » semble bien approprié à la criminalité organisée, puisqu'il élimine un intervenant dans le processus (le juge d'instruction), ce qui devrait simplifier la procédure, mais il semble beaucoup moins performant pour la petite

---

<sup>107</sup> « Ces auditions ont mis en évidence une approbation unanime de l'unification intégrale de la procédure pénale, c'est-à-dire une solution allant au-delà d'une simple loi cadre. En ce qui concerne le choix du modèle de poursuite pénale, une tendance assez nette s'est dégagée en faveur de la solution du ministère public, telle qu'elle est appliquée à Bâle-Ville par exemple. » (p. 2). Source : Documentation de presse du DFJP relatif à l'avant-projet d'un code de procédure pénale suisse (extraits du rapport explicatif) du 27 juin 2001

<sup>108</sup> « Le modèle "ministère public II" préconisé dans l'avant-projet emporte l'adhésion de 60% des participants, qui sont toutefois 40% à le rejeter. Parmi les cantons, 15 sont pour et 11 contre. Les motifs invoqués par les partisans du modèle "ministère public II" sont variables: si la majorité de ceux-ci se rallie au dit modèle parce qu'il lui semble être la meilleure solution, une minorité opte pour le même modèle considérant qu'il ne serait plus opportun de remettre en cause le modèle proposé dans l'avant-projet, étant donné que les travaux sont déjà bien avancés. Plusieurs participants relèvent que le choix du modèle n'a qu'une importance relative et insistent, en revanche, sur la nécessité de doter l'appareil de poursuites pénales de ressources humaines et de moyens appropriés ou encore de prévoir une procédure s'inspirant largement des principes fondateurs de l'Etat de droit. En sus de leur avis sur le modèle à choisir, certains participants demandent instamment que la police judiciaire ne soit pas subordonnée au ministère public. Un canton déplore que le système de poursuite pénale différencié qu'il applique depuis peu n'ait pas été mis en discussion; il propose que l'on prenne en compte ce système à titre de compromis dans le cadre de l'élaboration du code de procédure pénale suisse. » (p. 20). Source : Synthèse des résultats de la procédure de consultation relative aux avant-projets de code de procédure pénale suisse et de loi fédérale régissant la procédure pénale applicable aux mineurs, Office fédéral de la justice, février 2003.

criminalité ou la criminalité d'occasion puisqu'il alourdit le processus de nombreux droits de la défense pour contrebalancer le rôle accusatoire du procureur.

Le modèle organisationnel retenu dans le code de procédure pénale unifié aura bien évidemment des conséquences sur les organismes qui en dépendent (justice et police) et principalement dans les juridictions qui connaissent encore aujourd'hui le juge d'instruction. Mais, il s'agit d'adaptations structurelles et dans l'organisation et dans la pratique quotidienne, qui devra suivre de nouvelles règles de procédure.

Par exemple, par rapport à l'actuelle procédure vaudoise, la présence de l'avocat lors des auditions, ainsi que l'apport d'éléments écrits auprès du Tribunal des mesures de contraintes par le Ministère public pour une demande de mise en détention provisoire, demanderont aux enquêteurs de travailler avec encore plus de célérité, et de précision afin de pouvoir fournir ces dérivables écrits dans des temps très brefs.

Pour être en mesure de fournir des éléments factuels de qualité dans des délais très courts, il sera sans aucun doute nécessaire de mettre en place une stratégie de renseignement criminel<sup>109</sup> permanente qui permette d'apprécier les éléments recueillis en temps voulu, et, s'il n'est humainement ou techniquement pas possible d'amener des éléments probants (preuves), leurs présomptions devront être suffisamment étayées, pour pouvoir justement retenir un suspect particulièrement intéressant, le temps de réaliser les analyses techniques ou forensiques.

### **1.2.5.3 L'organisation de la police judiciaire**

Que ce soit au plan cantonal ou fédéral, des réglementations déterminent le rôle de la police judiciaire et son organisation. Constitutionnellement la compétence primaire étant dévolue aux cantons et la police judiciaire y affiche une grande stabilité. Comme on l'a vu au chapitre précédent, la criminalité organisée, « nouvelle menace » identifiée dans les années 1990, a débouché en 2002 sur un transfert de compétences du niveau cantonal au niveau fédéral. Ce qui a obligé les instances fédérales à se réorganiser et à créer un système judiciaire à part entière.

L'organisation de la police judiciaire vaudoise et de la nouvelle police judiciaire fédérale sont ici décrite succinctement.

#### La police judiciaire du canton de Vaud :

Dans le canton de Vaud, la police judiciaire est encore régie par le code de procédure pénale vaudoise (CPP – RSV 2.10) et la loi sur la police judiciaire (RSV 2.11). Ces textes datent de 1967 pour le code de procédure et de 1940 pour la loi sur la police judiciaire.

---

<sup>109</sup> Ainsi, l'analyse criminelle opérationnelle, qui, comme on le verra plus en détail au chapitre 1.4, constitue un soutien à l'enquête jouera certainement un rôle plus important qu'actuellement à ce stade de l'enquête et des rapports d'analyse non-démonstratifs devront sans doute être élaborés et standardisés fin de permettre l'évocation d'une suspicion suffisante (forts soupçons) devant permettre la mise en détention provisoire.



Sont faits mention à l'art. 4 du CPP vaudois des compétences d'instruction :

**Art. 4.** – Les juges instructeurs sont chargés d'instruire les enquêtes pénales. Ils comprennent le juge d'instruction cantonal, les substituts du juge d'instruction cantonal et les juges d'instruction.

Ils disposent de la police judiciaire dans les limites de la loi\*.

\*Voir loi du 3.12.1940 sur la police judiciaire (RSV 2.11).

Puis aux articles 164 et 165 du même code, les compétences spécifiques d'enquête :

**Art. 164.** – La police judiciaire est organisée par une loi spéciale. Ses attributions sont fixées par cette loi, le présent code et les instructions générales que le Département de justice et police et le tribunal d'accusation lui donnent d'entente entre eux, après avoir consulté le juge d'instruction cantonal.

**Art. 165.** – La police judiciaire recherche les infractions; elle rassemble les moyens de preuve et prend les mesures indispensables à leur sauvegarde; elle peut notamment ordonner une prise de sang en vue d'expertise, si le prévenu paraît avoir agi sous l'influence de l'alcool.

La police judiciaire agit en collaboration avec le juge; elle est tenue de le renseigner régulièrement et complètement sur toutes ses recherches préliminaires et de lui signaler immédiatement les infractions poursuivables d'office qui parviennent à sa connaissance.

La loi sur la police judiciaire du canton de Vaud de 1940 regroupe en une dizaine d'articles les caractéristiques propres au fonctionnement de la police judiciaire. L'article premier fait référence aux compétences au sens des articles 164 et ss. du code de procédure pénale et les art 2 et 3 aux organes qui exercent la police judiciaire, qui sont :

**Art. 2.** La police judiciaire est exercée:

- a) par la police de sûreté;
- b) par la gendarmerie;
- c) par la police locale dans les cas prévus à l'article suivant.

**Art. 3.** Le Conseil d'Etat peut décider qu'une police locale ou une section de police locale a compétence de police judiciaire.

Le chef du service chargé de la police cantonale peut, pour les besoins d'une enquête en cours, investir une police locale des pouvoirs conférés par la loi à la police judiciaire.

Ce sont donc les organes cantonaux de police, soit la police de sûreté pour une part prépondérante, et la gendarmerie pour les très nombreux cas de moindre ampleur, qui exercent la police judiciaire.

La seule police locale vaudoise qui détient actuellement un corps de police judiciaire est la police municipale de Lausanne.

Bien que des réglages fins aient eu lieu au sein de la police cantonale vaudoise entre la gendarmerie et la police de sûreté pour la prise en charge des délits de peu de gravité par des unités décentralisées de police judiciaire, une spécialisation des membres de la police de sûreté est apparue dans la seconde moitié du siècle dernier.

La nature toujours plus complexe des affaires que la police de sûreté devait traiter notamment au niveau financier a fait naître une brigade spécialisée dans cet environnement. Plus tard vont suivre les brigades des stupéfiants, des mineurs-mœurs, ainsi que des unités spécialisées dans les activités liées à l'établissement des étrangers, les renseignements généraux, la coordination et l'observation judiciaire. Une brigade spécialisée, l'unité judiciaire, demeure pour traiter de manière pointue, les infractions contre le patrimoine et contre l'intégrité corporelle.

Aujourd'hui, on trouve même des divisions spécialisées au sein des différentes brigades, preuve que la lutte contre la criminalité doit se spécialiser encore plus, afin de répondre à l'évolution technique des moyens d'investigation dans des environnements nouveaux ou à la complexification des procédures. Par exemple, la brigade financière est constituée de trois divisions : criminalité économique, criminalité organisée (complexification procédurale) et criminalité informatique (évolution technologique).

Cette spécialisation des agents de police judiciaire n'est pas sans effet dans la lutte contre la criminalité organisée, car bien qu'une division spéciale lui soit dédiée, des barrières organisationnelles et structurelles amènent des blocages dans le partage d'information, par des systèmes informatiques différents, ou simplement par la méconnaissance du travail de son collègue « de l'étage du dessus » et de ses compétences propres.

Ces spécialisations ont donc un impact sur la fluidité de l'information. Elles devront donc être prises en compte dans le développement des méthodes d'analyse criminelle opérationnelle.

#### La police judiciaire fédérale :

Au niveau fédéral, comme on l'a vu dans le chapitre précédent, des aménagements importants ont eu lieu ces quinze dernières années, suivant les démarches qui ont été entreprises dès le début des années 1990.

La réforme la plus spectaculaire a été indubitablement la création de la nouvelle *police judiciaire fédérale* au début des années 2000.

Alors que l'ancienne *police fédérale* - placée sous la direction du Ministère public de la Confédération - enquêtait sur les infractions relatives au terrorisme, aux activités de renseignement prohibées, à l'extrémisme violent, au commerce illicite d'armes et de substances radioactives ainsi

qu'au transfert illégal de technologie ; les investigations des Offices centraux de police criminelle portaient sur les infractions concernant le faux monnayage et le trafic intercantonal ou international de drogues.

La réforme qui définit encore aujourd'hui l'organisation de la police fédérale et qui a eu lieu en 2000 consistait en le regroupement de toutes les compétences fédérales en matière d'enquêtes (investigations préliminaires et enquêtes judiciaires) dans une seule et même unité, la nouvelle Police judiciaire fédérale. La *police judiciaire fédérale* (PJF) et le *service d'analyse et de prévention* (SAP) étaient nés.

Comme le mentionnait le communiqué de presse<sup>110</sup>, certaines contraintes légales qui n'ont pas été modifiées ont créé de nouveaux dédoublements de compétences entre la PJF et le SAP. Cet état de fait provoquera un certain nombre de réactions en 2004. Comme toutes les compétences d'enquêtes étaient regroupées au sein de la PJF, les informations détenues par le SAP (devenu par la suite officiellement le service de renseignement intérieur<sup>111</sup>) ne pouvaient désormais plus être utilisées par des enquêteurs de la PJF. Les renseignements étaient à nouveau séparés par des systèmes informatiques étanches.

La loi sur les Offices centraux de police criminelle<sup>112</sup> de 1994 en vigueur fait référence à la police judiciaire exercée au niveau fédéral. Les articles 1 et 2 sont les suivants :

---

<sup>110</sup> « **Regroupement des compétences en matière d'enquêtes** - La principale décision de la cheffe du DFJP concerne le regroupement de toutes les compétences fédérales en matière d'enquêtes (investigations préliminaires et enquêtes judiciaires) dans une seule et même unité, la nouvelle Police judiciaire fédérale. Dans toutes les catégories d'infractions précitées qui relèvent de la compétence fédérale, il importe, pour que l'efficacité soit maximale, qu'une seule organisation policière conduise les investigations préliminaires et les enquêtes judiciaires.

Les unités du renseignement de la Police fédérale, qui sont rattachées à l'actuel OFP, et les unités des actuels Offices centraux de police criminelle, qui établissent des analyses de la situation dans certaines catégories d'infractions, seront réunies au sein du nouveau Service d'analyse et de prévention (SAP). Tirant ses informations de sources publiques et privées, ce dernier mettra à la disposition du Conseil fédéral, du DFJP et des autorités fédérales et cantonales de poursuite pénale les données nécessaires aux évaluations de la situation. Le SAP apportera aussi son soutien direct à la PJF en fournissant des analyses stratégiques et des rapports de situations.

Pour des raisons légales (LMSI, loi sur les Offices centraux de police criminelle et loi sur la protection des données), il faut que les tâches analytiques liées à la lutte contre le crime organisé, le trafic de stupéfiants et la criminalité économique, d'une part, et les tâches de renseignement concernant le dépistage d'actions terroristes, le service de renseignements prohibé, l'extrémisme violent, le commerce illicite d'armes et de substances radioactives, d'autre part, soient accomplies par des unités distinctes au sein du Service d'analyse et de prévention, s'agissant notamment du traitement de données. Dans les domaines de la criminalité organisée et de la criminalité économique, le SAP établira également des rapports de situation dont les données anonymisées illustreront l'état et/ou l'évolution de la criminalité dans ces secteurs. » Communiqué aux médias du DFJP : Police judiciaire fédérale et Service d'analyse et de prévention, du 3 mai 2000

<sup>111</sup> Voir brochure du secrétariat général du DDPS n°92.400, « Les services de renseignements suisses », Berne 2004

<sup>112</sup> RS 360.0, Loi fédérale du 7 octobre 1994 sur les Offices centraux de police criminelle de la Confédération (LOC)

**Art. 1** Principe

1. La Confédération dirige des offices centraux de lutte contre le crime international organisé.
2. Les offices centraux travaillent en collaboration avec les autorités de poursuite pénale et les services de police des cantons et de l'étranger.

**Art. 2** Tâches

Au sens de la présente loi, les offices centraux:

- a. traitent les informations qui relèvent de leur domaine de compétences, qu'elles émanent de Suisse ou d'un pays étranger;
- b. coordonnent les investigations menées aux échelons intercantonal ou international;
- c. établissent des rapports de situation et dressent un bilan de la menace à l'intention du Département fédéral de justice et police (département) et des autorités de poursuite pénale;
- d. garantissent l'échange national et international des informations de police criminelle et traitent des demandes d'entraide judiciaire émanant de pays étrangers;
- e. détachent des agents de liaison à l'étranger;
- f. mènent des enquêtes de police judiciaire dans les domaines de compétence de la Confédération.

Outre les tâches de coordination voulues au lettres a à e de l'article 2, les offices centraux doivent mener les enquêtes de police judiciaire dans la sphère de compétence de la Confédération.

Or, avec l'élargissement des compétences, une nouvelle ordonnance a été nécessaire afin de réglementer plus précisément l'organisation de la nouvelle police judiciaire fédérale (RS 360.1 de 2001). Celle-ci remplaçait l'ancienne ordonnance sur les offices centraux de police criminelle de 1997. L'article 1 qui définit les tâches de la PJF doit donc faire référence aux offices centraux définis dans la LOC :

**Art. 1** Police judiciaire fédérale au sein de l'Office fédéral de la police

La Police judiciaire fédérale au sein de l'Office fédéral de la police exécute des tâches:

- a. en tant que police judiciaire de la Confédération;
- b. en tant qu'office central de lutte contre le crime organisé selon l'art. 7 LOC;
- c. en tant qu'office central de lutte contre le trafic illicite de stupéfiants selon l'art. 9 LOC et l'art. 29 de la loi fédérale du 3 octobre 1951 sur les stupéfiants et les substances psychotropes (LStup);
- d. en tant qu'office central de lutte contre la fausse monnaie selon l'art. 12 de la Convention internationale du 20 avril 1929 pour la répression du faux monnayage;

- e. en tant qu'office central de lutte contre la traite des blanches selon l'art. 1 de l'Arrangement international du 18 mai 1904 en vue d'assurer une protection efficace contre le trafic criminel connu sous le nom de traite des blanches;
- f. en tant qu'office central de lutte contre la circulation des publications obscènes selon l'art. 1 de l'Arrangement du 4 mai 1910 relatif à la répression de la circulation des publications obscènes.

Les tâches de police judiciaire telles que mentionnées à la lettre a de l'article 1, sont détaillées à l'article 2 :

**Art. 2** Tâches de police judiciaire

- 1 En tant que police judiciaire de la Confédération, la Police judiciaire fédérale mène, en présence d'indices ou d'informations liés à la commission d'une infraction, des procédures d'enquêtes préliminaires et d'enquêtes relevant du domaine de compétences de la Confédération, placées sous la direction du Ministère public de la Confédération.
- 2 Dans le cadre de ses activités de police judiciaire, la Police judiciaire fédérale procède à des analyses opérationnelles qui permettent d'assurer un suivi constant et d'apporter un soutien dans le traitement de cas complexes.
- 3 (...).

Ce texte récent est novateur, il faut le souligner. Le chiffre 2 de cet article 2 fait explicitement référence à l'analyse criminelle (*analyse opérationnelle*) telle que nous le verrons au chapitre suivant.

Enfin, la procédure pénale fédérale (PPF – RS 312.0 de 1934) reconnaissait la qualité de police judiciaire à son article 17 :

**Art. 17**

- 1 La police judiciaire est dirigée par le procureur général; elle est sous la surveillance de la Chambre d'accusation du Tribunal fédéral.
- 2 Elle est exercée:
  - par les ministères publics des cantons;
  - par les fonctionnaires et employés de police de la Confédération et des cantons;
  - par les autres fonctionnaires et employés de la Confédération et des cantons, dans la limite de leurs attributions.
- 3 La police judiciaire de la Confédération collabore, en règle générale, avec les autorités de police compétentes des cantons. Dans chaque cas, elle les informe de ses recherches, dès que le but et l'avancement de la procédure le permettent.
- (...)

Le jeune âge de l'actuelle police judiciaire fédérale fait que ses structures ne sont pas encore aujourd'hui totalement stabilisées. Bien que l'on retrouve une structure empreinte de la spécialisation de la criminalité comme c'est le cas dans les cantons, d'autres critères ont été pris en compte pour l'élaboration de leur structure.

#### *Enquête préliminaire et enquête ouverte*

Une particularité dans l'organisation de départ de la PJF était la spécialisation de groupes d'enquêteurs différents pour les enquêtes préliminaires et les enquêtes ouvertes.<sup>113</sup>

Comme les enquêtes préliminaires se faisaient déjà sous la supervision d'un procureur, des enquêteurs étaient détachés à cette seule tâche de dégrossissage. Une fois le travail effectué, le ministère public pouvait décider d'ouvrir formellement une enquête. Dès lors, c'est une autre équipe d'enquêteurs spécialisés par type de criminalité qui reprenait le flambeau et poursuivait l'enquête. Des commissariats d'enquête avaient été créés spécifiquement pour la criminalité organisée ou pour la criminalité financière. Certains de ces commissariats d'enquête ont été délocalisés depuis le printemps 2004 dans des divisions aux quatre coins du pays, soit Lausanne pour l'ouest, Berne pour le centre, Zurich pour l'est et Lugano pour le sud. Lorsque ces divisions sont suffisamment étoffées, elles reprennent un autre type d'organisation, décrit ci-dessous.

#### *Localisation ou origine géographique des auteurs ou suspects*

Pour répondre aux besoins de coordination décrits à l'art. 1 de la nouvelle ordonnance et aux connaissances sur la nature ethnique des organisations criminelles, de nombreuses divisions sont organisées en commissariats s'occupant spécifiquement de ressortissants de certaines régions du monde, Europe de l'Ouest, Afrique, Proche-Orient, Europe de l'Est, CEI, Extrême-Orient, Amérique du Nord, Amérique du Sud, Amérique Centrale et Caraïbes.

#### *Analyse des nouvelles structures et organisations du MPC et de la PJF*

En 2006, le chef du Département de justice et police demandait une analyse de la situation de la poursuite pénale fédérale et de la suite qu'il fallait donner au « ProjEff ». Le rapport<sup>114</sup> du comité de projet présidé par le Conseiller d'Etat zougais USTER a été rendu en août de la même année. Simultanément, et suite à des critiques répétées contre le Ministère public de la Confédération, dans les médias, M. le Conseiller fédéral BLOCHER avait ordonné une enquête administrative sur le MPC dont il avait chargé M. LÜTHI, avocat. Ce dernier a rendu son rapport<sup>115</sup> au département le 15 septembre 2006.

---

<sup>113</sup> Il faut relever ici que cette particularité est en train de disparaître avec une nouvelle réorganisation en 2007.

<sup>114</sup> USTER, La poursuite pénale au niveau fédéral – analyse de situation et recommandations, Comité de projet « Analyse de situation ProjEff », 31 août 2006

<sup>115</sup> LÜTHI, Enquête administrative au sein du Ministère public de la Confédération, 15 septembre 2006

Il ressort de ces deux rapports qu'aucun dysfonctionnement grave n'a été constaté. Cependant, dans les deux cas, des recommandations ont été faites.

On relèvera notamment, dans le rapport LÜTHI, la problématique de l'implication des procureurs du MPC dans les recherches préliminaires<sup>116</sup>. Ainsi, cette caractéristique particulière de voir des groupes d'enquêteurs différents en charge des enquêtes préliminaires et des enquêtes ouvertes créant des transmissions de dossiers en cours d'investigation devait être corrigée, ainsi que le rôle du procureur qui se voit confier la conduite d'investigations, sans qu'une enquête soit formellement ouverte, ce qui n'est sans doute pas dans les habitudes, tout du moins dans les cantons où la police conduit ces recherches préliminaires et en assume seule la responsabilité.

Sur un autre plan, le rapport USTER « *estime que l'on ne doit rien changer à la primauté de la poursuite pénale par la justice et la police cantonales, conforme à la Constitution. Afin de circonscrire les tâches de chacun et de définir clairement les zones où elles entrent en contact, il propose un catalogue de compétences que l'on pourrait réaliser, pour l'essentiel, sans modifier la*

---

<sup>116</sup> « **Délimitation des responsabilités entre la PJF et le MPC au début des enquêtes** - La police judiciaire, selon le règlement d'organisation de fedpol, est placée sous la conduite du procureur général de la Confédération. Ce dernier dirige les enquêtes. Si des soupçons suffisants portent à penser que des infractions relevant de la juridiction fédérale ont été commises, il ordonne l'ouverture de la procédure d'enquête de police judiciaire. A partir de ce point, les attributions sont claires : le procureur général porte la responsabilité.

Avant l'ouverture de la procédure d'enquête de police judiciaire, les responsabilités ne sont pas claires. Il s'agit du domaine des enquêtes préliminaires et des recherches préliminaires.

L'hypothèse que ces enquêtes préliminaires et recherches préliminaires font partie des enquêtes de police judiciaire, ce qui les place dans le champ de compétence du MPC, est renforcée par les faits suivants :

- le procureur général a édicté une directive à ce sujet;
- le MPC doit décider de l'ouverture formelle d'une procédure d'enquête de police judiciaire et il doit donc être responsable du relevé des faits déterminants qui s'y rapportent;
- le MPC donne des mandats, sur la base de la directive et en pratique, pour de telles enquêtes préliminaires et recherches préliminaires.

En revanche, les éléments suivants étayent l'idée que les enquêtes préliminaires et les recherches préliminaires sont placées sous la seule responsabilité de fedpol :

- la directive prévoit des enquêtes préliminaires et des recherches préliminaires hors mandat du MPC;
- la loi sur les offices centraux prévoit une certaine marge de manœuvre de la police, sans l'étendre toutefois à toutes les infractions fédérales;
- un tel domaine autonome de fedpol existe purement de facto en pratique;
- toutes les données issues de ce domaine de procédure sont stockées dans le système d'information JANUS, qui est placé sous la compétence de la PJF.

La loi fédérale sur la procédure pénale et la loi sur les offices centraux ne réglementent pas clairement ces questions de délimitation. (...)

**Recommandation : il faut clarifier la délimitation des responsabilités entre le MPC et la PJF quant aux enquêtes préliminaires et aux recherches préliminaires, la réglementer légalement et la mettre en œuvre rapidement.** » (p. 35-36 du rapport LÜTHI, *op.cit.*, 2006)

*loi. La poursuite pénale fédérale devrait se concentrer sur les grands cas complexes (...). Il faut renoncer à une révision de la loi, du moins dans un premier temps.»*<sup>117</sup>.

De plus, il recommande, entre autre, « *d'abroger le plus tôt possible l'instruction préparatoire par une modification anticipée de la procédure pénale fédérale et d'affecter au domaine de l'instruction les ressources libérées par l'abrogation de l'Office des juges d'instruction fédéraux* »<sup>118</sup>.

Cette dernière recommandation fait écho à l'actuelle procédure pénale fédérale qui crée des doublons en ajoutant l'instruction préparatoire à l'instruction et l'accusation, alors qu'il s'agit de mandats identiques ou similaires, mais qui sont donnés à la PJF par le MPC et les juges d'instruction fédéraux, les dossiers changeant deux fois de mains.

#### **1.2.5.4 Organisation pratique de l'enquête judiciaire**

Les compétences cantonales ou fédérales étant définies, on a vu quelle autorité devait se charger de l'enquête en fonction des règles légales et de l'organisation du système judiciaire. Mais l'organisation pratique de l'enquête est encore un tout autre sujet.

Les points de repères qui sont donnés au grand public sont issus de romans, films ou autres séries policières. Et bien que la qualité et la vraisemblance soient souvent de mise, l'image qu'ils restituent est très déformée de la réalité sur deux points : les ressources<sup>119</sup> et plus encore le temps nécessaires à l'investigation. Voici donc quelques affirmations sur les ressources réellement nécessaires au traitement de données complexes telles que celles obtenues dans les enquêtes criminelles. Ces ressources portent principalement sur les efforts à consentir pour rendre les données accessibles et traiter ces volumes de données disparates et importants.

##### Une enquête – un enquêteur ?

Dans la plupart des cas, la délégation judiciaire est attribuée à un seul enquêteur.

Celui-ci a la charge de l'enquête telle qu'elle est définie dans la délégation du juge. Si des moyens supplémentaires en personnel ou en moyens dits « spéciaux » sont nécessaires, l'enquêteur doit s'en référer à sa hiérarchie policière pour ce qui est de l'obtention des ressources internes et au juge ou au procureur pour l'obtention de mesures coercitives décidées par le magistrat.

Les enquêtes de grande envergure, dans le domaine de la criminalité organisée, nécessitent très souvent que plusieurs personnes traitent la même affaire. Ceci pour plusieurs raisons : premièrement, la durée de l'enquête et le rythme imposé par des mesures de surveillance telles que des écoutes téléphoniques, font qu'une seule personne ne peut physiquement et psychologiquement

---

<sup>117</sup> USTER, 2006, *op. cit.*, (p. 7)

<sup>118</sup> USTER, 2006, *op. cit.*, (p. 8)

<sup>119</sup> Par exemple, le budget utilisé à l'époque pour la production d'un épisode de la série américaine *Miami Vice* était supérieur au budget annuel de la brigade anti-drogue de Miami.



pas tenir longtemps ; deuxièmement, la masse d'informations accumulées n'est plus assimilable par une seule personne ; troisièmement, les compétences d'un seul homme ne suffisent souvent plus.

C'est pour ces quelques raisons que l'enquêteur désigné devra s'entourer d'un remplaçant, du renfort d'analystes et de spécialistes afin de mener à bien sa mission.

Il en découle qu'une véritable stratégie doit être fixée par l'encadrement policier afin de pouvoir distribuer les ressources de manière adéquate en temps et en nombre.

#### Une mesure discrète – un enquêteur ?

Que ce soit une observation policière, une écoute téléphonique, ou *a fortiori* une infiltration, les ressources nécessaires sont souvent très mal connues du grand public.

Chacun de ces moyens nécessite à lui-seul bien souvent l'engagement d'une dizaine de personnes (policiers et spécialistes) lorsque l'on veut du travail de qualité et qui réponde aux normes juridiques.

A nouveau, l'enquêteur désigné devra demander ces moyens et, s'il les obtient, ce sera pour une durée forcément limitée. Les options stratégiques étant fixées par l'état major, à lui de bien suivre son enquête et de demander les bons moyens au moment opportun.

#### Une opération – un enquêteur ?

Finalement, l'enquête arrivant dans sa phase active et visible de l'extérieur, il s'agira pour l'enquêteur désigné de requérir les moyens nécessaires au bon déroulement des opérations.

Les interpellations d'individus présumés dangereux se faisant aujourd'hui en général par les groupes d'intervention<sup>120</sup> spécialisés. Ce service doit être demandé.

Les visites domiciliaires et les perquisitions nécessitent également le renfort de quelques enquêteurs par lieu visité. Et si des traces ou des éléments matériels particuliers doivent être recherchés, le service d'identification judiciaire, des spécialistes en informatique<sup>121</sup> ou même des experts externes<sup>122</sup> doivent être requis. Cette collecte de données en masse et sur une durée très limitée nécessite également qu'elle soit préparée. Les recherches se doivent d'être ciblées si on ne veut pas devoir gérer un séquestre trop important en volume, et devoir ensuite exploiter de trop nombreuses données futiles. Le tri entre ce qui est utile de ce qui ne l'est pas est un élément clé lors des perquisitions.

Enfin, les premières auditions de prévenus doivent être faites par deux personnes au moins en respect de la procédure actuelle.

---

<sup>120</sup> Chaque corps de police dispose aujourd'hui d'un groupe spécialisé. Par exemple le DARD (Détachement d'Action Rapide et de Dissuasion) est le groupe d'intervention de la police cantonale vaudoise.

<sup>121</sup> La police de sûreté vaudoise dispose d'une division spécialisée dans la criminalité informatique (DCI) qui est responsable de la sauvegarde des traces informatiques.

<sup>122</sup> Par exemple, les gardes-frontière disposent d'un groupe spécialisé dans l'examen des véhicules automobiles (EVA) ; l'IPS de l'Université de Lausanne disposant lui de spécialistes de la détection de traces de stupéfiants.

La phase d'intervention doit donc être soigneusement préparée, la planification temporelle en est difficile, mais primordiale. A cause de l'évolution des événements dans le terrain, une grande disponibilité de toutes les unités requises est nécessaire.

### Une enquête – une langue ?

Enfin, dernier détail, qui n'en est pas un : la langue. Le temps est bien révolu où on pouvait se passer de parler d'autres langues que la sienne.

Les fréquents échanges avec des collègues d'autres régions linguistiques en Suisse ou avec l'étranger nécessitent de disposer de connaissances dans les langues nationales, ainsi que de l'anglais et même de l'espagnol.

Mais, plus encore, il est indispensable de comprendre la langue des suspects. Il est alors nécessaire de faire appel à des interprètes, qu'il faut quasiment inclure à temps plein à l'équipe d'enquête lorsque par exemple le rythme des écoutes téléphoniques est soutenu.

Tout ceci sans compter qu'il est parfois difficile de trouver des interprètes pour des dialectes lorsque ceux-ci sont parlés par de très petites communautés. Dans ces cas de figure, il n'est pas rare de devoir faire appel à des interprètes qui résident à l'étranger, et qui ne parlent pas français. Il est alors encore nécessaire de faire traduire une seconde fois la transcription du premier interprète. Et que dire du risque de collusion avec le recours à un interprète qui parle un dialecte pratiqué par une communauté de deux mille personnes (comme c'est le cas par exemple au Nigéria).

Ce multilinguisme nécessite que cette étape soit aussi formalisée et intégrée au processus de traitement des informations.

## **1.2.6 Synthèse**

L'environnement judiciaire, et plus précisément policier, dans lequel le praticien doit évoluer aujourd'hui est comme on l'a vu réglementé jusque dans ses moindres détails. Le système fédéraliste fait que l'on évolue toujours dans 27 microcosmes judiciaires en Suisse<sup>123</sup>, alors que la criminalité décrite au chapitre précédent ne connaît elle aucune frontière.

La loi se doit de garantir les libertés constitutionnelles. Les organes judiciaires qui ont pour but de les faire respecter de manière répressive, se doivent également de les suivre, ou du moins de ne les transgresser que dans des cas exceptionnels décrits dans les différents codes de procédures et autres lois spécifiques (LSCPT, LFIS). Le praticien du judiciaire, qu'il soit procureur, juge, policier, ou auxiliaire (expert, analyste, spécialiste, etc.) est entièrement lié par ces codes de procédures, ces lois spécifiques et autres ordonnances, qui garantissent la légalité de ses actions.

---

<sup>123</sup> Même si le futur code de procédure pénale unifiera formellement la manière de travailler, les cantons resteront souverains, avec toutes les conséquences qui en découlent : relative étanchéité des systèmes d'information et des procédures à l'instruction, complications multiples dans les affaires dépassant le niveau géographique cantonal.

L'organisation interne des corps de police judiciaire, que ce soit au niveau fédéral ou cantonal, crée, il faut bien l'admettre, encore souvent des blocages au niveau structurel dans la transmission d'informations, sans bien-entendu que ce soit le but recherché.

L'investigation que doit mener le praticien dans ce contexte règlementé a pour but de reconstruire la réalité sur des éléments passés ou présents en étant aussi près que possible de la vérité. Pour cela, il dispose de moyens traditionnellement basés sur le témoignage. Le découpage du processus d'enquête en trois étapes reprises de KIND et qui ont été mises en relation avec la taxinomie de BRODEUR par RIBAUX et MARGOT<sup>124</sup> nous semble particulièrement intéressant puisqu'il sépare des activités qui ne visent pas le même but, qui, par conséquent, développent des stratégies différentes, et qui sont diversement connues ou visibles des observateurs lorsqu'ils se trouvent à l'intérieur ou à l'extérieur des services de police. Les policiers rechignent souvent à communiquer, tout en se satisfaisant de la transmission coutumière d'un savoir empirique, fréquemment basé sur des condensés de bonnes expériences, plutôt que sur l'explicitation de méthodes qui sous-tendent réellement leur travail. Les seconds, les magistrats, ne pouvant avoir accès qu'à une information partielle par l'étude des écrits des enquêteurs qui ne reflètent que très partiellement la première étape de l'enquête policière : la recherche de l'activité délictueuse et de ses auteurs, où souvent une très grande activité policière est pourtant déployée afin de comprendre la situation présente ou passée, de déterminer si une ou plusieurs infractions ont été commises et d'en rechercher et localiser les auteurs.

Or, lorsque les autorités travaillent sur des délinquants professionnels plus ou moins organisés, pour autant que les infractions puissent être suspectées par les autorités de poursuite pénale, les moyens traditionnels ne suffisent plus et l'approche réactive n'est tout bonnement plus adaptée à ce phénomène criminel.

Avec la nouvelle procédure pénale suisse, les enquêteurs devront sans doute mettre en œuvre des moyens d'enquête dits « spéciaux » dans une phase proactive. Cette phase discrète et préliminaire a pour but de recueillir un maximum d'éléments permettant d'établir une suspicion suffisante ou même la preuve de l'activité délictueuse d'un criminel ou de l'organisation dont il fait partie. Elle doit ainsi par exemple permettre de maintenir les prévenus en détention préventive une fois qu'ils auront été interpellés. Cette manière de faire qui est habituelle dans le cadre de la lutte contre le trafic de stupéfiants est en train de se généraliser à d'autres types d'infractions qui sont désormais l'œuvre de groupements organisés, comme les cambriolages.

Il faut être conscient que les moyens engagés lors d'enquêtes proactives d'envergure engendrent un déferlement d'informations difficilement digérable par le ou les enquêteurs.

---

<sup>124</sup> Voir point 1.2.4 – Les étapes du processus d'enquête

Face à ce défi, on peut naïvement penser que l'informatique nous vient naturellement en aide. Ne disposons-nous pas aujourd'hui de puissantes bases de données permettant de gérer des quantités d'information gigantesques ?

Il peut en effet paraître que l'informatique est à même de résoudre seule ces questions. En fait, plus que d'un outil, c'est une méthodologie complète qu'il s'agira de développer. L'enquête criminelle est un processus qui peut être décomposé en étapes, qu'on doit chercher à optimiser. Cette optimisation nécessite par exemple de favoriser le partage et la communication entre des partenaires disposant de compétences propres selon le système légal en vigueur, de connaissances spécialisées, parlant potentiellement plusieurs langues et devant assumer la réalisation de diverses tâches dans le processus d'investigation. Le traitement et l'analyse de volumes de données importants, dispersés ou disparates est une caractéristique commune à la lutte contre la criminalité organisée. Le tout devant fournir un ensemble cohérent répondant à ces nouveaux besoins proactifs spécifiques.

C'est dans ce sens que l'informatique peut répondre à ces besoins. Le chapitre suivant montrera que ce n'a pas été jusqu'ici évident, principalement en raison du peu de conceptualisation des systèmes informatiques développés à des fins d'aide à l'enquête, dans le sens d'une méthodologie de renseignement criminel.

### 1.3 *Les bases de données de police*

Dans ce chapitre, nous survolerons rapidement quelques notions de base nécessaires à la compréhension minimale du lecteur dont ce n'est pas la spécialité, afin qu'il puisse comprendre certains choix et certaines critiques des systèmes préexistants qui ont été faits dans la partie pratique de cette recherche.

Mais, nous souhaitons surtout présenter comment l'informatisation des fichiers de police s'est faite durant les trente dernières années du XX<sup>e</sup> siècle et comment elle a débouché sur les systèmes qui sont ou qui étaient en fonction au début de ce travail de recherche. Notre attention sera forcément focalisée sur les bases de données d'enquête en opposition aux bases de données spécifiques<sup>125</sup> ou aux archives informatisées. Les aspects réglementaires au vu du contexte seront bien évidemment abordés.

#### 1.3.1 Notion de base de données

En voulant directement définir une base de données, on commet déjà un raccourci historique, tant ce terme est devenu évident et commun pour ceux qui sont nés avec l'informatique.

On devrait commencer par définir ce qui a précédé les bases de données informatisées, soit les fichiers<sup>126</sup>, au sens premier du terme, c'est-à-dire une collection de fiche<sup>127</sup>.

La notion de base de données telle que nous désirons l'utiliser dans ce travail est donc une version moderne et informatisée des collections de fiches papier ou cartonnées sur lesquelles on collecte des données en vue de pouvoir les retrouver lorsqu'on en a besoin, par exemple pour les mettre en relation. Le dictionnaire de base la définit d'ailleurs dans ces termes : « *Ensemble de données logiquement reliées entre elles et accessible au moyen d'un logiciel spécialisé* »<sup>128</sup>.

#### 1.3.2 Evolution des fichiers aux bases de données

Or, comme la justice, la police et leurs enquêtes préexistaient à l'informatique, des fichiers y ont également été exploités, notamment dans le domaine de la police technique.

##### 1.3.2.1 Fichiers

Voilà à quoi devait réellement ressembler un fichier il y a environ un siècle :

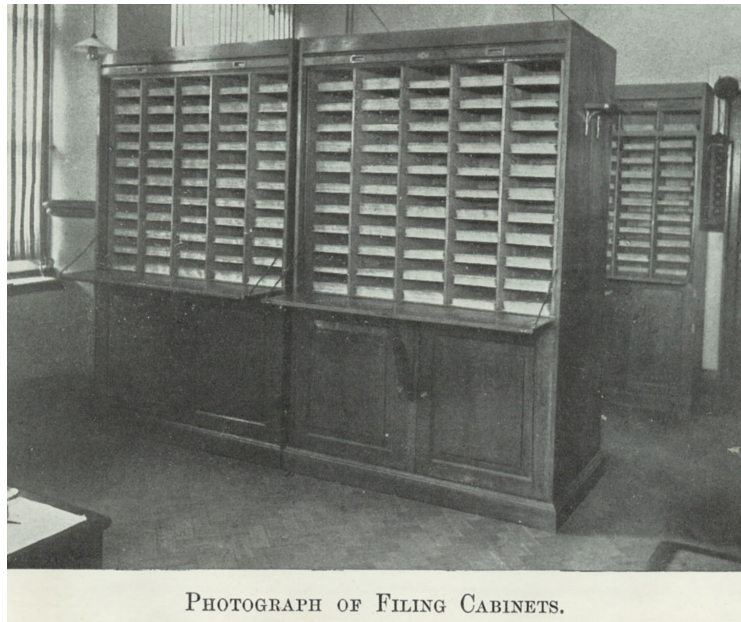
---

<sup>125</sup> Nous pensons ici aux bases de données qui recensent les empreintes digitales ou les profils ADN, ou encore les personnes recherchées ou les objets volés.

<sup>126</sup> **Fichier** 1922 de *fiche*, 1. Collection de fiches, 2. INFORMATIQUE Ensemble structuré d'informations numériques mémorisées sur un support physique. (Le Robert, 1994)

<sup>127</sup> **Fiche** 1413 de *ficher* ; 1865 MODERNE, 1. (...), 2. (...), 3. Carte ou feuille cartonnée sur laquelle on écrit des renseignements en vue d'un classement. (Le Robert, 1994)

<sup>128</sup> **Base de données** INFORMATIQUE; anglais *database*, Ensemble de données logiquement reliées entre elles et accessible au moyen d'un logiciel spécialisé. (Le Robert, 1994)



*fig. 9 : Meubles à fiches<sup>129</sup>*

Les fiches que contenaient des meubles devaient suivre une classification stricte, afin que l'on puisse les retrouver physiquement, selon leur indexation, lorsqu'on en avait besoin, selon les circonstances.

Si les systèmes de classification peuvent paraître triviaux en ce qui concerne des personnes, soit alphabétiquement selon le nom de famille<sup>130</sup>, des systèmes autrement plus ingénieux ont dû être développées lorsque les éléments à classer étaient d'une toute autre nature.

Par exemple, l'apparition de l'utilisation généralisée des empreintes digitales dans les enquêtes de police date du XIX<sup>e</sup> siècle. L'exploitation des empreintes digitales avait déjà pour but d'identifier par comparaison la personne ayant laissé une trace digitale sur les lieux d'un crime. Il était donc nécessaire de conserver et par conséquent de « ficher » des empreintes digitales de comparaison de suspects ou d'auteurs d'infractions connus de la police afin de pouvoir les comparer avec les traces, en cas de récidive.

Dans ce contexte, il est inutile de classer les fiches dactyloscopiques selon les données nominatives de leurs propriétaires légitimes. Il fallait trouver un autre moyen de classer ces fiches afin de pouvoir les retrouver en fonction de l'information de base à disposition : la trace digitale.

Ces systèmes beaucoup plus complexes dénotent l'ingéniosité des praticiens de l'époque comme PURKENJE, HERSCHEL et FAULDS, puis GALTON et HENRY.

---

<sup>129</sup> Illustration tirée de HENRY, *Classification and Uses of Finger Prints*, 1913

<sup>130</sup> Cela peut en effet paraître un mode de classification trivial, si on se limite à la classification alphabétique des noms propres de culture occidentale, mais cela devient vite beaucoup plus compliqué avec les patronymes originaires d'autres régions du globe : arabes, gitans, asiatiques, africains ou encore russes, dont certains connaissent leur propre alphabet, faut-il le rappeler.

C'est ainsi que des systèmes de classification ont vu le jour, tel que celui illustré ci-dessous.

This Form is not to be pinned.

MALE.

H.C.R. No. \_\_\_\_\_






Name \_\_\_\_\_

Aliases \_\_\_\_\_

Prison Reg. No. \_\_\_\_\_

Classification No.  $\frac{13 \cdot U \cdot 10}{18 \cdot U \cdot 10} 14$




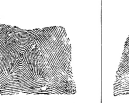

RIGHT HAND.

1.—Right Thumb.	2.—R. Fore Finger.	3.—R. Middle Finger.	4.—R. Ring Finger.	5.—R. Little Finger.
				
(Fold.) W	/	/	W	(Fold.) /

Impressions to be so taken that the flexure of the last joint shall be immediately above the black line marked (Fold). If the impression of any digit be defective a second print may be taken in the vacant space above it.

When a finger is missing or so injured that the impression cannot be obtained, or is deformed and yields a bad print, the fact should be noted under *Remarks*.

LEFT HAND.

6.—L. Thumb.	7.—L. Fore Finger.	8.—L. Middle Finger.	9.—L. Ring Finger.	10.—L. Little Finger.
				
(Fold.) W	/	/	W	(Fold.) /



LEFT HAND. <small>Plain impressions of the four fingers taken simultaneously.</small>	RIGHT HAND. <small>Plain impressions of the four fingers taken simultaneously.</small>
	

fig. 10 : Exemple de fiche dactyloscopique avec sa classification<sup>131</sup>

Par la suite, des systèmes mécaniques de classements, tels que les cartes perforées, ont été développés, mais c'est surtout avec l'avènement de l'informatique que le travail sur les fichiers a changé et que sont nées les *bases de données* telles que nous les connaissons aujourd'hui.

### 1.3.2.2 Bases de données

Comme on l'a vu, une base de données est un ensemble structuré et organisé permettant le stockage de grandes quantités d'informations pour en faciliter l'exploitation.

Les bases de données ont suivi, tout comme l'informatique depuis ses débuts, des modifications conceptuelles.

Historiquement, trois modèles principaux de bases de données ont été développés : *hiérarchique*, *réseau* et *relationnel*. Un quatrième modèle particulier est encore apparu : les bases de données

<sup>131</sup> Illustration tirée de HENRY, *op. cit.*, 1913

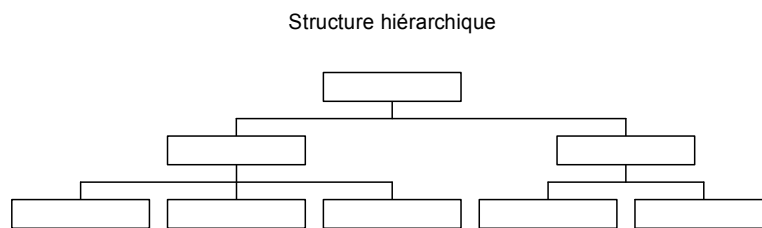
*orientées objet*, puis récemment un assemblage des deux modèles les plus courants : l'*objet relationnel*.

### Base de données hiérarchiques :

C'est le premier système de base de données à avoir été conçu. Il a été par exemple utilisé pour le programme spatial Apollo de la NASA.

Les données sont structurées dans des hiérarchies, comparables à une arborescence de façon à ce que chaque enregistrement n'ait qu'un seul père.

Les liens hiérarchiques entre différents types de données permettent d'obtenir d'un côté les réponses à certaines questions très simplement, mais d'un autre côté, les réponses à d'autres formes de questions deviennent très difficiles. Par exemple, si le principe de la relation « 1 vers n » n'est pas respecté (un téléphone peut être utilisé par plusieurs personnes), alors le modèle hiérarchique ne convient plus et il faut se tourner vers une base de données en réseau.



*fig. 11 : Structure hiérarchique d'une base de données*

Les structures de données hiérarchiques ont été largement utilisées dans les premiers systèmes de gestion de base de données<sup>132</sup>. Cependant, à cause de leurs limitations internes, les modèles de bases de données hiérarchiques ne peuvent souvent pas être utilisés pour décrire des structures existantes dans le monde réel, comme des entités et leurs relations essentielles dans le cadre des enquêtes judiciaires.

### Base de données réseaux :

Ce modèle a été inventé par C.W. BACHMANN, qui a été récompensé du prix Turing<sup>133</sup> en 1973.

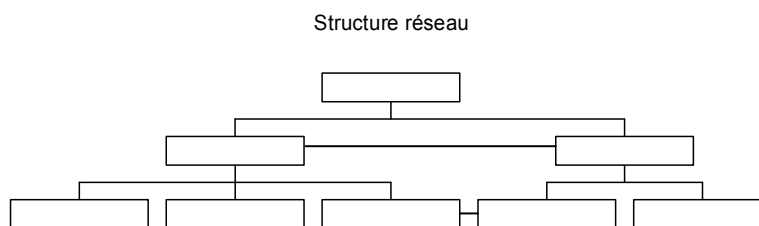
Comme le modèle hiérarchique, ce modèle utilise des pointeurs vers les enregistrements, reflétant la structure physique de l'enregistrement des données. Toutefois, la structure n'est plus forcément arborescente dans le sens descendant. Chaque information peut être associée à plusieurs autres. Il n'y a plus de limitations, un élément pouvant avoir plusieurs ascendants.

---

<sup>132</sup> Voir plus loin : Système de gestion de base de données (SGBD)

<sup>133</sup> Le prix Turing, en hommage à Alan Mathison Turing (1912 - 1954), est attribué tous les ans depuis 1966 à une personne sélectionnée pour sa contribution de nature technique faite à la communauté informatique. Les contributions doivent être d'une importance technique majeure et durable dans le domaine informatique. Cette récompense est parfois considérée comme étant l'équivalent du prix Nobel de l'informatique.





*fig. 12 : Structure réseau d'une base de données*

Le modèle en réseau est plus riche que le modèle hiérarchique, mais il est très difficile à gérer et le programmeur a beaucoup de mal à rendre les données réellement indépendantes les unes des autres en raison de la multiplicité des pointeurs et des ascendants d'un élément.

### Base de données relationnelles :

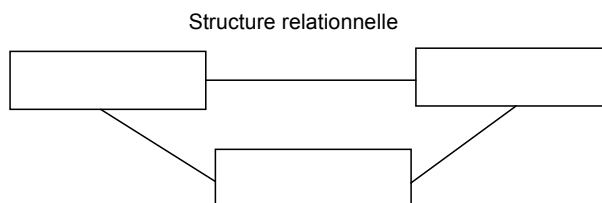
En 1970, au moment où les systèmes basés sur le modèle hiérarchique ou en réseau étaient en plein développement, E.F. CODD publiait un article où il proposait de stocker des données hétérogènes dans des tables, permettant d'établir des relations entre elles. De nos jours, ce modèle est extrêmement répandu, mais en 1970, cette idée était considérée comme une curiosité intellectuelle. On doutait que les tables puissent être jamais gérées de manière efficace par un ordinateur. Ce scepticisme n'a cependant pas empêché E.F. CODD de poursuivre ses recherches. Un premier prototype de *système de gestion de bases de données relationnelles* (SGBDR) a été construit dans les laboratoires d'IBM.

Depuis les années 80, cette technologie a mûri et a été adoptée par l'industrie. En 1987, le langage SQL, qui étend l'algèbre relationnelle, a été standardisé. A l'heure actuelle, les SGBDR sont présents dans de nombreux logiciels, sont très utilisés dans les bases de données et représentent une industrie de plusieurs milliards de dollars.

Le modèle relationnel consiste à représenter aussi bien les entités que les liens (associations) à l'aide de tables de relations. Chaque table décrit alors une partie de l'univers concret.

Une table est une structure tabulaire dont les colonnes, appelées *attributs* - obligatoires ou facultatifs - correspondent aux caractéristiques de *l'entité*. Les lignes sont généralement appelées *occurrences*, *tuples* ou *n-uplets*, ils correspondent aux objets de l'univers.

Tout attribut est désigné par un nom et caractérisé par un domaine. Un *domaine* est un type de données nommé.



*fig. 13 : Structure relationnelle d'une base de données*

Prenons l'exemple suivant :

Nous désirons enregistrer des personnes, leurs adresses et leurs numéros de téléphone. Si on veut s'en tenir strictement au principe qui veut que l'on n'ait pas de redondance d'information, on doit renoncer à une structure hiérarchique et on préférera une structure relationnelle au réseau, trop complexe.

Les entités en présence sont des PERSONNE, des ADRESSE et des TELEPHONE. Chacune de ces entités va contenir un certain nombre d'attributs, soit par exemple :

PERSONNE(Num\_AVS, Nom, Prénom, Date\_de\_naissance)

ADRESSE(NP, Localité, Rue, Numéro\_rue)

TELEPHONE(Numéro\_tél, Type, Prestataire)

Les domaines des attributs ci-dessus seraient :

Num\_AVS = { n°  $\in$   $[10^{12}; 9.9910^{12}]$ }

Nom = {chaîne de 30 caractères}

Prénom = {chaîne de 30 caractères}

Date\_de\_naissance = {chaîne de 8 chiffres}

NP = {chaîne de 4 chiffres}

Localité = {chaîne de 30 caractères}

Rue = {chaîne de 50 caractères}

Numéro\_rue = {chaîne de 5 chiffres}

Numéro\_tél = {chaîne de 11 chiffres}

Type = {fixe, fax, mobile}

Prestataire = {chaîne de 30 caractères}

Dans le monde réel, chaque entité (PERSONNE, ADRESSE OU TELEPHONE) est un individu unique. Toutefois, dans une base de données une personne est de coutume identifiée par ses nom et prénom. Mais si notre jeu de données est relativement important et qu'il existe un risque de confondre deux personnes qui auraient la même combinaison nom-prénom, il peut être nécessaire d'ajouter d'autres éléments qui permettent de les différencier, comme par exemple leur date de naissance. Informatiquement, la gestion de ces éléments discriminants qui peuvent porter sur des domaines différents (chaîne de caractères, de chiffres, dates ou autre) peut être peu satisfaisante et peut ralentir sensiblement les processus de tri et de gestion. On va donc généralement devoir définir des *clés* (aussi appelée *identifiants*), qui sont des contraintes d'intégrité portant sur une *table*. Il ne peut pas y avoir deux fois la même *occurrence* dans une *table*. Chaque enregistrement de la base de données est alors lui aussi unique.

Il faut donc définir les *clés* pour chaque entité. Dans l'exemple ci-dessous, on pourrait utiliser comme clé une donnée existante, soit le numéro AVS<sup>134</sup> qui est unique et spécifique à une PERSONNE, tout comme le numéro d'appel pour l'entité TELEPHONE, soit :

PERSONNE(Num\_AVS, Nom, Prénom, Date\_de\_naissance) ;  
 TELEPHONE(Numéro\_tél, Type, Prestataire).

Cependant, il n'en est, par exemple, pas de même avec l'entité ADRESSE. Dans ce cas, il va falloir définir un attribut supplémentaire de type AdrID = {chaîne de 4 chiffres}<sup>135</sup>.

On procède très souvent par analogie avec chaque entité, en lui définissant une identité informatique propre. Cela facilite la programmation et diminue la taille des fichiers, puisque l'on va travailler avec les données numériques facilement malléables. Par contre, les identifiants propres aux bases de données posent souvent des problèmes lorsqu'il s'agit de mettre en commun des éléments de différentes bases, mais qui concernent effectivement les mêmes entités réelles, leurs identifiants informatiques étant toujours différents !

Les entités et leurs attributs seraient donc finalement :

PERSONNE(PersID, Num\_AVS, Nom, Prénom, Date\_de\_naissance)  
 ADRESSE(AdrID, NP, Localité, Rue, Numéro\_rue)  
 TELEPHONE(TelID, Numéro\_tél, Type, Prestataire)

Ce qui donne sous la forme de la représentation tabulaire :

PERSONNE				
<u>PersID</u>	Num_AVS	Nom	Prénom	Date_de_naissance
1	33373241113	Lehero	Toto	01011970
2	...			

ADRESSE				
<u>AdrID</u>	NP	Localité	Rue	Numéro_rue
1	1006	Lausanne	Rue de la Gare	1
2	...			

<sup>134</sup> Bien que nous soyons conscient que cet identifiant ne soit valable que pour une partie de la population résidant en Suisse.

<sup>135</sup> Ce qui limite ici le fichier d'adresses à 9999 enregistrements.

TELEPHONE			
<u>TelID</u>	Numéro_tél	Type	Prestataire
1	41218611693	Fixe	Zcom
2	...		

fig. 14 : Exemple de tables relationnelles

Manquent encore les *liens* entre les différentes *entités* jusqu'ici disjointes.

Plusieurs solutions s'offrent à nous, selon une nouvelle contrainte d'intégrité, connue sous le nom de *cardinalité*. La cardinalité est le nombre de participation d'*entités* à une *relation*.

*Cardinalité un à un* : si et seulement si par exemple un numéro de téléphone ne peut être l'abonnement que d'une seule personne et qu'une personne ne peut avoir qu'un seul abonnement téléphonique.

*Cardinalité un à plusieurs* : une personne peut détenir plusieurs téléphones qui sont différents abonnements mais chaque téléphone ne fait partie que de l'abonnement d'une seule personne.

*Cardinalité plusieurs à plusieurs* : une personne peut avoir plusieurs abonnements de téléphone et un téléphone peut être utilisé par des personnes différentes.

Si l'on s'en tenait à des cardinalités un à un, on pourrait travailler avec un modèle hiérarchique, mais il est rare que cette seule cardinalité soit la règle.

Dans notre exemple, si on applique la cardinalité un à plusieurs en ce qui concerne les personnes et leur adresse (une adresse peut être la même pour plusieurs personnes, mais une personne n'a qu'une seule adresse), on peut inclure à la table PERSONNE une *clé externe* qui contient la référence au détail de l'adresse contenue dans la table spécifique ADRESSE.

PERSONNE					
<u>PersID</u>	Num_AVS	Nom	Prénom	Date_de_naissance	Adresse
1	25473241113	Lehero	Toto	01011970	1
2	...				

ADRESSE				
<u>AdrID</u>	NP	Localité	Rue	Numéro_rue
1	1006	Lausanne	Rue de la Gare	1
2	...			

fig. 15 : Exemple de tables de relation de cardinalité un à plusieurs

Si par contre, on travaille avec le principe de la cardinalité plusieurs à plusieurs pour ce qui est des téléphones et de leurs utilisateurs, il va être nécessaire de construire une table externe des liens entre ces deux entités.

LIEN_PERS_TEL			
LienPTID	Personne	Téléphone	Type
1	1	1	Abonné
2	...		

fig. 16 : Exemple de tables de relations de cardinalité de plusieurs à plusieurs

### Base de données orientée objet :

« Les modèles de données à objets ont été créés pour modéliser directement les entités du monde réel avec un comportement et un état. Le concept essentiel est bien sûr celui d'objet. Il n'est pas simple à définir, car composite, c'est-à-dire intégrant plusieurs aspects. Dans un modèle objet, toute entité du monde réel est un objet, et réciproquement, tout objet représente une identité du monde réel. »<sup>136</sup>

Un objet est donc une entité qui possède une identité, un état et un comportement. Par exemple, une voiture V1 est un objet. Un tel véhicule est caractérisé par un état constitué d'un numéro d'immatriculation, une marque, un type, un moteur, un nombre de kilomètres parcourus, etc. Il a aussi un comportement composé d'un ensemble d'opérations permettant d'agir dessus, par exemple : créer(), démarrer(), rouler(), stopper(), détruire(). Chaque opération a bien sûr des paramètres qui ne sont pas décrit en détail ici.

L'objet de type véhicule et d'identité V1 est donc représenté comme un groupe de valeurs nommées avec un comportement associé :

```
V1 {
  Numéro : VD11111, Marque : Peugeot, Type : 107, Moteur : essence 1.0 ;
  créer(), démarrer(), rouler(), stopper(), détruire() }.
```

fig. 17 : Exemple d'un objet d'une base de données orientée objet

Un objet peut être très simple et composé seulement d'une identité ou d'une valeur, mais il peut aussi être très complexe et lui-même être composé d'autres objets. Par exemple, un « avion » est composé d'une de plusieurs objets de type « moteur », de deux objets « aile » et d'un objet « fuselage », qui sont eux-mêmes des objets complexes.

Cette manière de concevoir un système de stockage propose un moyen plus riche et plus naturel de modéliser un problème complexe. En particulier, un objet peut référencer un autre objet. Ainsi, le véhicule V1 référence le moteur M1 et la personne P1 référence le véhicule V1. Le partage référentiel d'un sous-objet commun par deux objets devient possible sans duplication de données.

Au-delà d'une structure statique permettant de modéliser les objets et les liens entre eux, les modèles à objet permettent d'encapsuler les structures des objets par des opérations.

<sup>136</sup> GARDARIN, Bases de données – objet et relationnel, 2003

De plus, afin d'éviter la répétition de toutes les propriétés pour chaque *classe* d'objets (différents types objets avec les mêmes *attributs* et *opérations*), il est possible de définir de nouvelles classes par affinage de classes plus générales. C'est le mécanisme d'*héritage*.

Enfin, lors de la définition d'une hiérarchie de classes, certaines propriétés peuvent être spécifiées différemment pour chaque sous-classe. Cette faculté appelée *polymorphisme* permet donc à une même opération de s'appliquer à des objets de différentes classes ou à des objets d'une même classe.

Cette faculté des objets à représenter les entités pertinentes d'un problème et leur relation a révolutionné les méthodes de développement des systèmes informatisés. La possibilité de définir des architectures basées sur des composants réutilisables d'une application à l'autre est particulièrement importante dans le cadre de l'analyse criminelle opérationnelle. Cette modularité et cette souplesse permettent de traiter des affaires successives se ressemblant, tout en présentant des spécificités nécessitant parfois des adaptations mineures.

Base de données objet-relationnel :

Le développement des bases de données objet s'est rapidement heurté à la nécessité de conserver la compatibilité avec l'existant. En effet, la fin des années 1980 a vu le déploiement des systèmes de gestion de bases de données relationnelles et des applications client-serveur. Les utilisateurs n'étaient donc pas prêts à remettre en cause ces nouveaux systèmes dès le début des années 1990<sup>137</sup>. Cependant, les tables relationnelles ne permettaient guère que la gestion de données alphanumériques. Avec l'avènement du Web au milieu de la décennie 1990, la nécessité de supporter des données complexes au sein de la base de données s'est amplifiée. Ces objets complexes peuvent être des documents textuels, des données géométriques ou géographiques, audiovisuelles ou soniques. En bref, il s'agit de supporter de manière optimale des données multimédia.

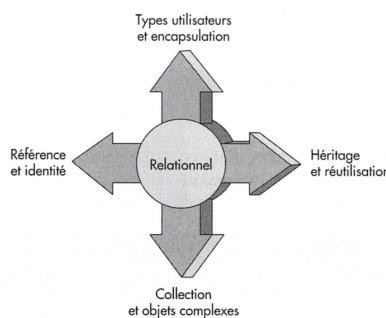


fig. 18 : Les extensions apportées au relationnel <sup>138</sup>

Le modèle objet-relationnel est fondé sur l'idée d'extension du modèle relationnel avec les concepts essentiels de l'objet. Le cœur du modèle reste donc conforme au relationnel, mais l'on ajoute les concepts clés de l'objet sous une forme particulière pour faciliter l'intégration des deux modèles.

<sup>137</sup> GARDARIN, *op. cit.*, 2003

<sup>138</sup> Tiré de GARDARIN, *op. cit.*, 2003

### Systèmes de gestion de base de données :

La gestion et l'accès à une base de données sont assurés par un ensemble de programmes qui constituent le Système de gestion de base de données (SGBD).

Un système de gestion de bases de données héberge généralement plusieurs bases de données, qui sont destinées à des logiciels ou à des thématiques différents.

Les objectifs des SGBD sont les suivants :

- Sécurité des données
- Partageabilité des données
- Efficacité des accès aux données
- Non-redondance des données
- Vérification de la cohérence des données
- Administration centralisée des données
- Manipulation des données par des non-informaticiens

Lors de la mise en œuvre d'un SGBD, on distingue trois niveaux d'appréhension d'une base de données:

- Le niveau interne avec le schéma physique
- Le niveau conceptuel avec le schéma conceptuel
- Le niveau externe avec les schémas externes

Le niveau interne spécifie comment les données sont enregistrées sur les mémoires secondaires (disques, bandes, etc.). Seule la base physique a une existence matérielle.

Le niveau conceptuel décrit par un schéma, en termes abstraits mais fidèles, la réalité sans souci d'implantation en machine.

Le schéma conceptuel permettra de définir les types de données élémentaires, soit les attributs, et les types de données composées qui permettent de regrouper les attributs afin de décrire les entités ou associations du monde réel, et enfin éventuellement les règles que devront suivre les données au cours de leur vie.

Au niveau externe, les schémas décrivent la partie des données présentant un intérêt pour un utilisateur ou un groupe d'utilisateurs.

## **1.3.3 Survol historique des bases de données de police en Suisse**

### **1.3.3.1 Au niveau cantonal**

Comme le mentionne la Constitution fédérale en son article 3, les cantons sont souverains. L'article 123 précise qu'en matière de droit pénal, bien que la législation soit de nature fédérale,

l'organisation judiciaire et l'administration de la justice sont du ressort des cantons. C'est donc à ce niveau que se trouvent historiquement les informations de police.

Il est clair qu'au temps des fichiers « papier » dans les différents cantons, les informations (fiches) ne pouvaient être consultées que par des personnes ayant un accès physique à l'information.

Lors de l'informatisation des fichiers, on aurait pu s'attendre à la mise en commun de ressources cantonales pour utiliser des systèmes compatibles. Au début des années 1990, comme le mentionne RIBAUX<sup>139</sup> des efforts avaient été entrepris pour harmoniser et coordonner les systèmes informatiques entre les cantons de Suisse romande. Une convention liait ces cantons à un centre informatique installé à Genève. Mais, en 1994, la convention n'a pas été renouvelée pour des raisons de difficultés budgétaires et de la trop grande influence des besoins spécifiques des Genevois. Une situation à nouveau du « chacun pour soi » était redevenue d'actualité.

Actuellement, au niveau des polices cantonales, une harmonisation technologique partielle s'est faite par le biais d'une solution logicielle spécifique mise au point par une société suisse spécialisée dans le domaine policier et de la sécurité. Cette société distribue un produit<sup>140</sup> qui est exploité dans une vingtaine de cantons, dont Genève depuis 2003. Les solutions en place ne sont toutefois pas immédiatement compatibles, puisque des versions différentes ont été produites et distribuées, certains cantons pionniers, qui ne peuvent plus financer une mise à jour des logiciels métier, travaillent désormais avec une version plus ancienne qu'un autre canton qui viendrait d'acquérir le système de gestion.

Le canton de Vaud, après avoir tenté de mettre au point un système d'information de police en collaboration avec le canton de Fribourg (projet *SiPol*), a mis un terme à cette collaboration et exploitait isolément son propre système *Zéphyr*. Ce dernier a toutefois été remplacé en 2009 par un nouveau système *Sinap*<sup>141</sup>, qui n'existe pas dans d'autres cantons, à cause de son incompatibilité avec les nouvelles exigences pour l'uniformisation de la statistique de police en Suisse.

Il est important de remarquer ici que les systèmes d'information de police actuellement développés ou en exploitation cherchent à s'intégrer le plus tôt possible dans le traitement de l'information. Ainsi, lors de la rédaction du premier rapport, soit lors de la prise d'une plainte, ou lors d'un constat

---

<sup>139</sup> RIBAUX, La recherche et la gestion des liens dans l'investigation criminelle : le cas particulier du cambriolage, 1997

<sup>140</sup> Il s'agit du produit « ABI » (Automatisierte Büro-Information), de ROLA SA.

<sup>141</sup> Finalement, une des deux sociétés proposant un système préexistant dans un autre grand canton (ZH) a retiré son offre, vraisemblablement pour des raisons de délais trop courts par rapport aux ressources disponibles et le choix s'est porté sur un nouveau système basé sur le précédent et fourni par une société équipant déjà la police cantonale vaudoise pour d'autres solutions connexes (journal des événements et générateur de rapports).



de flagrant délit, par exemple, un maximum de données sont directement référencées dans le système de fichier de police centralisé.

Cette tendance entraîne un « transfert » de charge dévolue précédemment à des services spécialisés (dossiers) au personnel du front (les policiers), qui n'est pas toujours accueilli avec bonheur par ces derniers, étant donné que cela rigidifie un processus qui peut demander beaucoup de souplesse, au vu du nombre important de situations différentes auxquelles les policiers doivent répondre. Des compromis doivent être trouvés, mais il n'est pas rare que les utilisateurs rejettent les nouveaux systèmes intégrés à cause d'une trop grande rigidité. Ce comportement influence ensuite directement la qualité des données saisies.

Quoi qu'il en soit, en ce qui concerne la criminalité intercantonale, voire internationale, le système fédéraliste avec ses 26 cantons souverains et une police fédérale pose un problème. C'est du côté fédéral qu'il faut se tourner, pour trouver une éventuelle planche de salut.

### **1.3.3.2 Au niveau fédéral**

En fait, comme le rappelle KREIS<sup>142</sup>, dès le début des années 1960, les cantons tentèrent de mettre sur pied un système d'information policier au niveau national. La centralisation de la lutte contre le crime était déjà considérée comme nécessaire pour répondre à l'augmentation des délits et à la mobilité accrue des criminels. La Confédération observa durant plusieurs années l'évolution à l'étranger et en 1970, décida que cette centralisation devait être couplée avec une informatisation.

A cette époque, la Confédération se pencha aussi sur la question de la centralisation et de l'informatisation de ses divers registres de police. Le Ministère public de la Confédération (MPC) proposa un plan très élaboré de système de traitement électronique en trois phases :

La première prévoyait l'informatisation du casier judiciaire central, avec la possibilité d'y intégrer les casiers judiciaires cantonaux.

La deuxième devait centraliser et informatiser les fichiers des criminels des banques de données cantonales et municipales.

Enfin, la troisième phase prévoyait l'introduction d'une technique permettant la comparaison électronique des empreintes digitales et éventuellement de la voix.

La première phase ne fut pas réalisée, une étude préliminaire ayant montré que cela aurait coûté trop cher. On commença donc directement la seconde phase par la préparation du KIS (*Kriminalpolizei Information System*).

#### Le système d'information de la police criminelle (KIS) :

Bien que les besoins de centralisation et d'informatisation des données fussent unanimement reconnus des praticiens et de la classe politique, il fut rapidement évident que la Confédération et les cantons de Genève et de Zurich, se présentant comme porte-parole de leurs régions, avaient des vues différentes sur la réalisation du KIS. Ces deux cantons avaient en effet eux-mêmes déjà

<sup>142</sup> KREIS, DELLEY, KAUFMANN, La protection de l'Etat en Suisse : l'évolution de 1935 à 1990, 1993

procédé à d'énormes travaux préparatoires en informatique, alors que le MPC proposait comme seule solution judicieuse et homogène une centralisation au niveau national par la suppression de certaines compétences au niveau cantonal.

Ce n'est qu'en novembre 1977 que la Conférence des chefs de départements cantonaux de justice et police (CCDJP) se prononça à l'unanimité pour un KIS national.

En 1978, environ 100 spécialistes des corps de police cantonaux, des villes de Berne et Zurich et de la Confédération, présentèrent trois rapports de concept sur trois sections du KIS : personnes, faits et personnes à antécédents. Les conventions qui en découlèrent furent acceptées en 1978 encore, par le Conseil fédéral et la CCDJP.

Les travaux furent déjà interrompus au cours de l'année suivante. Zurich et Genève avaient à nouveau tendance à prôner la régionalisation. Ils demandaient d'une part une liaison avec leur propre système régional et d'autre part Zurich voulait mettre en place sa propre solution de saisie. La Confédération refusa ces revendications, surtout parce qu'elle redoutait que les systèmes régionaux ne prennent trop d'avance.

A peu près à la même époque, des doutes furent émis sur les bases juridiques administratives du KIS, qui furent remises en question et on évoqua la protection des données. Aux niveaux fédéral et cantonal se fit jour une résistance politique qui voyait là un transfert de compétences et un embryon de « BUSIPO »<sup>143</sup>. Face à l'opposition grandissante contre le KIS, le MPC se vit dans l'obligation de justifier son engagement en haut lieu. Le concept « personnes à antécédents » fut revu de sorte que les informations ne faisant pas partie d'une procédure pénale, par exemple de nature administrative ou relevant de la police politique, ne devaient pas être intégrées au KIS.

Mais la forte résistance juridique, politique et fédéraliste avait déjà condamné le projet en 1980. Pourtant les travaux furent poursuivis en 1981, alors que plusieurs cantons se retiraient du KIS. L'abandon officiel du projet ne survient toutefois qu'en 1985.

Durant toute cette période, le MPC s'était entièrement consacré au KIS et avait repoussé ses autres projets de « Traitement Electronique des Données »<sup>144</sup> (TED). Il reprit cependant ses propres projets TED lorsque fin 1979, l'échec du KIS devint manifeste.

#### Les projets TED :

Dans les années 1980, le MPC put enfin réaliser quelques projets élaborés dans les années 1970. Ainsi, l'automatisation de l'index du casier judiciaire (ASTERIX) eut lieu en 1983, de même que l'automatisation du système d'identification des empreintes digitales (AFIS) en 1984<sup>145</sup>, alors que le fichier de détenus était totalement supprimé.

---

<sup>143</sup> Bundes Sicherheit Polizei (police fédérale de sécurité)

<sup>144</sup> TED est la mauvaise traduction de l'allemand EDV (elektronische Datenverarbeitung).

<sup>145</sup> Depuis, une autre base de données « technique » a rejoint AFIS, il s'agit de la base de données ADN, dont l'exploitation est réglementée dans la nouvelle loi sur l'utilisation des profils ADN dans les procédures pénales du 20 juin 2003 [FF 2003, 3981-3989], qui remplace l'ordonnance transitoire [RS 361.1] y référant.

A peu près à la même époque, le registre des recherches de la Rédaction du Moniteur suisse de Police (RIPOL) fut informatisé et devint par la suite accessible aux gardes-frontière et aux cantons et fonctionna comme succédané très partiel du KIS.

Si les projets TED avançaient dès lors rapidement, ceux de la Police fédérale n'avançaient qu'à pas lents. Dès 1975, un crédit avait été prévu pour un programme test TED, qui ne put finalement pas être réalisé. Ce n'est qu'en 1979 qu'un premier concept fut élaboré, mais il concluait de manière peu substantielle qu'il fallait d'abord déterminer les besoins globaux.

Ce n'est ensuite qu'en 1983 que la Police fédérale proposa au MPC d'introduire un projet-pilote TED. Ce projet-pilote était limité à l'extrémisme de droite et prévoyait une année entière pour élaborer le concept, et plus de 6 mois pour la programmation. Au terme d'un an et demi d'essai, il était prévu d'entamer en 1987 la planification et l'analyse préalable du système général proprement dit.

En juin 1984, le concept AHRBA (Automatisation du Registre central du Ministère public de la Confédération) fut présenté. Puis en 1986, le MPC demanda une modification du projet-pilote, l'extrémisme de droite ne permettant pas une récolte suffisante de données pour pouvoir rassembler suffisamment d'expériences utiles. Le projet-pilote se mua en ARABEX, mais il n'avança guère par des retards dus à la réorganisation du service informatique du MPC. Ce n'est qu'en août 1988 que la saisie des données commença. L'année suivante, la saisie rétrospective des noms arabes était terminée, mais l'élargissement du projet-pilote en janvier 1990 fut interrompu par l'« affaire des fiches ».

Après l'affaire des fiches, l'organisation du MPC et de l'Office fédéral de la police (OFP) a changé une première fois, avant la mue décrite au chapitre précédent.

Les années 1990 étaient marquées par les missions de coordination dévolues aux Offices centraux de police criminelle.

#### **1.3.4 Les bases de données centralisées de police judiciaire**

Lors des années 1990, la lutte contre le trafic illicite de stupéfiants a été le moteur des efforts consentis par la Confédération pour le décloisonnement des informations.

En effet, les Offices centraux de police criminelle ne disposant pas des compétences d'enquête, un pas important a été franchi dans la coordination des données recueillies par les cantons, lors d'opérations de grande envergure. Le système informatique DOSIS était né.

Ce système régi par une ordonnance fédérale permettait aux cantons de partager leurs données relatives aux enquêtes en cours sur le trafic illicite de stupéfiants. Les cantons y ont adhéré plus ou moins rapidement, mais en une dizaine d'années, la quasi-totalité des cantons suisses utilisait le système DOSIS.

Des relations simples directes ou indirectes pouvaient être introduites malgré la structure hiérarchique de la base de données. Il devenait dès lors possible de retrouver des liens de manière quasi automatique, sans passer par une diffusion nationale<sup>146</sup>.

Après quelques années d'alimentation de la base, qui constitua son « fonds de roulement », cet outil d'abord contesté, est ensuite très rapidement apparu comme indispensable aux yeux des enquêteurs en charge des affaires de trafic illicite de stupéfiants.

Les succès rencontrés avec le système DOSIS en ce qui concerne le trafic illicite de stupéfiants a encouragé la Confédération à étendre la palette des infractions pour lesquelles ce système d'information fédéral pouvait être utilisé. Des systèmes parallèles basés sur le même modèle conceptuel ont donc été créés et mis à la disposition des cantons. Il s'agissait de ISOK<sup>147</sup> pour le crime organisé et de FAMP<sup>148</sup> pour la fausse monnaie, la traite des êtres humains et la pornographie.

Ces trois systèmes étaient malheureusement cloisonnés entre eux et une nouvelle cécité des liens<sup>149</sup> était apparue, la Confédération ne disposant pas encore des bases légales nécessaires.

En 2000, une nouvelle ordonnance fédérale a été édictée et les trois systèmes ont été fusionnés dans le système JANUS. Ceci a enfin permis de regrouper les informations relatives au crime organisé, à la traite des êtres humains et au trafic illicite de stupéfiants.

Afin que la police judiciaire fédérale dispose de son propre système informatisé opérationnel, l'ordonnance JANUS<sup>150</sup> a été modifiée dès 2002 et en 2006 pour répondre aux nouvelles compétences de la Confédération.

Les données traitées concernent désormais non seulement le trafic illicite de stupéfiants, le crime organisé et la traite des êtres humains, mais aussi le faux monnayage, la mise en circulation de publications obscènes, le terrorisme, le trafic d'armes et la criminalité en relation avec la protection de l'Etat, la criminalité économique et le blanchiment d'argent, la corruption, et finalement dans une certaine mesure toutes les infractions relevant de la compétence des autorités cantonales.

#### **1.3.4.1 Les bases de données centralisées JANUS**

Il existe toujours à l'heure actuelle une unique base de données fédérale centralisée de renseignement de police. Elle fait partie du système informatisé de la police judiciaire fédérale

---

<sup>146</sup> La diffusion nationale est un processus plus lourd et moins rapide, qui consiste en une requête adressée à chaque canton et qui est tributaire de la bonne volonté de chacun.

<sup>147</sup> InformationsSystem zur Bekämpfung der Organisierten Kriminalität

<sup>148</sup> Datenverarbeitungssystem zur Bekämpfung der Falschmünzerei, des Menschenhandels und der Pornografie

<sup>149</sup> La notion de cécité des liens est la version française de *linkage blindness*

<sup>150</sup> RS 360.2 – Ordonnance sur le système informatisé de la Police judiciaire fédérale du 30 novembre 2001

(PJF), et elle peut également être utilisée par les cantons. Ce système informatisé d'enquêtes est réglementé par une ordonnance fédérale<sup>151</sup>, qui précise le but du système JANUS à son article 2 :

**Art. 2** But du système informatisé

JANUS a pour but de faciliter:

- a. les tâches légales d'information, de coordination et d'analyse de la police judiciaire fédérale;
- b. l'exécution, dans les domaines de compétence de la Confédération, des enquêtes préliminaires et des enquêtes de police judiciaire;
- c. la coopération de la police judiciaire fédérale avec les autorités cantonales de poursuite pénale et les services de police criminelle des cantons qui participent dans le cadre de leurs compétences à la lutte contre le crime intercantonal ou international;
- d. la collaboration de la police judiciaire fédérale avec les autorités étrangères dans la lutte contre la criminalité internationale;
- e. l'exécution, par les autorités cantonales de poursuite pénale et les services de police criminelle des cantons, des enquêtes préliminaires et des enquêtes de police judiciaire qui n'entrent pas dans la compétence fédérale et qui ne tombent pas sous les dispositions de la loi fédérale du 15 juin 1934 sur la procédure pénale (PPF), de la LOC et de la LMSI;
- f. la gestion des documents et des dossiers utilisés par la police judiciaire fédérale.

Comme il s'agit du système informatique de la PJF, le champ d'application est en relation avec le nouvel article 340<sup>ter</sup> CP qui définit les nouvelles compétences fédérales. Or, comme ce système poursuit également le but de faciliter les enquêtes préliminaires ou les enquêtes ouvertes des cantons, l'article 3 de l'ordonnance JANUS détaille son champ d'application :

**Art. 3** Champ d'application

1. Sont traitées dans JANUS, dans le cadre des tâches assignées à la police judiciaire fédérale à l'art. 2 LOC, les données nécessaires à:
  - a. la prévention et la lutte contre le trafic illicite des stupéfiants (...);
  - b. la reconnaissance et la lutte contre le crime organisé (...);
  - c. la lutte contre la fausse monnaie (...);
  - d. la lutte contre la traite des blanches (...);
  - e. la lutte contre la circulation des publications obscènes (...);
  - f. la lutte contre la criminalité économique (...);
  - g. la lutte contre le blanchiment d'argent (...);
  - h. la lutte contre les délits de corruption (...).
2. Sont également traitées dans JANUS les données nécessaires à l'accomplissement des tâches assignées à la police judiciaire fédérale dans les domaines de la lutte contre le terrorisme, le trafic d'armes et la criminalité en relation avec la protection de l'Etat ainsi

---

<sup>151</sup> RS 360.2 – Ordonnance du 30 novembre 2001 sur le système informatisé de la Police judiciaire fédérale

que la poursuite des autres délits mentionnés à l'art. 340 CP en tant qu'ils relèvent de la compétence de la Confédération. (...).

2bis. Sont également traitées dans JANUS les données transmises par l'Office européen de police (Europol) (...).

3. Les autorités cantonales de poursuite pénale et les services de police criminelle des cantons peuvent également traiter dans le sous-système «Journaux» JANUS des données se rapportant à des infractions qui n'entrent pas dans la compétence fédérale et qui ne tombent pas sous les dispositions de la PPF, de la LOC et de la LMSI. Le traitement de ces données se fait conformément aux dispositions cantonales.

L'alinéa 3 de cet article 3 mentionne un sous-système « Journaux ». Il est important de faire la distinction entre les deux sous-systèmes de JANUS, utilisés au quotidien par les différents utilisateurs fédéraux et cantonaux :

#### **Art. 4** Structure de JANUS

JANUS se compose des sous-systèmes suivants:

- a. «Personnes et antécédents» (PV), où sont enregistrées des données sur des personnes et leurs antécédents recueillies dans le cadre d'enquêtes préliminaires, d'enquêtes de police judiciaire ou de sources accessibles au public;
- b. «Journaux» (JO), où sont enregistrées par affaire des données provenant d'enquêtes préliminaires, d'enquêtes de police judiciaire ou de sources accessibles au public (notamment surveillances des télécommunications, observations, mains courantes d'enquête);
- c. (...)

Ces deux sous-systèmes opérationnels sont décrits plus en détail à l'article 5 de l'ordonnance :

#### **Art. 5** Structure des sous-systèmes «Personnes et antécédents» et «Journaux»

1. Le sous-système «Personnes et antécédents» (PV) se compose:

- a. des données de base relatives à l'identité des personnes;
  - b. des antécédents, à savoir les données relatives aux faits, répertoriées en fonction de différentes catégories criminologiques;
  - c. des sous-champs dont l'utilisation permet, entre autres, de marquer les éléments de comparaison, notamment avec des tierces personnes, dans le texte d'un antécédent et de consulter des données d'après ces éléments de comparaison.
- (...)

2. Le sous-système «Journaux» se compose:

- a. de l'en-tête, à savoir les données relatives aux journaux tenus dans le cadre d'une affaire;
  - b. des inscriptions, à savoir les données relatives aux faits.
- (...)

Suite aux demandes répétées des analystes criminels actifs dans les différents cantons et au sein de l'OFP, il est remarquable que les fonctionnalités d'analyse aient enfin été prévues dans la révision de l'ordonnance en 2002. Elles sont réglées à l'article 19 :

**Art. 19** Traitement de données dans des systèmes d'analyse externes

1. Les données personnelles JANUS peuvent être copiées et traitées dans un système externe spécifiquement destiné à l'analyse pour exécuter une mission d'analyse dont le contenu et la durée sont définis:
  - a. par la direction de la police judiciaire fédérale; une telle mission ne peut être entreprise que par des spécialistes de la police judiciaire fédérale expressément autorisés. Les transferts de données qui dépassent la simple visualisation nécessitent l'accord du conseiller à la protection des données de l'office;
  - b. par l'autorité de police judiciaire compétente; une telle mission ne peut être entreprise que par des spécialistes de police criminelle des cantons expressément autorisés et après information de l'autorité cantonale compétente en matière de protection des données.
2. Une fois la mission accomplie, les données copiées dans le système externe doivent être immédiatement détruites.
3. L'office précise les modalités dans le règlement sur le traitement des données.

De par la rapidité des recherches, les relations détectées permettent de récolter une masse d'informations significatives durant l'enquête préliminaire. Il devient dès lors légitime de vouloir reconstituer le puzzle et d'apprécier la structure de l'organisation criminelle.

### **1.3.5 Les bases de données utiles à l'enquête**

De tout temps, l'enquêteur a eu pour but de rassembler des informations, de les analyser et d'en tirer une image, représentation d'une situation passée, dans le cadre des enquêtes classiques, ou présente, dans le cadre des enquêtes préliminaires.

Pour remplir sa mission, il dispose d'une multitude de sources d'informations. Il peut s'agir de registres à caractère judiciaire, par exemple le casier judiciaire, ou les dossiers de police judiciaire. Mais il s'agit aussi et en très grande mesure de registres administratifs, nécessaires à l'élaboration d'un examen de situation d'un suspect, comme le contrôle des habitants, les offices des poursuites et faillites, le registre foncier, le registre du commerce, etc. Il va sans dire que pour mener à bien sa mission, les informations dont la police judiciaire a besoin ne se trouvent pas toujours dans des registres. Il va falloir aller chercher des informations auprès de privés, de sociétés commerciales (principalement financières ou de télécommunication) et d'informateurs.

Toutes ces informations se retrouvent en main de l'enquêteur pour en faire la synthèse dans un rapport circonstancié qui sera délivré à l'autorité d'instruction et archivé aux dossiers de police judiciaire.

Dans le cadre de la criminalité organisée, de très nombreuses informations concernant le même sujet (personnes physiques ou morales) se trouvent dans de très nombreux registres de police différents, à cause du découpage fédéraliste. Les systèmes d'information de police cantonaux sont sans doute très bons, bien qu'ils répondent parfois plus à des soucis d'archivage que d'analyse.

Mais à l'heure actuelle, il n'est plus raisonnable de ne pas suivre la voie de la centralisation que ce soit au niveau des registres administratifs ou de bases de données spécifiques permettant de mettre en commun le détail des informations d'enquête autant que les codes de procédures cantonaux le permettent, et en respect de la loi sur la protection des données personnelles (LPD<sup>152</sup>).

### 1.3.6 Synthèse

Dans le contexte judiciaire, le besoin de répondre à des problématiques spécifiques ou générales a amené la police à exploiter dès le début du XX<sup>e</sup> siècle des fichiers physiques, remplacés dès les années 1970 par des bases de données informatiques. Comme nous l'avons vu, leur développement ne s'est d'ailleurs pas fait sans heurts dans ce contexte sensible qui doit allier efficacité des organes de sécurité de l'Etat, dont la police fait partie, et protection des libertés individuelles.

Dans le cadre des enquêtes contre la criminalité organisée le développement et l'implantation de bases de données centralisées ont offert dès le milieu des années 1990 des potentialités jusqu'ici inexistantes dans le traitement de l'information. La volonté politique, initiée à cette même époque, de poursuivre dans cette voie est affichée et a été renforcée en 2002 par l'attribution de certaines compétences à la police judiciaire fédérale au sens de l'art 337 CP<sup>153</sup>.

Le cadre juridique spécifique à ces bases de données partagées permet aussi aux cantons d'utiliser le système centralisé JANUS. Il est légitime que ce système soit au bénéfice de la Confédération, puisque le système lui appartient, mais que ce dernier soit partagé avec l'ensemble des autorités de poursuites pénales en Suisse démontre la prise de conscience du besoin constant de coopération et de coordination lorsque l'on veut lutter efficacement contre le phénomène de la criminalité organisée.

Le précédent chapitre traitant de l'enquête a cherché à montrer que les structures et l'organisation des autorités de poursuite pénale sont directement influencées par les contraintes fixées par le cadre légal qui régit leurs compétences territoriales ou contextuelles. Nous avons également vu que les corps de police s'organisent en conséquence et essaie de se doter des moyens nécessaires à mener à bien leur mission, que ce soit des ressources humaines ou matérielles. Les systèmes d'information font traditionnellement partie de ces ressources matérielles. Leur mise en place et leur exploitation peuvent parfois créer des situations dans lesquelles le traitement des affaires et le flux des

---

<sup>152</sup> RS 235.1 – Loi fédérale du 19 juin 1992 sur la protection des données (LPD)

<sup>153</sup> Anciennement art. 340<sup>bis</sup> CP.



informations n'est en définitive pas optimal. Souvent, le praticien se trouve confronté à des obstacles qui n'ont pas de sens pour lui et qui, en fin de compte, lui compliquent la tâche. Par exemple, il a fallu un changement important de la politique criminelle en Suisse et plusieurs réformes législatives successives pour qu'un système informatique d'aide à l'enquête, centralisé et partagé voie enfin le jour (DOSIS), puis qu'il soit dévoué à plusieurs types de criminalité (DOSIS, ISOK, FAMP), et enfin que toutes ces informations soient regroupées en une seule base commune (JANUS). Alors qu'au début, le praticien ressentait un besoin en fonction de l'efficacité des premières bases de données, l'évolution de ces dernières s'est faite avec un manque de méthodes explicites et une mauvaise formalisation des besoins des différents partenaires actifs dans l'enquête (policier, spécialiste, analyste ou encore expert forensique).

Cependant, l'existence de cette base de données commune, bien qu'elle soit nécessaire, ne peut pas être, à elle seule, une condition suffisante à la réussite des investigations. La complexité des interconnexions ne permet parfois plus de pouvoir apprécier une situation particulière lorsque la taille des groupements criminels augmente, et *a fortiori*, d'en extraire une image globale du phénomène traité.

Sur un plan structurel, et comme l'a mentionné le rapport de situation 2000 de l'Office fédéral de la police, la police judiciaire fédérale avec ses compétences étendues au territoire de la Confédération lève un obstacle important par la conduite de l'enquête sur l'ensemble du territoire national.

Toutefois, l'appréciation de situations complexes et l'interprétation des informations deviennent difficiles, voire impossibles avec les techniques d'enquête traditionnelles. Si les outils informatiques permettent actuellement de rechercher des liens et d'intégrer les données brutes, leur interprétation est un tout autre problème.

Entre les cadres légal, structurel, organisationnel et celui des outils développés, il manque clairement un niveau qui aide à conceptualiser le traitement des informations et à donner du sens à l'ensemble du processus d'enquête dans le cadre de la lutte contre la criminalité organisée. Ce niveau, méthodologique, doit s'inscrire dans une démarche de renseignement criminel, dont l'analyse criminelle fait partie.

## 1.4 L'analyse criminelle

La littérature à disposition sur l'analyse criminelle est encore aujourd'hui relativement peu importante. Jusqu'à récemment, on constate que, comme pour l'enquête criminelle, la littérature a surtout proposé des recueils de bonnes pratiques et d'expériences dans lesquels une technique avait donné de bons résultats<sup>154</sup>.

Au tournant du XXI<sup>e</sup> siècle, le rôle assigné initialement à l'analyse criminelle dans le monde policier a quelque peu changé et la notion d'*Intelligence-led Policing*<sup>155</sup> a fait son apparition. Depuis quelques années, l'application des méthodes issues de l'analyse criminelle (*Criminal Analysis*) en sa qualité d'auxiliaire dans les enquêtes de police, a démontré son efficacité et elle a atteint le niveau managérial. Ainsi, une fois que l'activité d'analyse permanente du renseignement fait explicitement partie des activités déployées par la police, on parle de renseignement criminel (*Criminal Intelligence*). Enfin, si ce renseignement est utilisé pour guider les activités policières, on aboutit au concept d'*Intelligence-led Policing*. LEMIEUX<sup>156</sup> décrit cette évolution récente au sein de certaines organisations policières en ces termes :

« Certes la collecte et l'analyse des informations relatives à la perpétration d'un crime ne sont pas des activités récentes dans l'histoire de la police. Aussi loin que l'on puisse remonter, la recherche d'indices, le recueil des témoignages, l'utilisation d'informateurs et la formulation d'hypothèses ont toujours caractérisé la démarche du détective. Cependant au cours des deux dernières décennies, le modèle de l'Intelligence-led Policing (ILP) est venu formaliser le recours aux renseignements au sein des services policiers afin de répondre à des considérations économiques, organisationnelles, politiques et technologiques. » (p.1)

La littérature s'est aujourd'hui étoffée sous l'angle des activités policières guidées par le renseignement criminel comme en témoigne la part importante qui lui est réservée dans le « Traité de sécurité intérieure » de CUSSON, DUPONT et LEMIEUX<sup>157</sup>.

Nous souhaitons toutefois nous concentrer ici sur l'activité d'analyse dans le contexte criminel (analyse criminelle), procédé qui aboutit à la production du renseignement désormais aussi utilisé par le management des organisations policières et qui tire essentiellement ses origines du domaine militaire et du renseignement de sécurité. Comme le relève encore LEMIEUX<sup>158</sup> : « *Bien que les*

---

<sup>154</sup> Voir notamment : GOTTLIB *et al.*, *Crime Analysis: From first report to final arrest*, 1994; ANDREWS & PETERSON, *Criminal Intelligence Analysis*, 1990; PETERSON, *Application in Criminal Analysis. A Source Book*, 1994; PETERSON *et al.*, *Intelligence 2000 : Revising the Basic Elements*, 2000

<sup>155</sup> *Intelligence-led Policing* peut être traduit par *les activités policières guidées par le renseignement*

<sup>156</sup> LEMIEUX, *Normes et pratiques en matière de renseignement criminel – une comparaison internationale*, 2006

<sup>157</sup> CUSSON, DUPONT, LEMIEUX, *Traité de sécurité intérieure*, 2008

<sup>158</sup> LEMIEUX, *op.cit.*, 2006

*travaux de GODFREY et HARRIS<sup>159</sup> et de HARRIS<sup>160</sup> aient permis d'initier les services de police aux rudiments du processus cyclique de production de renseignement, l'application procédurale de cette activité a longtemps été rattachée à un discours plus rhétorique que pragmatique* » (p.5).

Nous nous attacherons donc dans ce chapitre d'une part à insister sur ce point précis qui est la production de renseignement, étape qui, si elle n'est pas maîtrisée réduit à néant toute la bonne volonté affichée par une activité policière guidée par le renseignement et d'autre part nous tenterons de montrer que l'activité de renseignement nécessite que le processus soit modélisé de bout en bout en tenant compte de contraintes apparaissant à différents niveaux, et qui ne sont pas toujours aisées à lever.

### 1.4.1 Définitions

Dans les années 1990, lors de l'expansion de l'analyse criminelle dans le monde entier, de nombreuses définitions ont été proposées par divers auteurs. Le groupe de travail sur l'analyse criminelle d'INTERPOL<sup>161</sup> définit l'analyse criminelle dans ces termes :

« L'analyse criminelle consiste en la recherche et la mise en évidence méthodiques de relations - d'une part entre les données de la criminalité elles-mêmes et, d'autre part entre des données de la criminalité et d'autres données significatives possibles - à des fins de pratiques judiciaires et policières. »

Nous lui préférons toutefois la définition suivante, donnée par RIBAU<sup>162</sup> et qui se distancie du terme de *relation* à notre sens trop réducteur et qui introduit la notion de *renseignement* :

« L'analyse criminelle recouvre l'ensemble des méthodes et des techniques qui permettent de gérer des informations et de produire des renseignements à des fins de sécurité, en particulier de pratiques judiciaires et policières. »

### 1.4.2 Origines de l'analyse criminelle

Des efforts de standardisation des méthodes et de gestion des informations furent entrepris par les services de renseignements des grandes puissances durant les deux guerres mondiales du XX<sup>e</sup> siècle. Mais, ce n'est que dans les années 1960 que ces idées de base refont surface dans le contexte judiciaire aux Etats-Unis par la commission présidentielle sur le crime organisé qui débouche sur le renseignement criminel. Dans les faits, les organisations policières étaient incapables de souscrire aux exigences procédurales et de produire des preuves d'une qualité suffisante pour obtenir des

---

<sup>159</sup> GODFREY & HARRIS, *The Basic Elements of Intelligence*, 1971

<sup>160</sup> HARRIS, *Basic Elements of Intelligence- Revised*, 1976

<sup>161</sup> INTERPOL, *Guide sur l'analyse criminelle*, 1997

<sup>162</sup> RIBAU<sup>et al.</sup>, *L'analyse criminelle face à la complexité des données*, 2002

condamnations en vertu de la nouvelle loi RICO<sup>163</sup> (*Racketeering Influenced and Corrupted Organisation*).

En 1971, un ouvrage de référence *Basic Elements of Intelligence* écrit par GODEFREY et HARRIS jettera la base de l'analyse criminelle.

Bien que les notions de base, en particulier sur la production du renseignement, aient été décrites à cette époque, elles n'ont pu se développer vraiment au sein des organismes policiers que grâce aux nouvelles technologies de l'information. Grâce à elles, l'efficacité des méthodes a pu être très nettement augmentée et l'intérêt a logiquement grandi. L'informatisation des fichiers qui servent à gérer des éléments techniques (empreintes digitales, ADN) ou des événements circonstanciels (casier judiciaire, dossiers de police) constitue autant d'exemples de ce développement technologique. Cette informatisation s'est faite, on l'a vu, non sans heurts.

En Suisse, l'analyse criminelle, reconnue sous cette dénomination, ne fait son apparition dans les corps de police qu'au milieu des années 1990, comme dans de nombreux pays européens suite aux efforts d'INTERPOL. Il s'agissait alors d'une volonté des offices centraux de police criminelle de fournir aux corps de police des outils adaptés à l'évolution de la criminalité organisée intercantonale et transnationale à l'instar de ce qui fut entrepris Etats-Unis à la fin des années 1960.

Parallèlement, de véritables stratégies de renseignement criminel se mettent petit à petit en place, comme en témoigne le travail effectué au sein de la coordination judiciaire vaudoise par RIBAU<sup>164</sup> et devant déboucher aujourd'hui sur un véritable guidage des activités de police par le renseignement.

### **1.4.3 Cadre de l'analyse criminelle**

Précurseur en Suisse, RIBAU nous rappelle que l'analyse criminelle est délimitée par des cadres qui lui imposent des contraintes de différents types :

- La politique criminelle est définie par les pouvoirs exécutif et législatif. Elle donne les stratégies générales et les priorités, que ce soit au niveau fédéral ou cantonal.
- Les règles légales régissent tout système judiciaire. Elles définissent les infractions et les procédures, notamment pour recueillir, stocker et exploiter certains types d'informations.
- Les contraintes économiques influent sur les moyens qui sont donnés aux organisations pour remplir leur mission.
- Les organisations régissent les contraintes structurelles et organisationnelles dans lesquelles les méthodes seront appliquées.

---

<sup>163</sup> Pour un historique de cette loi : WHEATLEY, Contre le crime organisé aux Etats-Unis : le RICO, 2009

<sup>164</sup> RIBAU, La recherche et la gestion des liens dans l'investigation criminelle : le cas particulier du cambriolage, 1997

- Les méthodes de travail déterminent de quelle manière le travail doit être accompli (selon quel processus) et avec quels outils.
- Les outils informatisés servent à appliquer les méthodes et doivent dans l'idéal se trouver en bout de la chaîne de réflexion et pas avant.

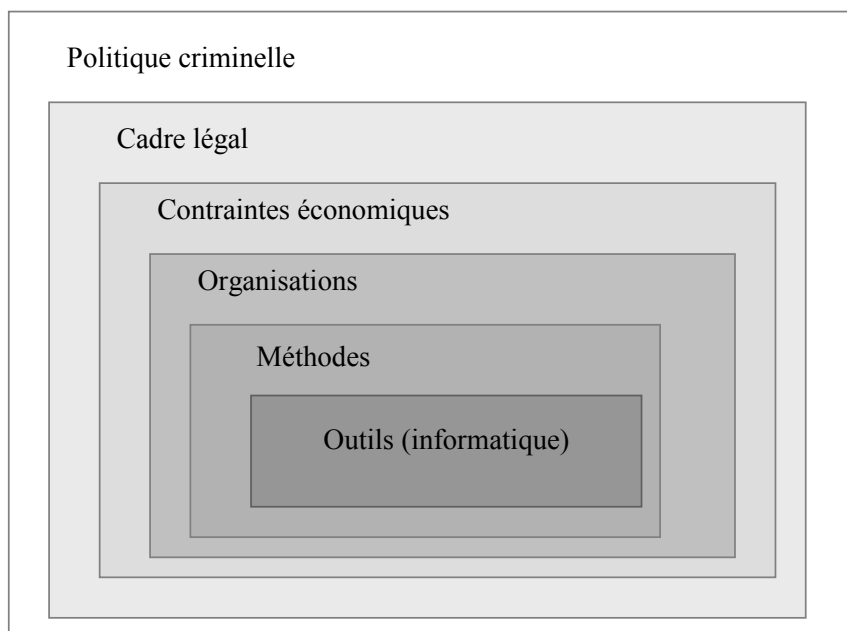


fig. 19 : Cadres des contraintes de l'analyse criminelle<sup>165</sup>

Ces contraintes, dans leur ensemble, concernent un très grand nombre de personnes qui ont des champs d'activités et de connaissances très variés. La conciliation des intérêts de tous ces participants est une tâche très ardue. Et comme il se doit en Suisse, il est d'usage de faire des compromis. Seule une solution qui tient compte de l'ensemble de ces contraintes peut amener une plus-value et a une chance de succès sur le long terme.

La démarche entreprise par les offices centraux de police criminelle dans les années 1990, qui n'a consisté qu'à fournir des outils et à former des spécialistes à leur utilisation, a longtemps contribué à masquer les réelles implications de l'usage de l'analyse criminelle et de la portée des réformes réellement nécessaires à son intégration dans le contexte de la poursuite pénale en Suisse.

#### 1.4.4 Champ d'application de l'analyse criminelle

La définition très peu restrictive de l'analyse criminelle lui laisse un très large champ d'application, qui se subdivise en deux catégories reconnues et définies en ces termes par le GTAC<sup>166</sup>:

L'analyse stratégique qui est axée sur le suivi et la prévention de l'évolution de la criminalité à une échelle géographique donnée et à moyen ou à long terme.

<sup>165</sup> Figure tirée de RIBAUX *et al.*, *op. cit.*, 2002

<sup>166</sup> INTERPOL, *op. cit.*, 1997

L'analyse opérationnelle (et tactique<sup>167</sup>), qui a un objectif de répression à court terme assorti d'un résultat immédiat, par exemple une arrestation, une confiscation ou une saisie.

Ces deux catégories principales s'étendent à tout le catalogue des infractions poursuivies par le système judiciaire. D'une part, des études stratégiques sont nécessaires par rapport à de grands phénomènes criminels tels que le trafic de stupéfiants, l'implantation du crime organisé, les groupes de cambrioleurs itinérants, ou encore des réseaux internationaux d'escrocs ; et d'autre part, les enquêtes menées contre les auteurs des infractions relatives aux phénomènes décrits plus avant nécessitent des analyses opérationnelles. Les formes que peuvent revêtir l'analyse criminelle sont donc extrêmement variées.

Le GTAC propose une classification des différentes formes d'analyses, en fonction du but recherché (opérationnelles ou stratégiques) et du sujet de l'étude (délit, auteur ou méthode). Le tableau suivant résume ces différentes formes telles qu'elles ont été identifiées :

	Stratégique	Opérationnelle
Infraction	Analyse de phénomène de la criminalité	Analyse de cas Analyse comparative de cas
Auteur	Analyse de profil général	Analyse de groupe d'auteurs Analyse de profil spécifique
Méthode	Analyse de méthode générale	Analyse d'enquête

fig. 20 : Formes de l'analyse criminelle <sup>168</sup>

*Analyse de phénomène de la criminalité:*

Il s'agit de l'étude de la nature, de l'ampleur et du développement de la criminalité ou de certaines formes de criminalité dans une zone géographique et au cours d'une période donnée, ayant pour but la définition de la politique préventive, de priorités dans la recherche, ou de répartition de moyens.

<sup>167</sup> Selon RIBAUX et TOURNIE, une notion supplémentaire doit être définie. Il s'agit de l'analyse tactique, notion intermédiaire qui consiste en des processus de surveillance en fonction des risques identifiés et ayant pour but d'anticiper les problèmes de sécurité. *In* Le renseignement et l'analyse criminels – Application à la lutte contre le crime économique et financier, à paraître dans : Les meilleures pratiques en analyse financière criminelle.

<sup>168</sup> INTERPOL, *op. cit.*, 1997. Cette classification est un peu démodée, mais elle n'a pas été remise à jour par INTERPOL depuis sa publication.

*Analyse de profil général:*

L'étude des caractéristiques communes aux individus ayant commis le même type d'infraction constitue ce travail criminologique. Par exemple, des études de profil sur des cas connus, en vue de déterminer les traits psychologiques ou comportementaux caractéristiques de délinquants.

*Analyse de méthode générale:*

Cette analyse stratégique consiste à évaluer une méthode de répression appliquée dans plusieurs affaires en vue de définir les meilleures pratiques pour des affaires à venir ; par exemple, la comparaison des opérations mises en œuvre pour limiter globalement le trafic de stupéfiants de rue.

*Analyse de cas:*

Cette notion consiste en la reconstitution de la genèse et du déroulement d'une infraction précise, afin de déterminer l'enchaînement des événements et les caractéristiques des agissements, en vue d'obtenir des indications sur la direction dans laquelle il conviendrait d'orienter les recherches, ou de déceler les incohérences parmi les informations provenant de différentes sources.

*Analyse comparative de cas:*

Cette analyse opérationnelle est produite par la comparaison des informations relatives à des infractions présentant des similitudes, dans le but de découvrir si certaines de ces infractions ont pu être commises et/ou organisées par le ou les mêmes individus. Le travail de coordination dans le domaine des délits sériels contre le patrimoine en est le parfait exemple, et constitue une spécialisation à part entière<sup>169</sup>. Un travail systématique et permanent de ce type d'analyse entre dans la nouvelle catégorie générale de l'analyse tactique telle que décrite précédemment.

*Analyse de groupe d'auteurs:*

Cela consiste à organiser les informations dont on dispose sur un certain groupe de malfaiteurs afin de comprendre la structure du groupe et le rôle de chaque individu, société, etc. dans ce groupe ; par exemple, les réseaux de criminalité en bande ou organisée.

*Analyse de profil spécifique:*

Il s'agit d'établir le profil du ou des auteurs d'une infraction précise d'après les caractéristiques de l'affaire et des autres informations comportementales de l'auteur ; par exemple, dans le cas d'agressions violentes à caractère sexuel.

*Analyse d'enquête:*

Cette forme d'analyse consiste en l'évaluation des tâches opérationnelles qui ont été accomplies au cours d'une enquête particulière dans le but de faire progresser les méthodes de travail.

---

<sup>169</sup> RIBAUD, *op. cit.*, 1997

## 1.4.5 Méthodes de travail

### 1.4.5.1 Le cycle du renseignement

Le mot clé lorsque l'on parle d'analyse criminelle, est processus. Dans l'ouvrage de référence<sup>170</sup> édité par l'IALEIA<sup>171</sup> en 2000, MOREHOUSE dans son introduction reprend HARRIS dans ces termes :

« What is criminal intelligence ?

Criminal intelligence conjures up a variety of meanings, depending on who is asked. Intelligence can mean the information collected or a specific function. However, it is generally conceded that intelligence consists of pieces of raw information that when collected, evaluated, collated, and analysed from meaningful and useful judgments that are both accurate and timely. Taking this raw information and turning it into intelligence requires a sequential process. The following depicts the step-by-step process described by Harris:

Collection → Collation → Evaluation → Analysis → Dissemination → Re-Evaluation »

(p. 7)

Ce processus appelé communément le *cycle du renseignement* en français est souvent représenté dans les ouvrages d'analyse criminelle, nous reproduisons et traduisons ici la version qui figure sur la couverture de l'ouvrage de PETERSON susmentionné.

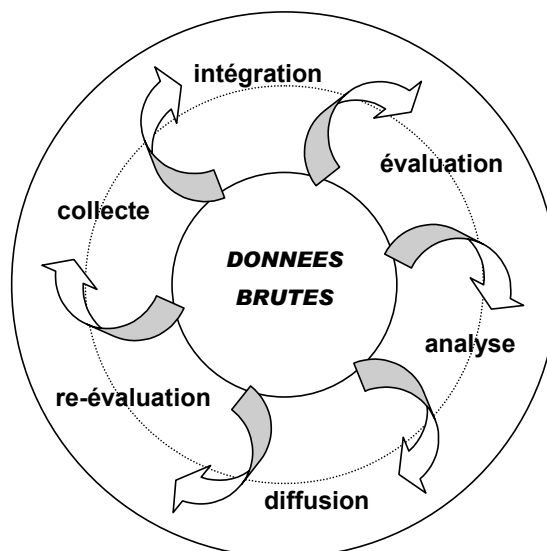


fig. 21 : Cycle du renseignement

Le processus du cycle du renseignement est, selon une approche holistique, un modèle de système d'apprentissage ouvert qui contient une boucle de rétroaction, simple ou double, suivant qu'elle

---

<sup>170</sup> PETERSON *et al*, Intelligence 2000 : Revising the Basic Elements, 2000



s'applique à une ou plusieurs des phases du processus. Il représente un schéma systématique dont la matière traitée (l'information) évolue par apprentissages successifs.

### 1.4.5.2 Raisonnements

Tout au long du cycle du renseignement et plus particulièrement dans la phase d'analyse, le praticien est amené à raisonner, soit à faire des inférences et *a fortiori* à combiner ses inférences. L'inférence est une étape du raisonnement, entendu comme activité, soit définie comme une opération discursive par laquelle on passe de certaines propositions à une proposition nouvelle. Cette inférence est l'opération par laquelle est acceptée une proposition dont la vérité n'est pas admise directement, mais en vertu de sa liaison avec d'autres propositions. La science du raisonnement en lui-même est ce qu'on définit généralement comme la Logique.

La Logique a été la préoccupation de nombreux philosophes de l'Antiquité à nos jours. L'analyste criminel en fait usage pour expliciter le polymorphisme du raisonnement qui sera intimement lié aux différentes phases de l'analyse.

Une division traditionnelle répartit les raisonnements en deux groupes complémentaires, opposés par le sens de leur démarche : la *déduction* et l'*induction*. La déduction repose sur un raisonnement direct et progressif qui va « du général au particulier », ou du *principe* à la *conclusion*. L'induction, au contraire régressive, va « du particulier au général », c'est-à-dire qu'il se base sur les *conséquences (conclusion)* pour énoncer un *principe*, ou des *effets* à la *cause*, du *présent* au *passé*.

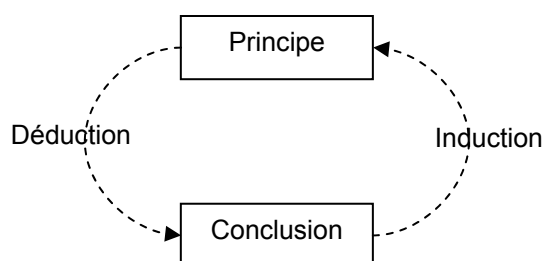


fig. 22 : Division traditionnelle des raisonnements<sup>172</sup>

L'induction a souvent posé problème aux philosophes qui n'y voyaient pas un raisonnement démonstratif, bien que BACON<sup>173</sup> ait vu dans l'induction la méthode par excellence des sciences

<sup>171</sup> International Association of Law Enforcement Intelligence Analysts

<sup>172</sup> Tiré du support de cours de Jean-Marc GINOUX, « Histoire des Sciences / Epistémologie », Université du Sud Toulon – Var, 2005.

<sup>173</sup> Francis BACON (1561-1626), homme d'État et philosophe anglais est un des pionniers de la pensée scientifique moderne. Il est le père de l'*empirisme* et auteur du *Novum Organum* dans lequel il écrit que la connaissance nous vient sous forme d'objets de la nature, mais que l'on impose nos propres interprétations sur ces objets. D'après lui, nos théories scientifiques sont construites en fonction de la façon dont nous voyons les objets ; l'être humain est donc biaisé dans sa déclaration d'hypothèses.

expérimentales. GINOUX<sup>174</sup> précise que : « *s'il était juste de maintenir comme fondamentale, la division des raisonnements en rigoureux et non rigoureux*<sup>175</sup>, on ne pouvait la faire coïncider avec le couple déduction-induction qu'en élargissant de façon fâcheuse le sens de ce dernier mot.

*Mieux valait sans doute conserver pour lui le sens traditionnel, déjà suffisamment ambigu, et adopter un troisième terme pour désigner les raisonnements non rigoureux qui ne sont ni des généralisations de l'expérience ni des anticipations d'une loi. D'où une division ternaire ».*

PIERCE<sup>176</sup> répartit les raisonnements élémentaires en trois classes : *déduction*, *induction* et *abduction*, dans laquelle il s'agit de donner une raison plausible à une observation et une loi coïncidant avec elle. Mais comme le précise POLITZER<sup>177</sup>, il va plus loin que ce sens restreint, classique :

« De cette première conception, dans laquelle l'activité est limitée à la recherche d'une loi dans une base de données, Pierce est passé à une autre conception de l'abduction, plus féconde, qui consiste en l'élaboration d'une explication (ce qui peut inclure une activité créatrice) à partir de laquelle ultérieurement on va inférer déductivement une hypothèse, qui sera alors à son tour soumise à un test constituant l'étape inductive au sens particulier de cette conceptualisation : on a donc une séquence triangulaire réitérable, l'ensemble décrivant la démarche scientifique. » (p.21)

GINOUX<sup>178</sup> reprend l'illustration classique des trois formes de raisonnements fondamentaux en les appliquant au syllogisme aristotélicien :

« Dans cette forme élémentaire et exemplaire de déduction qu'est le syllogisme, et plus précisément celui de la première figure, on voit qu'un tel syllogisme raisonne à partir d'une règle (majeure) et de la subsomption d'un cas (mineure) pour obtenir (conclusion) le résultat de cette règle dans ce cas. Par exemple :

Règle : Tous les haricots de ce sac sont blancs

Cas : Ces haricots sont tirés de ce sac.

Résultat : Ces haricots sont blancs.

Dans l'induction, on aboutit à la règle en partant d'un cas et d'un résultat :

---

<sup>174</sup> GINOUX, *op. cit.*, 2005

<sup>175</sup> Entendre ici les raisonnements « *rigoureux / non rigoureux* » comme « *démonstratifs / non démonstratifs* », que l'on retrouve également dans la littérature.

<sup>176</sup> Charles Sanders PIERCE (1839 - 1914) sémiologue et philosophe américain.

<sup>177</sup> POLITZER, *Le raisonnement humain*, 2002

<sup>178</sup> GINOUX, *op. cit.*, 2005

Cas : Ces haricots sont tirés de ce sac.  
 Résultat : Ces haricots sont blancs.  
 Règle : Tous les haricots de ce sac sont blancs

Enfin, dans l'abduction, que Pierce appelle aussi hypothèse, on aboutit au cas en partant de la règle et d'un résultat :

Règle : Tous les haricots de ce sac sont blancs  
 Résultat : Ces haricots sont blancs.  
 Cas : Ces haricots sont tirés de ce sac.

Ailleurs, Pierce présente ainsi son système ternaire, en l'accordant à la hiérarchie des modalités :

la déduction prouve que quelque chose doit être,  
 l'induction montre que quelque chose est effectivement,  
 l'abduction suggère que quelque chose pourrait être. »

Ces trois raisonnements fondamentaux, soit la déduction, l'induction et l'abduction, sont des raisonnements qui, pratiqués en séquence selon le contexte, participent au polymorphisme du raisonnement humain<sup>179</sup>.

#### Raisonnements dits « non démonstratifs » ou probables

Un élément qu'il est particulièrement important d'intégrer lorsque l'on pratique l'analyse criminelle est l'évolution que subissent les données qui nous parviennent tout au long du processus de renseignement. Durant ce processus cyclique, itératif et continu, les différents types de raisonnements vont être utiles et utilisés. A l'instar de Sherlock Holmes, les analystes font très souvent appels à des raisonnements non démonstratifs, qu'ils se doivent de maîtriser afin d'être en mesure de justifier leurs allégations. A l'inverse de la déduction qui démontre qu'une telle *cause* a eu tel *effet*, l'analyste criminel va donc très souvent employer le cheminement récursif contraire, soit de déterminer la *cause* en constatant les *effets*, par induction. Ou alors, il procède par abduction, processus qui n'est ni totalement progressif, ni entièrement récursif. Dans ce cas, l'analyste propose une *hypothèse* en connaissant un *principe (cause)* et une *conséquence (effets)*, alors que cette *conséquence* peut avoir une toute autre *cause*.

En appliquant l'illustration de GINOUX ci-dessus et en lui appliquant un contexte plus proche de l'analyste, on peut peut-être apprécier ces différents types de raisonnements plus aisément :

---

<sup>179</sup> Pour approfondir cette matière, voir par exemple GEORGE Ch., Polymorphisme du raisonnement humain – Une approche de la flexibilité de l'activité inférentielle, 1997 et PIERCE C.S., Le raisonnement et la logique des choses, 1995

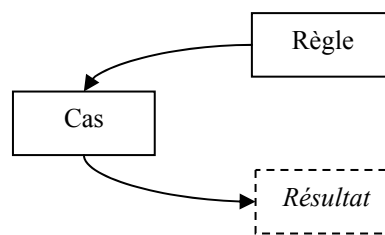
### Déduction

Règle : Tous les braqueurs sont armés

Cas : Toto est un braqueur.

Résultat : *Toto est armé.*

(démonstratif)



Ici, on connaît la règle qui stipule que tous les braqueurs sont armés et on est en présence d'un individu (Toto) qui est un braqueur. On peut donc prédire *avec certitude* (on en déduit) que Toto est armé.

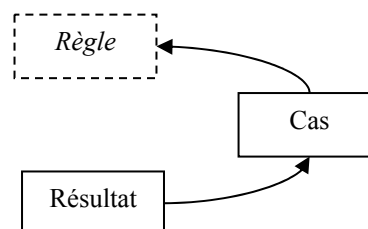
### Induction

Cas : Toto est un braqueur.

Résultat : Toto est armé.

Règle : *Tous les braqueurs sont armés*

(non démonstratif ou probable)



Confronté à un, ici Toto, (ou plusieurs *n*) braqueur(s) armé(s), l'analyste sera tenté de généraliser sa (ou ses *n*) constatation(s) en établissant une règle qui propose que tous les braqueurs sont armés. La validité ou la qualité de cette règle dépend bien évidemment du nombre de cas rencontrés. Dans certains cas, on peut même empiriquement calculer une probabilité.

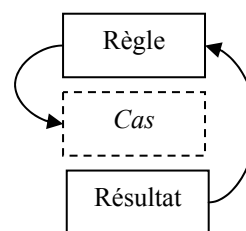
### Abduction (classique)<sup>180</sup>

Règle : Tous les braqueurs sont armés

Résultat : Toto est armé.

Cas : *Toto est un braqueur.*

(non démonstratif ou probable)



Constatant qu'un individu est armé (Toto), le policier (ou l'analyste) pour déterminer dans quelle situation il se trouve, fait appel à une règle de sa connaissance, soit que tous les braqueurs sont armés. Il fera donc l'hypothèse qu'il est potentiellement en présence d'un braqueur (Toto).

Cependant, si l'on s'en tient à ce dernier exemple classique d'abduction, il existe bien d'autres règles qui peuvent amener au même résultat. Par exemple : *Tous les policiers sont armés*. Ce qui aurait pour conséquence une réaction toute différente. Idéalement, il est nécessaire d'élaborer un nombre maximum d'hypothèses, mais bien souvent et instinctivement, le choix se porte sur celle

<sup>180</sup> Aussi appelée « hypothèse », « rétroduction » ou « présomption », cf. GEORGE Ch., *op. cit.*, 1997, p.114

qui est la plus dangereuse ou qui comporte le plus grand risque, et, toujours dans le cas idéal, de pouvoir les tester. On se trouve alors dans cette forme plus élaborée de raisonnement énoncé par PIERCE et décrivant la démarche scientifique et communément appelée la méthode hypothético-déductive, que CRISPINO<sup>181</sup> nous décrit en ces termes :

« La méthode hypothético-déductive, raisonnement mêlant abduction et déduction éventuellement issue d'une expérimentation inductive, semble alors la meilleure solution pour déterminer le maximum d'hypothèses plausibles concernant la source de l'objet, sans être assuré avoir embrassé toutes les hypothèses possibles. » (p.19)

Relevons à ce stade un dernier point, sans nous prononcer sur la *scientificité*<sup>182</sup> des inductions qui sont faites par les praticiens au stade de l'analyse des informations, on s'applique pratiquement à tenter de réfuter des hypothèses plutôt qu'à les confirmer selon la démarche des *conjectures et de réfutations* de POPPER<sup>183</sup> qui permet de faire croître les *connaissances scientifiques*. Ainsi, on peut lire dans BERNIER<sup>184</sup> :

« Aussi une motivation centrale de l'Approche de Popper est d'insister sur l'aspect ouvert et critique de la recherche scientifique, sur l'aspect sceptique, dans le bon sens du terme, de l'attitude scientifique qui nous dispose à réviser certaines de nos assertions à la lumière de la critique rationnelle. La forme la plus évidente que prend l'opposition de Popper au cadre empiriste est son rejet de la confirmation par l'évidence empirique. Cette notion, centrale dans le modèle hypothéticodéductif, sera remplacée par celle de la réfutation. Le principe directeur de la recherche scientifique serait de formuler des conjectures qui sont en principe réfutables par l'expérimentation, et de tenter de les réfuter avec rigueur, honnêteté, et acharnement. » (p.84)

Enfin, nous retiendrons la schématisation proposée par CRISPINO<sup>185</sup> qui représente les trois raisonnements fondamentaux en une forme élémentaire unique :

---

<sup>181</sup> CRISPINO, Le principe de Locard est-il scientifique ? ou analyse de la scientificité des principes fondamentaux de la criminalistique, 2006. *Celui-ci définit en note de bas de page les trois raisonnements fondamentaux cités ici de la sorte : L'abduction, appelée aussi rétroduction, est un raisonnement logique déterminant les conditions ayant permis d'observer un résultat en connaissant la règle générale qui s'applique. La déduction, appelée aussi syllogisme logique, est un raisonnement logique décrivant le résultat à partir d'une règle générale et de conditions données. L'induction, appelée aussi empirisme logique, est un raisonnement logique établissant la règle générale à partir de conditions données ayant permis d'observer un résultat.*

<sup>182</sup> A ce sujet, lire CRISPINO, *op. cit.*, 2006

<sup>183</sup> Karl R. POPPER (1902 – 1994) est l'un des plus influents philosophes des sciences du XX<sup>e</sup> siècle. Lire notamment : La logique de la découverte scientifique, 1973, et Conjectures et réfutations – la croissance du savoir scientifique, 1985.

<sup>184</sup> BERNIER, La normativité du raisonnement non démonstrative, in POLITZER, *op. cit.*, 2002

<sup>185</sup> CRISPINO, Nature and place of crime scene management within forensic sciences, 2008

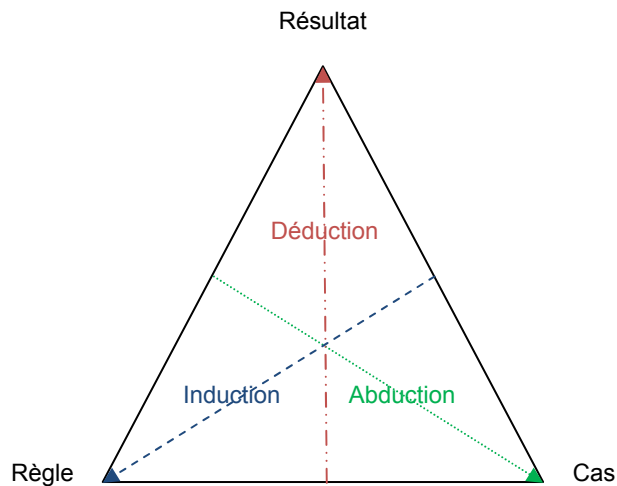


fig. 23 : Schématisation des trois raisonnements fondamentaux

### 1.4.5.3 Décomposition et interprétation des informations

En suivant le cycle du renseignement, durant le processus d'acquisition d'informations, les nouvelles données doivent être intégrées et évaluées par l'investigateur (analyste ou policier). Elles sont alors naturellement confrontées aux informations dont il dispose déjà. Cette interprétation de la signification des nouvelles données, synonyme d'analyse, va lui permettre d'obtenir *in fine* un renseignement.

Il est primordial que l'investigateur soit en mesure de décomposer les informations qui lui sont transmises en données factuelles, afin de pouvoir les recomposer dans le contexte de l'enquête. Chaque pièce élémentaire d'information pouvant avoir une influence particulière sur l'ensemble. Les données factuelles sont les pièces élémentaires qui nous sont transmises. Ces données sont généralement grammaticalement et sémantiquement structurées de sorte qu'elles contiennent un message informatif (ce qui nous est effectivement transmis). Ces informations doivent être décomposées, confrontées et recomposées avec les éléments connus *a priori*, pour qu'elles puissent être interprétées en fonction du contexte préalable. L'interprétation des données est l'étape d'analyse qui fournit alors un, ou parfois plusieurs renseignements.

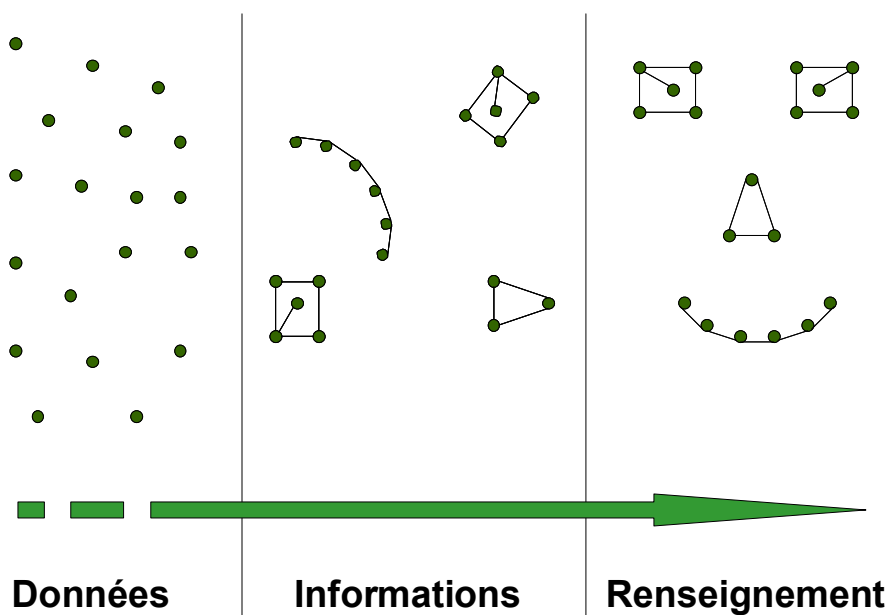


fig. 24 : Données – Informations - Renseignement

Cette transformation des données en informations, puis en renseignements, peut être illustrée par l'exemple suivant :

Une personne gagne à un concours et reçoit chez elle un carton. Sur celui-ci ne figure aucune indication. A l'intérieur, se trouve un certain nombre d'éléments disjoints (ce sont les données brutes) ainsi qu'un plan de montage, qui indique, par étapes, de quelle manière les éléments doivent être fixés les uns aux autres (chaque étape est une information). Jusqu'ici, la personne raisonne par déduction, le plan de montage ne devant pas être ambigu. Par ailleurs, s'il manque des pièces, le gagnant du prix va le remarquer et va tout faire pour les obtenir. Et c'est lors de l'assemblage des différentes pièces qu'il est le plus aisé de se rendre compte de la qualité de ce qui est transmis (il en est de même dans les enquêtes criminelles).

Enfin, une fois les pièces assemblées selon les informations du plan de montage (ou les informations synthétisées), l'objet offert sera prêt à être utilisé. A cet instant, le gagnant du concours identifie l'objet qu'il a reçu et se demande à quoi il sert et à quoi il pourra bien lui être utile. Les raisonnements qu'il utilise à cet instant sont principalement « non démonstratifs ». Par exemple, il peut comparer les informations à disposition à ses connaissances au sens large, soit à son expérience (de vie), et s'il a déjà rencontré un objet ressemblant ou qui lui a été utile en telle ou telle situation, en tirer un renseignement en généralisant (induction) son emploi et en anticipant un résultat futur, ou s'il ne connaît pas son utilisation, il va imaginer dans quelles situations ces informations sont valables, en produisant un renseignement sous la forme d'une ou plusieurs hypothèses (abduction). Dès cet instant apparaît une subjectivité certaine. Le renseignement tiré découle de l'interprétation de la personne qui le fournit.

L'interprétation d'une somme d'informations peut donc mener à des résultats différents, voire contradictoires, comme le caricature le schéma suivant :

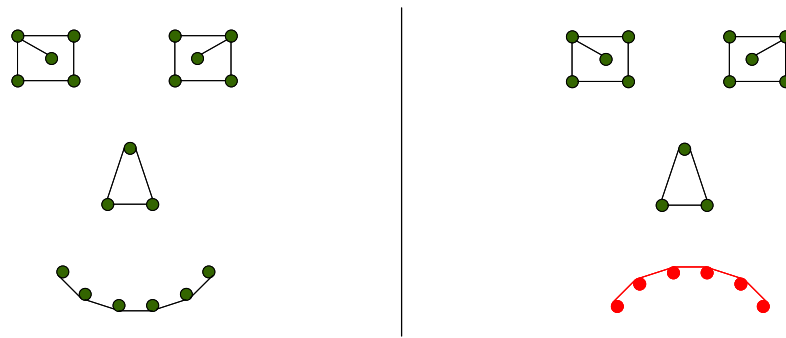


fig. 25 : Développement d'hypothèses différentes, voire contradictoires

La subjectivité des interprétations entraîne que différents individus ne vont pas forcément arriver au même résultat. Dans certains cas, une solution peut paraître évidente, car elle correspond à des expériences communes qui sont partagées par de nombreuses personnes (intersubjectivité). Mais, il ne faut en général pas s'en tenir à cet unique renseignement. Un analyste attentif devra aussi rechercher des solutions nouvelles, même si elles paraissent justement moins probables que l'hypothèse la plus communément partagée.

Comme le montre la figure ci-dessus, d'autres renseignements peuvent être tirés des mêmes informations. Et ce n'est pas une faute que d'arriver à des renseignements différents lorsqu'on se trouve dans la frange des raisonnements « non démonstratifs » ou probables. C'est justement la valeur ajoutée de l'étape *subjective* du cycle du renseignement. Il s'agit pour l'analyste de rechercher, souvent par abduction, justement ce que les informations peuvent signifier lorsqu'elles sont mises en regard de ce qui est déjà connu ou de ce qui reste à découvrir, en tenant compte de la qualité relative des informations. Le développement d'hypothèses différentes, voire contradictoires, doit pousser l'investigateur à agir. Il va falloir comme le dit le jargon policier « fermer des portes », en testant une à une les hypothèses et en éliminant celles qui ont pu être infirmées, comme le ferait un scientifique qui teste ses théories<sup>186</sup>. Ce n'est qu'une fois que tous les éléments qu'il était possible de recueillir l'ont été et que l'image de la situation aura évolué par itération que la synthèse générale de toutes ces informations pourra être entreprise, basée sur des raisonnements dits *démonstratifs*, en vue de la poursuite du processus judiciaire.

C'est justement là que la différence entre synthèse et analyse est intéressante, car il s'agit comme pour la différenciation entre la *déduction* et l'*induction* de démarches opposées, mais complémentaires. La relation illative peut être parcourue dans les deux sens :

<sup>186</sup> Voir ci-avant méthode hypothético-déductive.



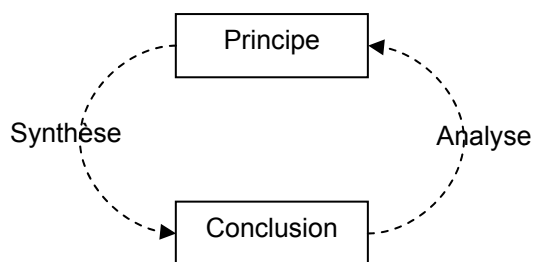


fig. 26 : Division traditionnelle des raisonnements<sup>187</sup>

On voit que *l'analyse* ainsi conçue n'est pas une action qui cherche à structurer des *preuves*, mais qu'elle apparaît bien, par rapport à la *synthèse* démonstrative, comme un mouvement inverse, qui se doit d'énoncer des *principes* hypothétiques en regard du résultat observé.

On doit encore admettre que les raisonnements abductifs et par extension la démarche hypothético-déductive soient rattachés à *l'analyse* et non à la *synthèse*, à cause de leur nature intrinsèque probabiliste et subjective donc *non-rigoureuse*, bien qu'ils soient partiellement démonstratifs. En effet, comme le dit GEORGE<sup>188</sup> :

« Dans le raisonnement abductif courant, les informations disponibles ne sont pas équivalentes à deux prémisses, le « résultat » à expliquer et la « règle », mais à une seule : le « résultat » étant connu, il faut faire des hypothèses sur la « règle » pour inférer le « cas ». Il faut donc compléter les prémisses avant de formuler une conclusion constituant l'explication d'un fait, contrairement aux arguments déductifs dont les prémisses sont d'emblée complètes. » (p.114)

Ce qui nous permet pour être tout à fait complet de proposer la schématisation suivante :

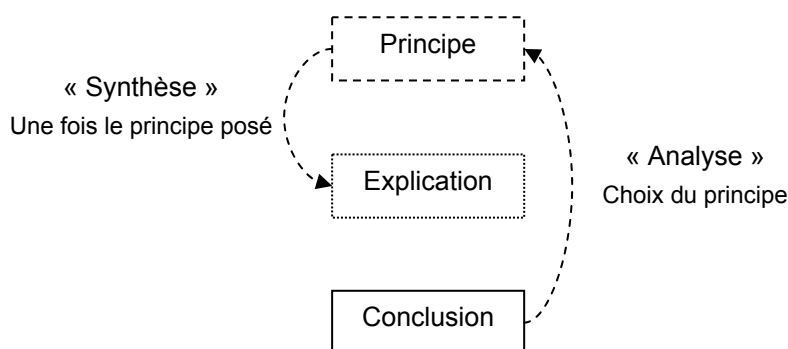


fig. 27 : Processus en jeu dans l'abduction

<sup>187</sup> Tiré du support de cours de Jean-Marc GINOUX, *op. cit.*, 2005.

<sup>188</sup> GEORGE, *op. cit.*, 1997

Il existe encore bien d'autres formes de raisonnements qui sont souvent qualifiés de « type inductif » de par leur conclusion probable (raisonnements dont la conclusion n'est que probable), mais il n'est pas possible de les discuter tous ici. Mentionnons simplement qu'il ne sera pas rare de rencontrer des raisonnements *par analogie*, qui peuvent revêtir la forme d'un raisonnement démonstratif lorsqu'ils prennent la forme d'une proportionnalité (mathématique), ou pas « *lorsqu'ils ne désignent plus qu'une certaine ressemblance entre des choses ou des qualités, qui, par ailleurs, diffèrent* »<sup>189</sup>, par exemple l'analogie entre la foudre et une étincelle électrique.

Dans d'autres situations, on peut être amené à rencontrer des raisonnements *séméiologiques* ou *du fait au fait*, qui consistent à conclure un fait d'un autre qui en est le signe, sans passer par un principe. « *On y retrouve les deux formes, régressive ou progressive, selon que l'on remonte de l'effet (signe révélateur) à la cause (reconstruction de l'historien ou du policier, diagnostic du médecin) ou que l'on va de la cause (signe annonciateur) à l'effet (prévision du météorologiste, pronostic, prospective). (...) Un cas complexe de cette première forme est celui où l'on conclut, quelquefois avec une quasi certitude, par une convergence d'indices dont chacun, pris isolément, serait peu convaincant (instruction criminelle, consilience des inductions).* »<sup>190</sup>

Nous ne voulons pas entrer ici plus avant dans le débat philosophique de la Logique, qui a été le centre d'intérêt de nombreux philosophes qui ont consacré tout ou partie de leur vie. Cependant, je ne peux résister à laisser quelques pistes de réflexions pour ceux qui désireraient approfondir ce sujet. GANASCIA<sup>191</sup> qui est l'auteur d'un chapitre dans un ouvrage dédié au *Data Mining*, nous dit ceci dans sa conclusion :

« (...) L'étude des paradoxes soulevés dans la première moitié du XXème siècle pose une question inquiétante : l'horizon de notre travail et nos ambitions sont-ils, dès leur énonciation, condamnés à n'être que des chimères vaines, semblables à celles qui ont motivé les philosophes de l'induction pendant les siècles passés ? Les critères de Nicod sur la limitation des procédures de confirmation et d'infirmité, les paradoxes de Hempel ou de Goodman sont-ils susceptibles d'affecter les travaux poursuivis en apprentissage symbolique ou en analyse de données, sur la classification, la discrimination ou la généralisation ?

Une étude attentive montre que tous ces travaux portent sur des processus incrémentaux dont ils essaient de saisir l'essence : lorsqu'une expérience est vécue, Nicod et Hempel souhaitent comprendre les transformations par lesquelles nos croyances ou les plausibilités de nos connaissances en sont modifiées. Or, dans la formulation contemporaine et technique de l'apprentissage symbolique ou de l'analyse de données, l'incrémentalité n'est presque jamais posée comme un pré requis indispensable à toute induction. Le problème est donc fondamentalement différent, quand bien même, à

---

<sup>189</sup> BLANCHE, in OLERON, Le raisonnement – Que sais-je, 1996.

<sup>190</sup> BLANCHE, in Encyclopedia Universalis, 1996

<sup>191</sup> GANASCIA, Logique et induction : un vieux débat, 2000

certaines égards, il apparaîtrait semblable : d'un côté, il faut, pour le philosophe, comprendre le mécanisme par lequel une accumulation successive d'expériences conduit à la certitude, d'un autre côté, pour les scientifiques contemporains, il s'agit de construire des procédures effectives qui permettent d'inférer des résultats plausibles en conformité avec un ensemble d'exemples formalisés provenant de séries d'expériences plus ou moins lacunaires.

En somme, les limitations intrinsèques de l'induction, sur lesquelles ont pointé les philosophes du XXème siècle, concernent assez peu les scientifiques des sciences de l'information... Bref, les philosophes ne nous donnent aucun prétexte pour cesser notre travail !» (p.30)

#### **1.4.6 Techniques proposées dans le cadre de la criminalité organisée**

D'après la classification du GTAC d'Interpol, le type d'analyse criminelle opérationnelle qui correspond le mieux au travail qui est envisagé ici est l'*analyse de groupe d'auteurs*. Il s'agit donc d'organiser les informations dont on dispose sur un certain groupe de personnes physiques ou morales afin de comprendre la structure du groupe et le rôle de chacun.

Nous avons donc posé le cadre, mais il reste encore à savoir quelles sont précisément les techniques que nous allons utiliser pour mener à bien nos analyses. PETERSON<sup>192</sup> dénombre plus de 65 « techniques » utilisées couramment en analyse criminelle. Ces techniques passent par des standards d'investigations connues et utilisées quotidiennement par les enquêteurs de police, par des statistiques, par des supports de réunions ou des rapports, mais aussi par des techniques de représentations graphiques.

Dans son catalogue figurent enfin toutes les activités qui peuvent être déployées au sein d'une équipe d'analyse criminelle qu'elle soit stratégique ou opérationnelle.

PETERSON décrit également les besoins spécifiques à la lutte contre la criminalité organisée. Selon elle, l'utilisation de systèmes de renseignement intégrés dans ce contexte est indispensable :

« The final key to organized crime investigation has been the development of intelligence collection and analysis systems. (...) The intelligence process takes all these (*data, information*) and, though analysis, combines them into an overview of the suspect which is often termed an "intelligence product". » (p.125)

Les techniques qui doivent être mises en œuvre lors de l'élaboration de ces produits d'analyse sont entre autres les :

---

<sup>192</sup> PETERSON *et al.*, Applications in criminal analysis – a Sourcebook, 1994

- diagrammes relationnels (*Association Analysis*),
- analyses de contrôles techniques (*Telephone Analysis and Content Used in Electronic Surveillances*),
- analyses financières (*Financial Investigations*) par le biais des :
  - analyses de flux bancaires (*Bank Account Analysis*),
  - activités commerciales (*Business Record Analysis*),
  - analyses économiques (*Economic Analysis*).

Nous ne nous attarderons pas ici sur les analyses financières. Les données financières n'apparaissent dans les systèmes centralisés de la Confédération que de manière partielle. Ces analyses sont encore aujourd'hui du ressort de spécialistes policiers ou civils qui n'utilisent que trop rarement les méthodes de visualisation graphique et de *Data Mining*<sup>193</sup>. La faute en revient aussi pour beaucoup à la pratique en vigueur quant aux supports des données qui sont transmises à la justice, celles-ci n'étant que très rarement sur support digital<sup>194</sup> et le plus souvent sur un simple support papier nécessitant une ressaisie totale.

Pour revenir aux techniques qui doivent selon PETERSON être mises en œuvre dans le processus d'analyse dans le cadre spécifique de la criminalité organisée, nous allons en détailler trois.

- les diagrammes relationnels,
- les analyses de contrôles techniques,
- les diagrammes chronologiques.<sup>195</sup>

Les analyses de contrôles techniques méritent d'être traitées de manière spécifique, bien qu'elles se basent essentiellement pour leur élaboration sur les mécanismes des schémas relationnels ou chronologiques. Elles nécessitent de plus de solides connaissances en télécommunication lors de l'interprétation des données recueillies.

#### **1.4.6.1 Diagrammes relationnels**

Les diagrammes relationnels représentent, comme leur nom l'indique, des relations entre différentes entités, et ceci dans les trois dimensions de l'enquête. On cherche donc à synthétiser les relations entre les personnes et les choses (*qui avec qui ou quoi ?*), les relations des personnes ou des choses

---

<sup>193</sup> Peut-être que le Guide méthodologique et des bonnes pratiques de l'analyse financière criminelle, qui sera prochainement édité par l'UE, fera changer cet état de fait.

<sup>194</sup> Une commission suisse de juristes praticiens (COMINTEL) cherche depuis de nombreuses années à faire changer ces habitudes. Au début 2005, seul *Postfinance* transmet les extraits de compte de ses clients en format digital.

<sup>195</sup> Cette technique n'est pas spécifiquement mentionnée par PETERSON, mais elle est aujourd'hui indissociable des diagrammes relationnels comme on le verra plus loin.

avec les lieux (*qui ou quoi est où ?*) et les relations des personnes avec des événements (*qui a fait quoi et quand ?*).

Le but d'un tel schéma est de représenter des relations de manière graphique en schématisant:

- leur type,
- leur nombre,
- leur sens,
- leur qualité.

Selon CONFUCIUS<sup>196</sup> « *Une image vaut mille mots* ». La plus-value immédiate dépasse la seule quantité d'informations structurées présentée par unité de surface.

Ce type de représentation permet dans un premier temps pour l'analyste :

- d'apprécier l'implication des entités,
- d'obtenir une vue d'ensemble de la situation,
- de repérer les lacunes sur l'état des connaissances et
- d'émettre des hypothèses de travail et ainsi de faire avancer l'enquête.

Dans un second temps, ces représentations graphiques lui permettent :

- de transmettre la masse d'informations d'une manière beaucoup plus réceptive qu'un long texte explicatif,
- de soutenir plus facilement ses arguments qui se basent sur de très nombreux éléments, le cheminement logique pouvant être suivi graphiquement par l'interlocuteur.

A l'origine, alors que l'informatique n'intervenait pas dans l'élaboration de schémas relationnels, les phases de l'élaboration de schémas de relations ont été explicitées dans une méthode développée aux Etats-Unis dans les années 1960. MORRIS<sup>197</sup> reproduit cette méthode originelle. Il est évident qu'à l'heure actuelle, l'utilisation de logiciels spécifiques rend ce travail d'élaboration beaucoup plus simple.

L'élaboration pratique<sup>198</sup> des schémas se faisait en sept phases successives :

---

<sup>196</sup> CONFUCIUS (551 av. J.-C. - 479 av. J.-C.) est le personnage historique ayant le plus marqué la civilisation chinoise. Considéré comme le premier « éducateur » de la Chine, son enseignement a donné naissance au confucianisme.

<sup>197</sup> MORRIS , Crime Analysis Charting, 1993

<sup>198</sup> A l'époque, ces schémas étaient réalisés à la main, au mieux sur une planche à dessin !

1. la collecte des informations,
2. le choix des entités pertinentes,
3. l'élaboration de la matrice relationnelle,
4. l'inscription des codes de relation,
5. la comptabilité des codes de relation,
6. l'établissement du croquis provisoire,
7. la clarification du croquis provisoire.

Nous ne nous étendons pas ici sur la collecte des informations et le choix des entités relevantes, qui sont du travail sur dossier. La matrice relationnelle, par contre était une étape incontournable. Elle consistait à relever les liens entre les entités dans une structure représentant un tableau à double entrée tronqué :

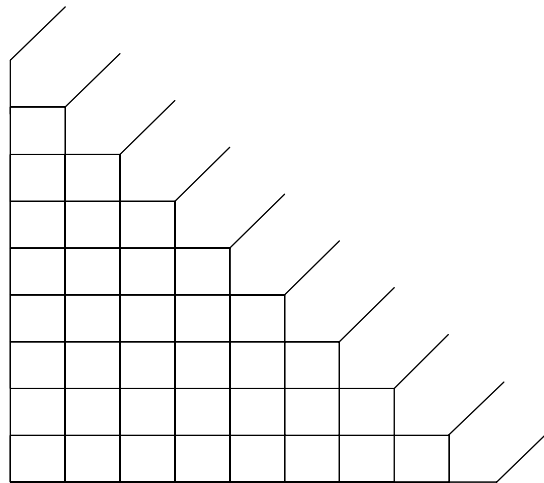


fig. 28 : Squelette d'une matrice relationnelle

Les entités étaient alors ajoutées à la matrice :

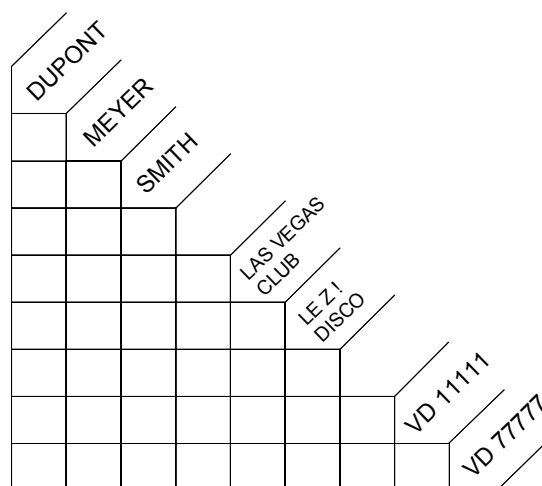


fig. 29 : Placement des entités dans la matrice relationnelle

Les liens étaient symbolisés par des pastilles codantes selon les standards suivants :

<b>Relation confirmée</b>	●
<b>Relation présumée</b>	○
<b>Fonction confirmée</b>	+
<b>Fonction présumée</b>	-

fig. 30 : Codes de relations des matrices relationnelles

Ce qui donnait la matrice complétée suivante :

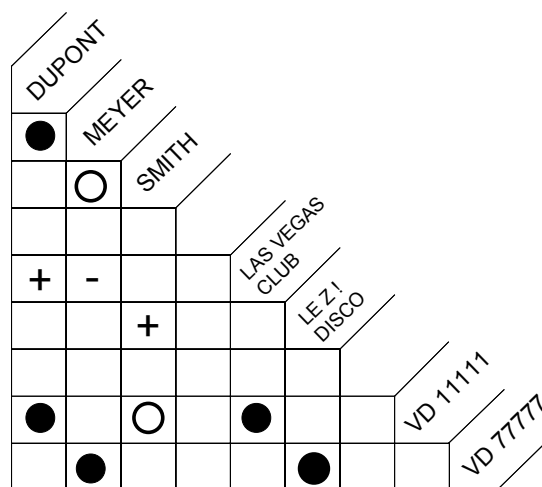


fig. 31 : Matrice relationnelle complétée

L'étape suivante qui était le comptage des relations, permettait de déterminer, *a priori*, les entités à faire figurer au centre de la représentation.

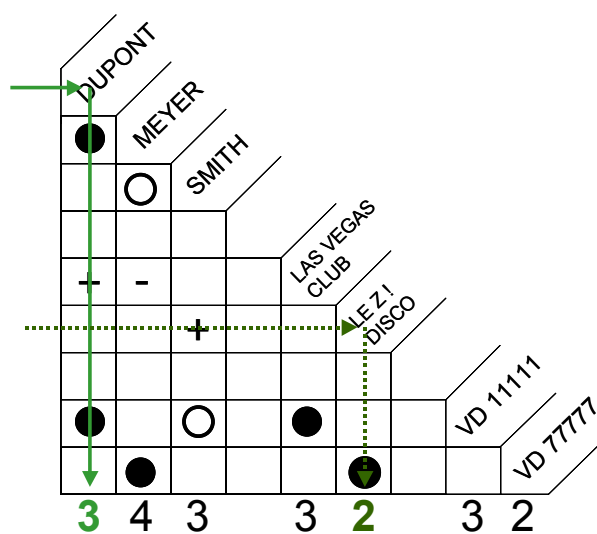


fig. 32 : Comptage des relations dans la matrice relationnelle

Une fois la matrice réalisée et comptabilisée, il était possible de passer à la représentation graphique en tant que telle. Pour cela, un standard a également été édicté :

Élément à représenter	MATRICE	SCHEMA	Relation confirmée	●	—
Personne Chose	DUPONT	DUPONT	Relation présumée	○	- - - -
Entreprise Organisation	LE Z ! DISCO	LE Z ! DISCO	Fonction confirmée	+	⊕
			Fonction présumée	-	⊖

fig. 33 : Standard de traduction de la matrice relationnelle au schéma relationnel

Dans l'exemple utilisé jusqu'ici, cela aurait donné la représentation suivante :

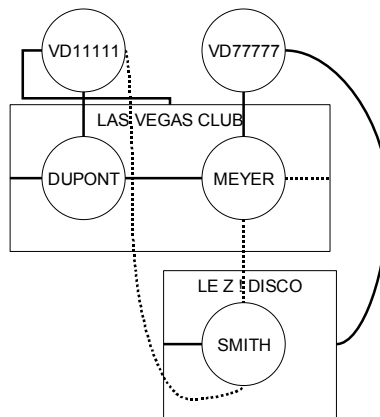


fig. 34 : Exemple de schéma relationnel brut

Enfin, ultime étape de l'élaboration d'un schéma relationnel : la clarification.

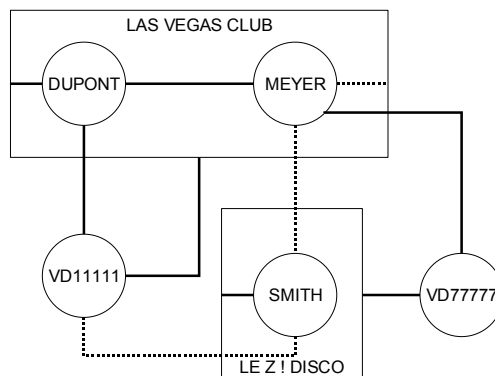


fig. 35 : Exemple de schéma relationnel clarifié



Le processus de réalisation de tels schémas a évolué. Le passage obligé par la matrice relationnelle a été supprimé grâce à la faculté des logiciels de réordonner automatiquement ou manuellement les entités du schéma.

De plus, les standards de visualisation ont changé. Les deux seules formes (rectangles et carrés) ont été remplacées par une multitude d'icônes dépeignant des personnes, des choses, des lieux ou encore des événements et des activités. La qualification des relations a été multipliée par l'apparition de codes de couleur. Le potentiel informatif des représentations a donc logiquement grandi.

Cependant, certains standards, tels que les boîtes représentant des groupes ou des organisations, subsistent encore. L'exemple utilisé jusqu'ici donnerait les représentations suivantes aujourd'hui.

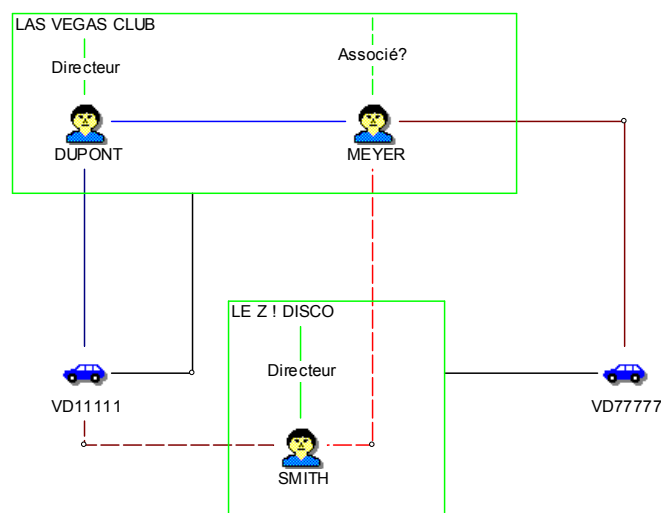


fig. 36 : Exemple de schéma relationnel actuel

Ou, en réduisant les sociétés en icônes pour éviter les croisements de traits :

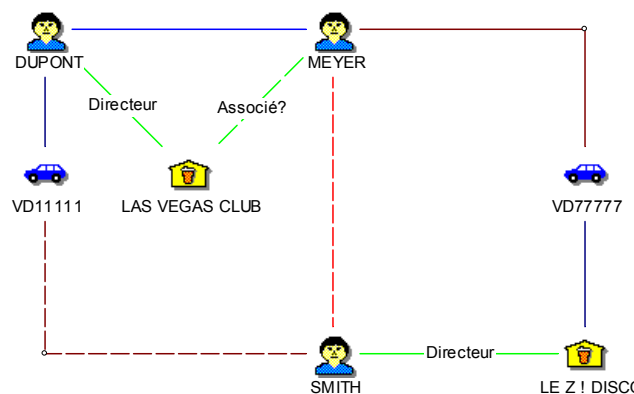


fig. 37 : Exemple de schéma relationnel moderne simplifié

En plus des simples relations, il est possible de représenter des flux. Il s'agit de la même technique de représentation que le schéma de relations, mais avec l'indication du flux de biens, de marchandises ou d'informations représentés simplement par l'indication du sens de la transaction en ajoutant une flèche au lien.

Bien souvent, les schémas de relations comprennent une partie de flux. Il s'agit de schémas relationnels mixtes.

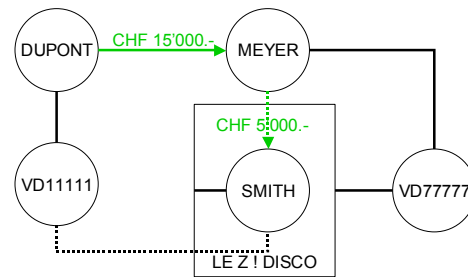


fig. 38 : Exemple de schéma relationnel mixte ancien

Ce qui donne avec les logiciels actuels :

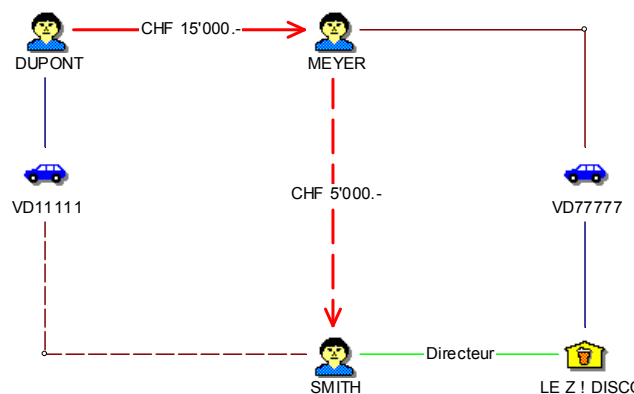


fig. 39 : Exemple de schéma relationnel mixte moderne

### 1.4.6.2 Les analyses de contrôles techniques

Certaines représentations graphiques des analyses de contrôles techniques se construisent de la même manière que les diagrammes relationnels. Le type d'entité est cependant limité. Il s'agit de postes de communication fixes ou mobiles, comme des raccordements de téléphone fixe, des télécopieurs, des téléphones cellulaires, des pagers, ou tout système informatique en réseau. La définition précise du type de poste de communication est de moindre importance, de même que le type de relation qui se réduit à un seul : la connexion établissant une communication. Il est toutefois possible de différencier tant les entités que les types de connexions, si l'analyse des communications le rend nécessaire.

En plus, des schémas relationnels, des tableaux statistiques de fréquences d'appels en fonction des jours et de l'heure permettent de tirer une image des habitudes téléphoniques des utilisateurs. Ils sont d'une grande importance.

Ces tableaux sont décrits en détail par PETERSON<sup>199</sup>. Un exemple d'une matrice jour/heure est reproduit à la page suivante.

Il est alors possible de représenter graphiquement l'information contenue dans ces matrices, en veillant à ne pas tomber dans les pièges de la représentation graphique de données et suivre les recommandations de TUFTE<sup>200</sup> de l'excellence graphique, soit:

« Excellence in statistical graphics consists of complex ideas communicated with clarity, precision, and efficiency. Graphical excellence displays should :

- show the data
- induce the viewer to think about the substance rather than about methodology, graphic design, the technology of graphic production, or something else
- avoid distorting what data have to say
- present many numbers in a small place
- make large data sets coherent
- encourage the eye to compare different pieces of data
- reveal the data at several levels of detail, from a broad overview to the fine structure
- serve a reasonably clear purpose : description, exploration, tabulation, or decoration
- be closely integrated with the statistical and verbal descriptions of a data set. »  
(p.13)

Des outils tels que le CTAnalyser<sup>201</sup> permettent de fournir ce type de *matrice jour/heure* sur la base d'une liste de connexions téléphonique ou informatique.

---

<sup>199</sup> in ANDREWS & PETERSON, *op. cit.*, 1990 (p.92)

<sup>200</sup> TUFTE, *The visual Display of Quantitative Information*, 2001

<sup>201</sup> Le logiciel CTAnalyser développé par Sébastien CAPT est issu de nos recherches menées en commun, tant à l'IPS en 2000 et 2001, que depuis lors au sein de la police de Sûreté vaudoise. Aujourd'hui le logiciel en est à sa troisième version et il contient les différentes fonctions présentées ici.

Heure	jour							Totaux
	Lundi	Mardi	Mercredi	Jeudi	Vendredi	Samedi	Dimanche	
01:00	-	-	-	1	1	-	-	2
02:00	-	1	-	-	-	-	-	1
03:00	-	-	-	-	-	-	-	0
04:00	-	-	-	-	-	-	-	0
05:00	-	-	1	-	-	-	-	1
06:00	-	-	-	1	-	-	-	1
07:00	2	1	1	2	1	-	-	7
08:00	-	1	-	1	2	-	-	4
09:00	9	2	1	3	4	-	-	19
10:00	12	7	9	8	10	1	-	47
11:00	15	10	12	11	17	-	-	65
12:00	10	6	5	7	11	-	-	39
13:00	9	7	8	6	9	3	2	44
14:00	14	12	11	13	18	-	-	68
15:00	16	14	16	18	20	2	3	89
16:00	13	9	7	6	8	1	-	44
17:00	6	3	5	4	7	-	4	29
18:00	7	2	4	-	1	4	-	18
19:00	5	4	-	1	4	-	1	15
20:00	3	3	1	-	4	-	-	11
21:00	-	-	2	1	2	-	2	7
22:00	2	-	1	1	3	-	-	7
23:00	-	1	-	2	2	-	-	5
24:00	-	-	-	-	2	-	1	3
Totaux	123	83	84	86	126	11	13	526

fig. 40 : Exemple d'une matrice jour/heure d'un contrôle technique

Suivent quelques exemples de graphiques, qui découlent de cette matrice et qui ont été intégrés au logiciel CTAnalyser :

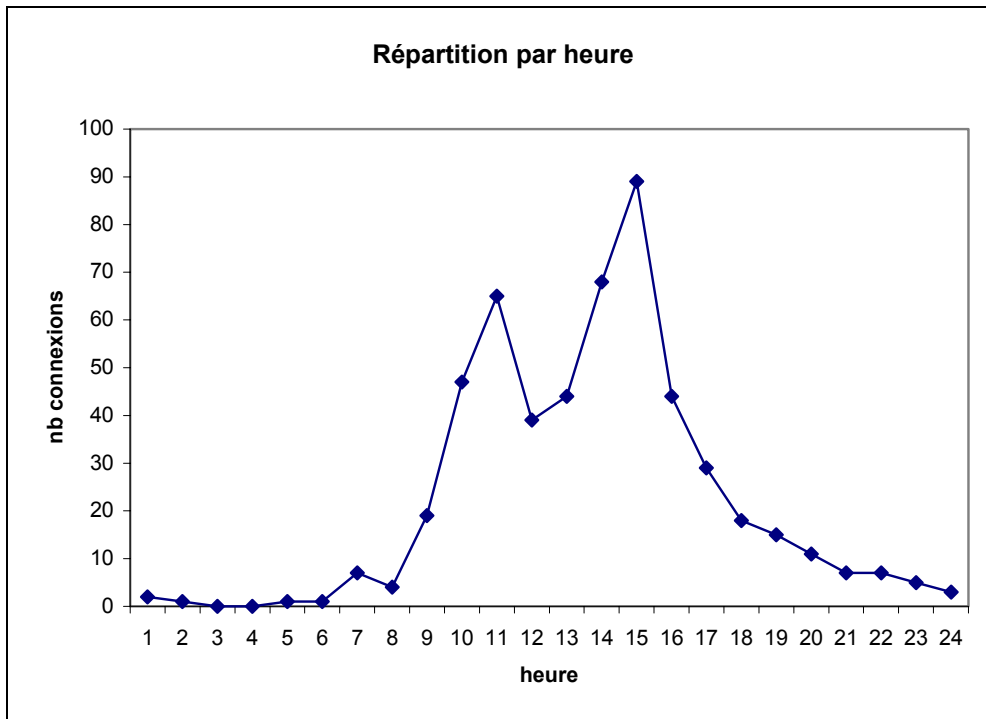


fig. 41 : Exemple de représentation des connexions / heures

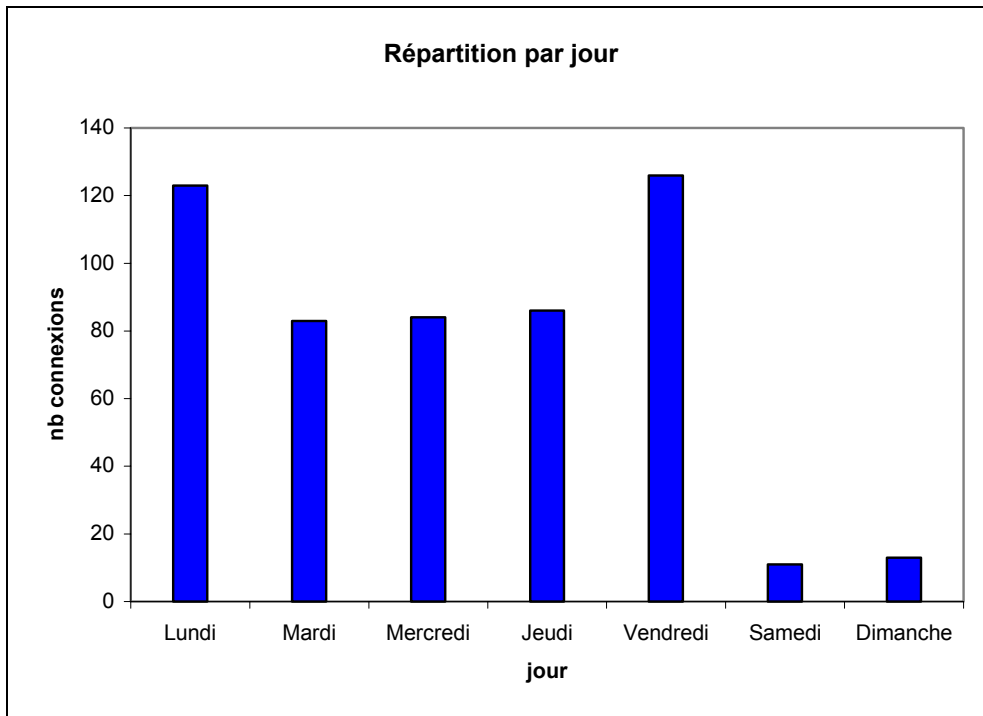


fig. 42 : Exemple de représentation des connexions / jours

Ou, en combinant ces deux critères, on obtient un graphique de la répartition par heure selon le jour de la semaine.

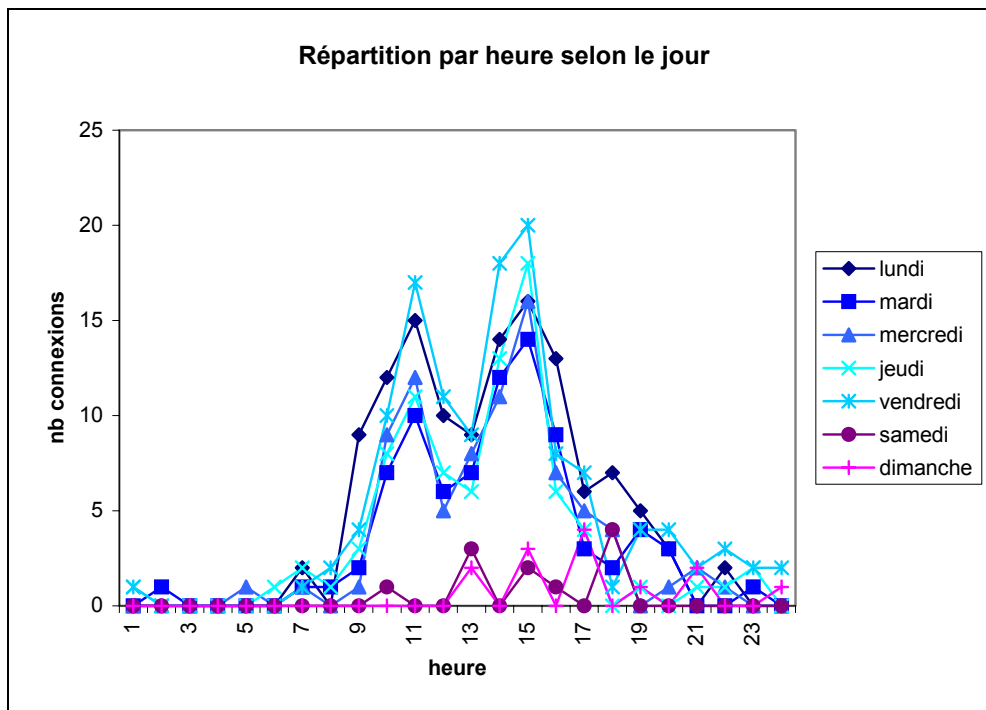


fig. 43 : Exemple de représentation des connexions / heures selon le jour

D'autres développements sont en cours. La composante de l'analyse spatiale sera bientôt entièrement intégrée pour le traitement des données issues de téléphones cellulaires. Elle permettra

de pouvoir apprécier rapidement sur le territoire suisse les régions dans lesquelles le téléphone cellulaire a été le plus utilisé, ainsi que les déplacements particuliers<sup>202</sup>.

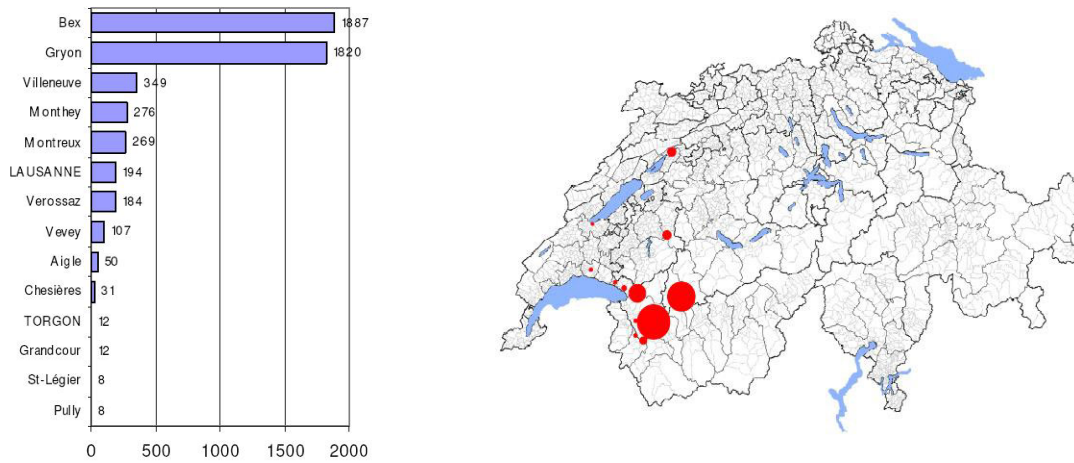


fig. 44 : Exemple de représentations géographiques rendues possibles par le CTAnalyser 3.0

Avec bien évidemment la possibilité de produire des cartes plus précises au besoin.

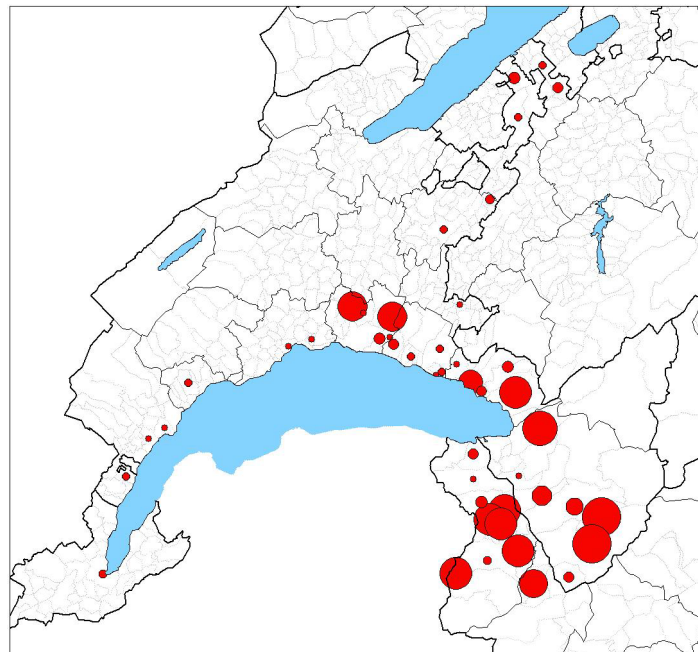


fig. 45 : Exemple de représentation géographique précise

<sup>202</sup> Un autre outil spécifique a été récemment développé par Q. ROSSY, analyste à la police de sûreté neuchâteloise et doctorant IPS. Il s'agit du prototype VISUALIST qui permet une analyse spatio-temporelle très fine de données historiques ou de trajets GPS, par exemple.

De telles représentations, qui permettent de visualiser les habitudes temporelles et les déplacements géographiques des utilisateurs de moyens de communications, apportent une plus-value immédiate à l'enquêteur et lui économisent bien du travail, face auquel il se trouvait en général désarmé.

Mais, comme on l'a mentionné au début de ce propos sur l'analyse des contrôles techniques, les schémas de relations qu'il est possible de créer sont complémentaires aux diagrammes temporels et géographiques et sont en soi extrêmement intéressants. Ils permettent par exemple d'obtenir une vue d'ensemble des connexions, ce qui est quasiment impossible en lisant les données techniques lorsque celles-ci deviennent trop nombreuses. Grâce aux logiciels actuels et au fait que les informations nous parviennent sous forme numérique, il est désormais facile et rapide de représenter les relations dans un schéma. Ce que l'analyste recherche alors visuellement est de mesurer l'implication des personnes, de repérer les rôles principaux, et d'interpréter les données atypiques. Enfin, le schéma permet à l'analyste de transmettre l'ensemble de l'information sous une forme visuellement réceptive, beaucoup plus facilement et d'illustrer ainsi ses interprétations et par là de représenter son argumentation.

A l'origine, les standards développés notamment par PETERSON étaient les suivants :

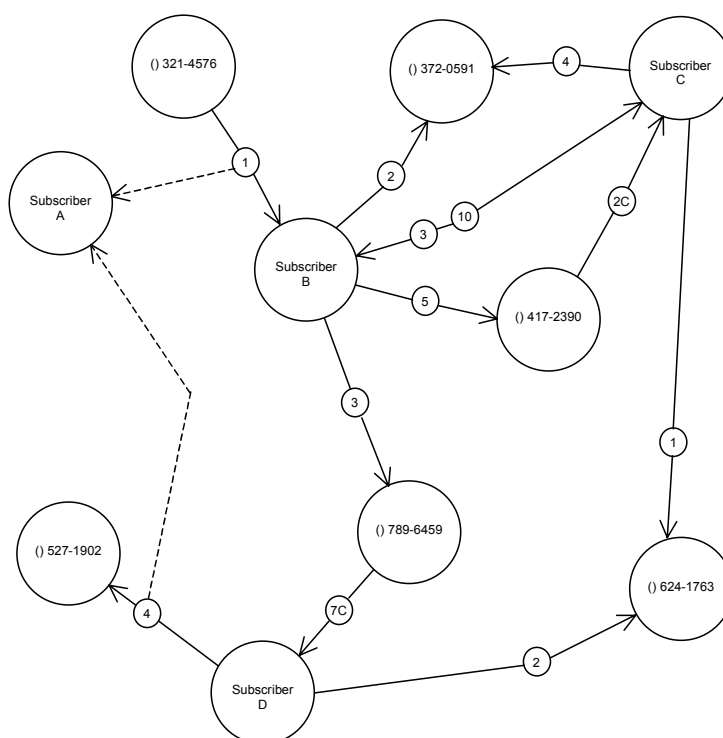


fig. 46 : Représentation graphique de contrôles techniques selon d'anciens standards<sup>203</sup>

Les abonnés ou les numéros appelés figuraient dans des cercles. Les flèches pleines représentent la direction des appels entrants ou sortants ; les flèches en pointillés représentent les appels payés par

<sup>203</sup> Illustration tirée de ANDREWS & PETERSON, *op. cit.*, 1990 (p.100)

des cartes de crédit ou à prépaiement. Les nombres dans les cercles de flèches indiquent le nombre d'appels ; le « C » indique les appels en PCV (Collect calls).

Comme pour l'établissement des schémas relationnels présentés au point précédant, le passage par une matrice relationnelle était recommandé par les auteurs.

A l'aide des logiciels actuels, les données ci-dessus donneraient la représentation suivante :

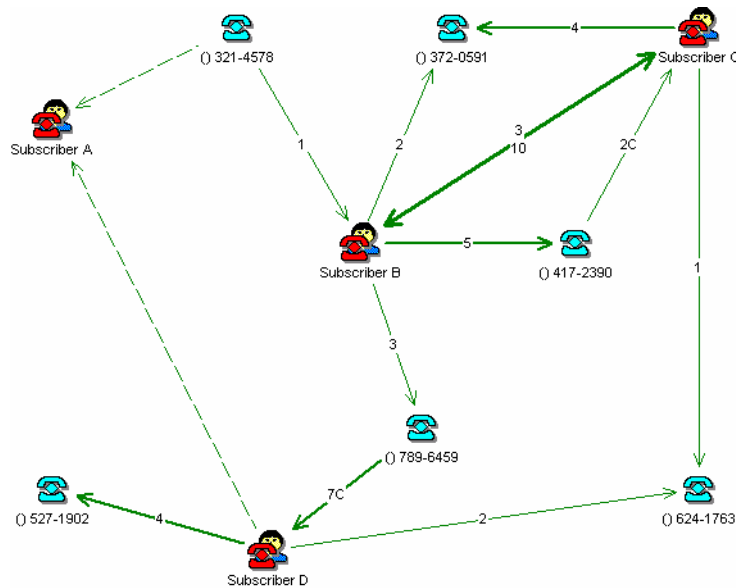


fig. 47 : Représentation graphique de contrôles techniques à l'aide des outils actuels

D'autres possibilités graphiques sont apparues depuis. Les codes couleur peuvent être utilisés, par exemple, pour différencier la source des données. L'épaisseur des liens peut également être proportionnelle au nombre d'appels, ce qui permet d'apprécier visuellement les contacts principaux. Le sens des appels peut être signifié par une seconde flèche adjacente, si les connexions sont bidirectionnelles, ce qui constitue une plus grande richesse d'expression.

L'exemple suivant, tiré d'un cas réel montre qu'un nombre important de données peuvent figurer sur une représentation de contrôles techniques (ici plus de 880 raccordements et plus de 1300 liens représentant près de 10'000 connexions<sup>204</sup>). La vue d'ensemble est malgré tout facilement appréciable.

Il s'agit de la représentation des connexions de trois téléphones cellulaires pour une durée allant jusqu'à six mois. Dans le cas présenté ci-après, un numéro commun aux trois protagonistes contrôlés ressort immédiatement {1}.

<sup>204</sup> Ce qui représente un listing de plus de 200 pages.



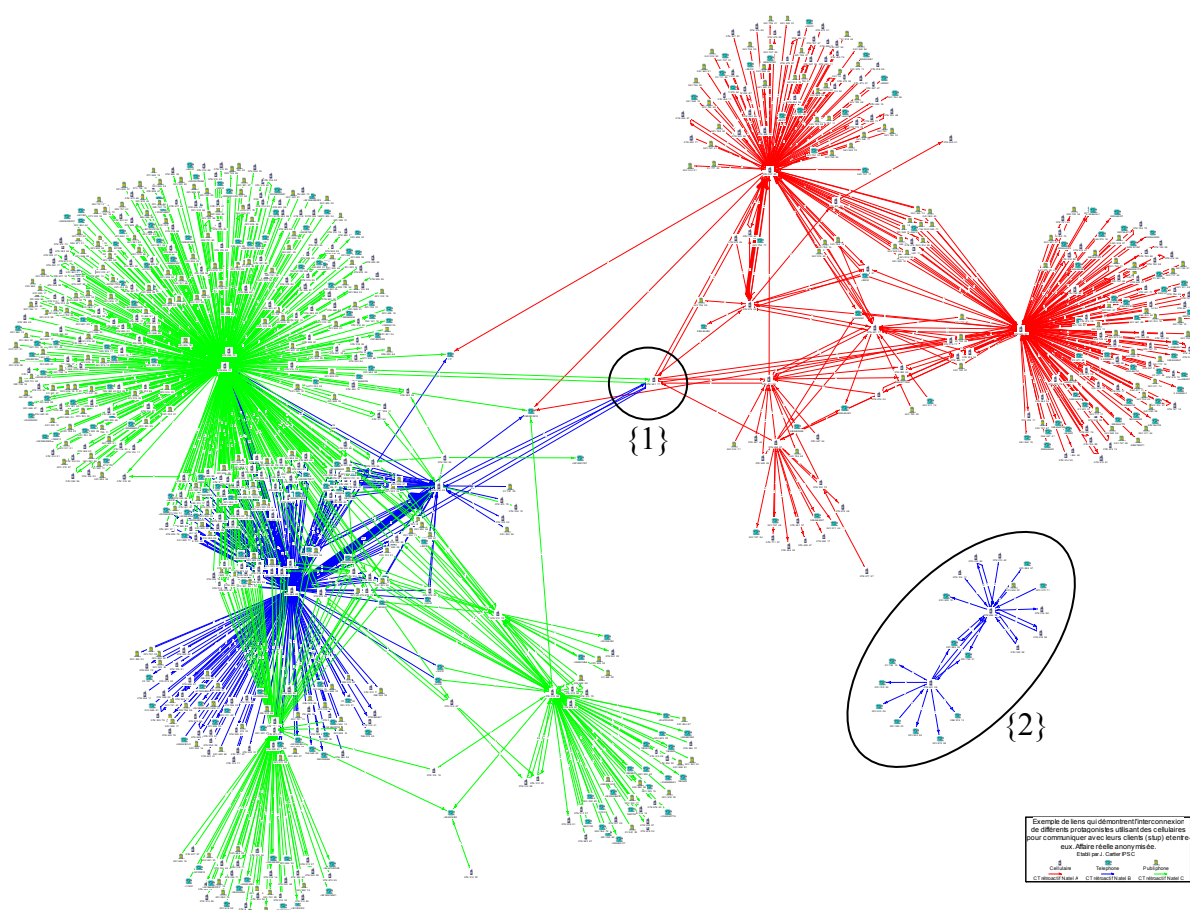


fig. 48 : Exemple de représentation relationnelle d'un contrôle technique

Par ailleurs, on remarque immédiatement que des raccordements d'un cellulaire ne sont en contact avec aucun autre raccordement lié à l'activité principale des protagonistes {2}. Après contrôle, il s'est avéré qu'il s'agissait d'appels passés par le propriétaire légitime du cellulaire avant qu'il ne se le fasse voler et qu'il soit utilisé par les personnes ciblées par la mesure technique. Ses données y figurent encore car le vol s'était passé moins de six mois avant que la mesure soit demandée, soit dans le délai légal de transmission des données historiques par les opérateurs. Grâce à la visualisation, les personnes présentes dans les données techniques, mais pas liées à l'activité délictueuse déployée par les personnes visées ont pu être immédiatement mises hors de cause.

### 1.4.6.3 Schémas relationnels et analyse de réseaux sociaux

Les diagrammes relationnels tels qu'entendus dans ce chapitre ne correspondent pas aux « analyses de réseaux sociaux » (*Social Network Analysis - SNA*<sup>205</sup>) apparus en sociologie, bien qu'ils y ressemblent. Les analyses de réseaux se basent sur des « socio-matrices », les entités sont réduites à

<sup>205</sup> FREEMAN décrit les premiers pas de cette discipline : les « *sociograms* » de MORENO en 1932. Puis, il passe en revue les différents outils utilisés, de la planche à dessin, jusqu'aux logiciels en 3D, en passant par des objets. Voir FREEMAN, *Visualising Social Network*, 2000

un seul type, soit des personnes ou acteurs appelés « nœud » (*nodes*), ainsi que les relations appelées « liens » (*ties*).

Suite à cela, des modèles mathématiques et les théories sociologiques qui en découlent peuvent être appliquées. Certaines de ces notions, la « centralité » (*Centrality*), « l'équivalence » (*Equivalence*), et les « maillons faibles » (*Weak-ties*), pourraient, selon SPARROW<sup>206</sup>, avoir un intérêt en analyse criminelle.

IANNI<sup>207</sup> parle de l'utilisation de l'analyse de réseaux dans le cadre de l'analyse criminelle opérationnelle. Malheureusement, aucun exemple pratique n'est présenté.

Plus récemment, les attentats terroristes islamistes, ont relancé l'intérêt de certains sociologues d'appliquer les techniques de l'analyse des réseaux sociaux aux réseaux terroristes. Ainsi, KREBS<sup>208</sup> a recueilli tous les éléments disponibles dans la presse et sur Internet sur les attentats du 11 septembre 2001 à New-York et en a fait une analyse par *SNA, a posteriori*. La masse et la qualité des informations étaient suffisantes pour produire un schéma instructif. Toutefois, KREBS concluait de la sorte :

« To draw an accurate picture of a covert network, we need to identify task and trust ties between the conspirators. The same four relationships (*Trust, Task, Money & Resources, Strategy & Goals, ndlr*) we map in business organizations would tell us much about illegal organizations. This data is occasionally difficult to unearth with cooperating clients. With covert criminals, the task is enormous, and may be impossible to complete. » (p. 51)

En Espagne, RODRIGUEZ<sup>209</sup> faisait de même avec l'attentat du 11 mars 2004 à Madrid. Cet auteur relevait que les liens qui régissent les réseaux terroristes sont *faibles*. Ce qui rend la détection des noyaux terroristes encore plus difficile :

« September 11th and March 11th terrorist attacks have shown the importance of new forms of organization (networks). They are especially relevant in cases of secret societies and terrorism. They are more difficult to detect because they are based on weak rather than on intense relationships. The visible network (the acting network) is a part and a product of a larger and more diffuse network. » (p. 14)

Le contexte criminel semble poser d'autres difficultés que simplement d'ordre technique ou méthodologique. Alors que les sociologues travaillent habituellement avec des personnes

---

<sup>206</sup> SPARROW, The application of network analysis to criminal intelligence. An assessment of the prospects, 1991

<sup>207</sup> in ANDREWS & PETERSON, Criminal Intelligence Analysis, 1990

<sup>208</sup> KREBS, Mapping Networks of Terrorist Cells, 2002

<sup>209</sup> RODRIGUEZ J. A., The March 11th Terrorist Network: In its weakness lies its strength, 2004

consentantes, l'utilisation de l'analyse de réseaux sociaux avec des données recueillies secrètement semble difficile ou impossible *a fortiori* de manière préventive.

SPARROW<sup>210</sup> relève un certain nombre de caractéristiques des réseaux criminels qui les rendent difficilement analysables à l'aide des techniques sociologiques :

« Much criminal intelligence data, as mentioned above, either appears in link form or is readily convertible to it. It would be enormously gratifying, therefore, if we could simply throw the existing network analysis toolkit at criminal intelligence databases, and come away with a set of valuable new insights. Of course it is not that easy. If it were, it would surely have been done before.

The fact is that most network analysis tools have been developed within the context of retrospective social science investigations, and they are therefore designed for use on networks which are small, static, and with very few distinct types of linkages (generally only one).

It is worth considering the properties of criminal networks, and associated intelligence databases, which present significant challenges to the science of network analysis as it now stands. » (p. 261)

La première difficulté est la taille des réseaux criminels. SPARROW notait qu'en 1991 peu d'algorithmes étaient capables de traiter un grand nombre de données, et même si c'est désormais possible aujourd'hui, le nombre de relations en jeu n'entraînerait pas forcément un résultat théoriquement valide :

« Size :

First and foremost, criminal intelligence databases can be huge, with many thousands of nodes. The computational ramifications are obvious - mandating the use of sparse matrix techniques or extensive exploitation of parallel processing should any analytical algorithm exceed  $O(n^3)$ <sup>211</sup>. Some network analysis algorithms do claim to be able to handle very sizeable networks. (...). But it contains an unfortunate reliance on a one-dimensional interim stage in the analysis of groups and cliques, which will inevitably render its results suspect when applied to networks of any complexity. » (p. 261-262)

Ensuite, les données recueillies dans le contexte criminel sont par essence incomplètes. Cet état de fait pose, selon SPARROW<sup>212</sup>, un problème de fond à l'application des méthodes de réseaux sociaux :

---

<sup>210</sup> SPARROW, *op. cit.*, 1991

<sup>211</sup> L'auteur ne légende pas cette formule, mais on peut sans doute l'attribuer à une « complexité moyenne de temps » dans le calcul d'un algorithme d'apprentissage. Voir, par exemple, SCHMIDHUBER, A Fixed Size Storage  $O(n^3)$  Time Complexity Learning Algorithm for Fully Recurrent Continually Running Networks, 1992

<sup>212</sup> SPARROW, *op. cit.*, 1991

« Incompleteness :

Criminal network data is also inevitably incomplete; i.e. some existant links or nodes will be unobserved or unrecorded. Little research has been done on the effects of incomplete information on apparent structure. There is some work on the problems of statistical inference from incomplete graphs (FRANK 1978<sup>213</sup>), researched using random link samplings from known networks; also on the relationship between network density and structural properties (FRIEDKIN 1981<sup>214</sup>). But the relevance of such work to criminal networks is largely negated by the fact that the incompleteness in the criminal databases will be anything but random - it will be systematic, at least in part, in accordance with the biases introduced by investigative methods and assumptions. The focus of existing intelligence data is determined more by the prior subjective judgments of investigators than by objective reality. » (p. 262)

De plus, pour SPARROW, dans l'analyse préventive de réseaux criminels, on le verra aussi par la suite, un des problèmes centraux est la délimitation d'un réseau dit criminel à l'autre :

« Fuzzy boundaries :

The boundaries of any particular criminal web are quite ambiguous. Even organized crime families are often interrelated. And many significant crime figures are significant precisely because they are connected to a number of different criminal organizations. So there is no obvious criterion by which players can be excluded or included in any one network analysis (...). Of course criminal networks, like any other, can be split unambiguously into maximal connected subcomponents, but these may still be extensive. » (p.262)

Enfin, le dernier critère déterminant et qui pourrait être d'une grande utilité est selon SPARROW l'évolution dynamique des réseaux :

« Dynamic :

Criminal networks are, for all practical purposes, dynamic, not static. Each contact report, telephone call, or financial transaction has a time and date. The relationship between any two individuals is not merely present or absent (binary), nor is it simply weaker or stronger (ascribed a static analogue weighting); rather it has a distribution over time, waxing and waning from one period to another. Many of the most useful network questions depend heavily on this temporal dimension, begging information about which associations are becoming stronger, or weaker, or extinct.

---

<sup>213</sup> FRANK O., Sampling and estimation in large social networks, *Social Networks* 1: 1978, pp 91-101, in SPARROW, *op. cit.*, 1991

<sup>214</sup> FRIEDKIN N., "The development of structure in random networks: An analysis of the effects of increasing network density on five measures of structure", *Social Networks* 3, 1981, pp 41-52, in SPARROW, *op. cit.*, 1991

The problematic absence of research on dynamic networks was echoed by BARNES and HARARY (1983)<sup>215</sup>. A little work has been done on the evolution of network connections over time in dynamic networks (...), and a little on structural change within networks (...) but little or nothing has been done to develop algorithms for revealing significant network changes over time in the context of networks where each link has a time-dimension coordinate. » (pp. 262-263)

Ces limitations mettent sérieusement en doute l'utilité réelle d'une telle approche dans le contexte de l'analyse criminelle. GIANNAKOPOULOS<sup>216</sup> a utilisé ce modèle pour analyser des systèmes de corruption dans le cadre d'affaires judiciaires en Suisse. Dans son étude, la complexité très rapidement atteinte par les « socio-matrices » ne permet pas, à mon avis, de tirer des conclusions qui soient pertinentes dans le contexte opérationnel. L'intérêt peut toutefois exister au plan stratégique.

Les réseaux sociaux permettent de représenter naturellement certains faits sous la forme de relations uniques et indifférenciées. On suppose que les réseaux criminels peuvent s'exprimer sous cette forme et que cette méthode peut être utile aux investigations, mais dans le contexte de l'analyse criminelle, deux raisons fondamentales s'opposeront, à mon avis, encore longtemps au traitement mathématique des schémas relationnels « simplifiés », tels que les « socio-matrices ».

La première raison, énoncée par SPARROW, est que les données dont nous disposons sont trop imparfaites et trop incomplètes. Or, dans le cadre des analyses de réseaux sociaux, le moindre changement peut avoir des effets très importants sur le résultat en raison de l'effet domino. IANNI<sup>217</sup> le présente ainsi :

« Once again, the eventual usefulness of a network chart is heavily dependent on the accuracy and comprehensiveness of the identification of the points or units and their relational content. Because of a kind of domino effect of independent units, mistakes in the units or points have ramifications well beyond that single error by suggesting relations that do not exist or failing to be aware of relations that do exist. » (p. 70)

On imagine donc mal appliquer strictement les modèles mathématiques développés dans le cadre des *SNA* à des données incomplètes et imparfaites par essence pour en retirer un quelconque résultat significatif.

---

<sup>215</sup> BARNES J.A. & HARARY F., "Graph-theory in network analysis.", *Social Networks* 5 (2): 1983, pp 235-244, in SPARROW, *op. cit.*, 1991

<sup>216</sup> GIANNAKOPOULOS, *Criminalité organisée et corruption en Suisse*, 2001

<sup>217</sup> *in* ANDREWS & PETERSON, *Criminal Intelligence Analysis*, 1990

La seconde raison qui ne permet pas d'appliquer ces modèles est le manque de décomposition, en comparaison des schémas relationnels classiques qui permettent de représenter une grande diversité d'entités et de relations qui sont représentées par des codes graphiques (icônes) ou de couleur (relations), en sus des codes de qualité des relations (confirmée ou non) connues des standards initiaux.

Cette grande variété ne s'intègre absolument pas aux modèles développés dans l'analyse des réseaux sociaux jusqu'ici, et il est sans doute extrêmement difficile d'élaborer des modèles mathématiques permettant d'intégrer ces facteurs aux situations aussi complexes et diverses que nous réserve la réalité.

Des efforts sont toutefois encore consentis aujourd'hui pour trouver les bons algorithmes d'aide à l'analyse qui donneront un résultat exploitable. Par exemple, XU & CHEN<sup>218</sup> étudient un algorithme particulier dans le contexte criminel. Ils butent malheureusement actuellement encore et toujours sur le problème de l'intégration des données, problème récurrent dans le monde judiciaire :

« Analysis of the evaluation results suggests that the effectiveness might be improved by extracting more appropriate entities from texts and using them as network nodes. In our future research, we will apply effective named-entity extraction techniques to replace our current noun phraser. We will also incorporate some domain-specific heuristics to help the system select only entities and associations that are considered useful by crime investigators. » (p. 14)

A ce sujet, certains éditeurs de logiciels d'analyse criminelle opérationnelle spécifiques tentent d'apporter des réponses, en fournissant sur le marché des solutions partiellement automatisées<sup>219</sup>. A mon avis, ces solutions ne sont absolument pas satisfaisantes. Elles dénaturent le travail réfléchi de l'analyste dans la création de ses schémas en lui fournissant en contrepartie peu d'avantages, soit de lui éviter de ressaisir les noms des entités. La reconnaissance des entités pertinentes est l'élément clé et les systèmes informatiques peinent à y parvenir et induisent de nouveaux biais.

Tout au plus, on peut concevoir, et c'est souvent le cas dans la pratique, que dans le cadre d'une collaboration entre des enquêteurs et des analystes chargés de leur apporter un soutien dans la structuration de leurs données, que des canevas pré-formatés soient mis à la disposition des enquêteurs lors de la saisie des entités pertinentes, afin de répartir la charge de ressaisie de ces éléments. Les entités pertinentes peuvent être soit générales et un modèle de données réaliste peut s'appliquer, soit spécifiques et nécessitent la définition d'un modèle de données pouvant permettre de répondre aux interrogations des enquêteurs.

---

<sup>218</sup> XU & CHEN, *Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks*, 2004

<sup>219</sup> A l'instar du *TextChart* de *i2 inc.*

Des solutions automatiques de détection de données plus ou moins pré-formatées seraient plus intéressantes, mais là encore, le chemin à parcourir semble encore long. LEE<sup>220</sup> concluait sa recherche de la sorte :

« Integrating an information extraction tool and a link analysis tool with a relational data base is a natural and proven way to provide the latter with plenty of usefully structured data to work with. The association information automatically placed in the data base by the former tool is the natural source of link data to drive that analysis. (...)

One limitation of the IE (*Information Extraction, ndlr*) tool is that it makes no effort to decide whether an item it has found in a message is the “same” as another item already in the data base; it errs on the side of assuming it is not. Thus, each message that refers to a “Pablo Garcia”, or a “Cessna Firebat”, for example, will result in a new record for that item being generated. It is up to the analyst to use various tools – including link analysis – to decide that two records refer to the same item. This leads to a useful synergy between the two tools and the analyst. » (p. 5)

Si son système automatique connaît le vocabulaire, il peine encore à comprendre la grammaire. Il semble donc nécessaire de reprendre le tout pour remodeler les schémas ainsi produits. Il n’est pas sûr que dans ce cas le gain de temps soit effectif.

Les développements de l’intégration de données et du traitement mathématique des schémas sont donc encore au stade d’ébauches en ce qui concerne les schémas de relations tels qu’utilisés dans le contexte judiciaire de l’analyse criminelle. La situation est complètement différente dans le cadre de l’analyse des contrôles techniques.

#### Analyse de contrôle technique et analyse de réseaux (sociaux)

Si nous comparons l’analyse des contrôles techniques, à la notion d’analyse de réseau (sociaux), on remarque que dans les deux cas les entités et les relations sont bien définies. On pourrait donc penser appliquer les principes mathématiques développés initialement pour l’analyse de réseaux sociaux aux contrôles techniques.

Alors, la tentation devient grande d’augmenter toujours plus la taille du réseau pour arriver théoriquement au « réseau total » (*total network*) représentant l’ensemble des connexions du monde entier. IANNI<sup>221</sup> nous met cependant en garde :

« In its original inception, network analysis involved a representation of reality based on plotting points for persons, connected by lines to other persons (represented by other points), thus depicting a relationship between and among those so connected or linked. The resulting pattern of lines resembling a web or a net was characterised as a network. A

<sup>220</sup> LEE, Automatic information extraction from documents: a tool for intelligence and law enforcement analysts, 1998

<sup>221</sup> in ANDREWS & PERTERSON, *op. cit.*, 1990

total network would theoretically include the population of the entire world, since by definition there is no one that is not connected to someone else. However, for the purpose of the investigation, we can and should take care that we limit the range in which the net is cast. The reason for using network construction as a tool in intelligence analysis is not in the furtherance of some theoretical application, but in its usefulness as a means of developing alternate hypotheses to direct or facilitate current or future investigations. »  
(p. 67)

Une première limitation à l'idée de pouvoir représenter le réseau « total » est que plus on représente de données sur un schéma, plus les interprétations que l'on est capable de faire sont générales. Il est alors nécessaire de produire des représentations à des niveaux de détail différents pour répondre aux différentes questions qui peuvent se poser lors de l'enquête. La représentation « totale », n'est pas utile en soi, ce qui l'est en fait, c'est la disponibilité des données, pour pouvoir « zoomer » sur des parties de celui-ci. Car, plus il y a de données représentées, plus les renseignements que l'on peut en tirer sont généraux.

De plus, cette entreprise serait bien sûr vaine dans le cadre judiciaire. Les analystes ne disposent heureusement que des données issues de mesures ordonnées par les instances judiciaires autorisées au sens de la LSCPT<sup>222</sup>. Pour travailler de la sorte, il faudrait, soit se trouver chez les opérateurs (services internes anti-fraude), soit travailler pour le renseignement militaire (p.ex. projet Onyx<sup>223</sup>).

Pour donner un ordre d'idée de la différence entre l'approche dirigée du domaine judiciaire et l'approche globale de l'analyse de réseaux globaux, voici quelques chiffres :

En 2003, en Suisse, on comptait plus de 10 millions de raccordements<sup>224</sup> (4 millions de raccordements fixes pour 6,2 millions de raccordements mobiles). Le nombre d'appels se monte à près de 10 milliards (5,7 milliards sur le réseau fixe et 3,9 milliards sur le réseau mobile).

En comparaison, en 2003 toujours, le nombre d'interceptions actives<sup>225</sup> s'est monté à 2928, pour 3815 demandes rétroactives.

Les chiffres parlent d'eux-mêmes. Même si l'on pouvait réunir toutes les informations recueillies dans le cadre judiciaire, ce qui n'est pas possible légalement, il ne constituerait qu'un échantillon ridicule par rapport au « réseau total » suisse (env. 0.06%).

Pour 2004, on peut estimer qu'environ 2 raccordements sur 10'000 ont été « écoutés ». Mais, comme les personnes qui occupent les autorités de poursuite pénale changent fréquemment de

---

<sup>222</sup> RS 780.1 – Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

<sup>223</sup> FF 2003 1377 – Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx»)

<sup>224</sup> OFCOM – Statistique officielle des télécommunications 2003, [www.ofcom.ch](http://www.ofcom.ch)

<sup>225</sup> STS / DETEC – Statistiques des surveillances de la poste et des télécommunications



numéro pour brouiller les pistes, il n'est pas rare de devoir déployer plusieurs mesures pour un seul individu. On peut donc raisonnablement estimer le nombre d'utilisateurs de téléphonie (fixe ou mobile) à moins d'une dizaine pour 100'000 personnes. Ce qui est peu en regard des missions dévolues aux autorités de poursuite pénale<sup>226</sup>.

Les techniques présentées précédemment seraient sans doute inutiles à cause de l'ampleur des informations à gérer. D'autres moyens devraient être mis en œuvre pour trier les cas potentiellement intéressants sur le plan pénal ou de la protection de l'Etat. Puis, ensuite seulement, dans une analyse plus fine d'un cas détecté, les techniques traditionnelles pourraient être engagées.

Dans le domaine pénal, lorsque l'on sait travailler sur des données incomplètes, la délimitation des données à analyser et la parfaite connaissance des sources de données à disposition sont des éléments primordiaux dans la réalisation d'une analyse de qualité.

Ceci est d'autant plus vrai que les contrôles techniques sont obtenus contre rémunération<sup>227</sup>. Le prix des émoluments est relativement dissuasif pour les magistrats. Ce qui a pour effet que parfois des données qui auraient pu être utiles à l'enquête ne sont pas demandées uniquement pour des raisons budgétaires.

Par exemple, entrent en jeu trois appareils cellulaires GSM (*Global System for Mobile communication*) et trois cartes SIM (*Subscriber Identity Module*). Il est possible – et souvent recommandé pour les criminels – de changer fréquemment de carte pour obtenir une plus grande discrétion<sup>228</sup>.

Dans notre exemple, les différentes cartes ont été introduites et utilisées dans différents appareils de la manière suivante : la carte SIM 1 dans les appareils X et Y et la carte SIM 3 dans les appareils Y et Z. Le schéma suivant résume le tout :

---

<sup>226</sup> CARTIER, La localisation des téléphones portables, *in* Nouvelles technologies et criminalité : nouvelles criminologie ?, 2006

<sup>227</sup> RS 780.115.1 - Ordonnance du DETEC sur les émoluments et les indemnités en matière de surveillance de la correspondance postale et des télécommunications

<sup>228</sup> Notons que les cartes SIM pouvaient être totalement anonymes en Suisse jusqu'en octobre 2004, date à laquelle il est devenu nécessaire de présenter une pièce d'identité pour l'acquisition d'une carte SIM prépayée. L'enregistrement d'une identité pour les abonnements prépayés devait se faire rétroactivement pour les cartes acquises après le mois d'octobre 2002. Le nombre de raccordements prépayés en 2003 se montait à 2,6 millions (pour 6,2 millions de raccordements mobiles).

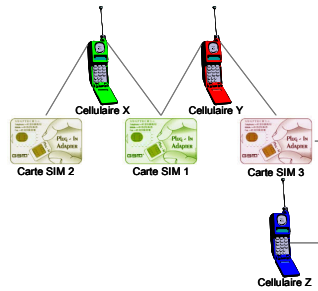


fig. 49 : Exemple d'utilisation de plusieurs GSM et de plusieurs cartes SIM

Notre point de départ est le numéro de téléphone correspondant à la carte SIM 1, dont nous avons eu connaissance par dénonciation.

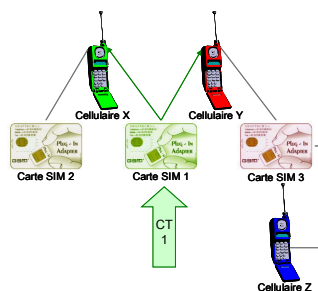


fig. 50 : Demande d'un premier contrôle technique

En demandant un contrôle technique sur cette carte SIM 1, les appareils utilisés avec cette carte vont apparaître dans nos données.

Comme on voit apparaître ces deux appareils, il va devenir nécessaire de poursuivre les investigations en effectuant deux nouvelles demandes sur les appareils X et Y.

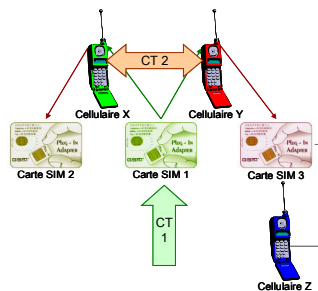


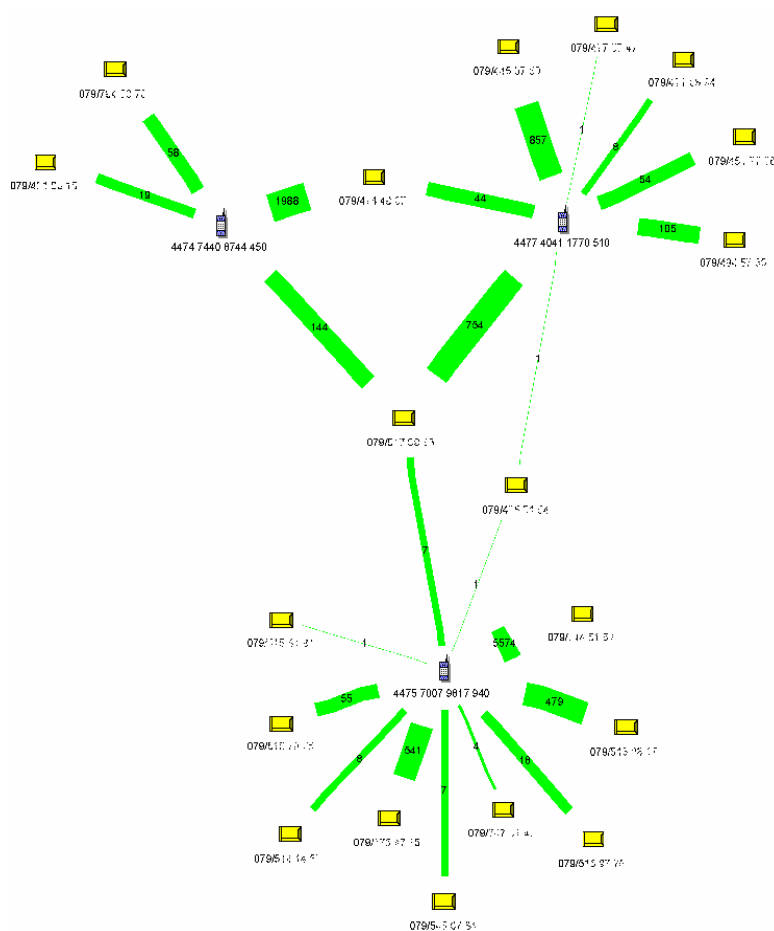
fig. 51 : Demande de deux nouveaux contrôles complémentaires

A ce stade, nous avons désormais obtenu les appels passés à l'aide des appareils cellulaires X et Y. En plus des appels passés avec la carte SIM 1, dont nous disposons déjà, les utilisations des cartes SIM 2 et SIM 3 avec ces appareils X et Y seront connues. Cependant, malgré ces deux demandes successives, nous n'avons pas encore découvert les utilisations faites avec la carte SIM 3 dans le cellulaire Z. Pour ce faire, il faudrait faire encore des demandes de contrôles techniques supplémentaires sur les cartes SIM 2 et SIM 3, et ainsi de suite.

Sachant que le tarif est de SFr. 700.- par demande et par opérateur, l'exemple ci-dessus montre que pour 1 SIM et deux cellulaires, le magistrat aurait du déboursier SFr. 4900.- d'émoluments.

En conclusion, cette situation montre que la délimitation du champ des recherches, en connaissance de cause, est un élément primordial à l'analyse puisqu'il va conditionner le niveau de connaissance avec lequel nous devons conduire l'analyse et interpréter les résultats en conséquence. Comme nous l'avons vu l'absence d'information est un élément extrêmement pénalisant dans l'analyse automatique des réseaux sociaux. Ce qui rend son application même dans ce domaine bien plus structuré encore très hasardeux.

Pour illustrer ceci, voici un exemple réel de la multiple utilisation des cartes (à préparation) dans les appareils cellulaires. Dans ce cas, les contrôles techniques ont été faits dès le départ sur les trois cellulaires. Il est donc très vraisemblable que certaines cartes aient été utilisées dans d'autres appareils, mais nous n'en savons rien !



*fig. 52 : Exemple réel d'échange de cartes SIM dans les téléphones GSM*

#### 1.4.6.4 Diagrammes chronologiques

Ces diagrammes ont pour fonction de représenter des événements de manière chronologique, afin de faciliter la recherche de la vérité et éventuellement de trouver de nouvelles pistes d'enquête. Ils

sont mis en œuvre préférentiellement dans des cas complexes avec des actions compliquées et nombreuses ou lorsque les déclarations des témoins sont contradictoires.

Les diagrammes chronologiques permettent, à l'instar des diagrammes relationnels, de mesurer l'implication des entités, d'obtenir une vue d'ensemble de la situation, de repérer les lacunes sur l'état des connaissances, et d'émettre des hypothèses de travail qui indiquent des pistes d'enquête possibles.

Ensuite, ils facilitent également la transmission de la masse d'informations d'une manière beaucoup plus réceptive qu'un long texte explicatif, et peuvent servir de document de base dans la poursuite du processus judiciaire.

Comme pour les diagrammes relationnels, une méthode originale a été proposée aux Etats-Unis, dans les années 1970. MORRIS<sup>229</sup> décrit également en partie la méthode d'élaboration.

L'élaboration se faisait en six phases: la collecte des informations, le choix des entités relevantes, le rassemblement des événements, l'élaboration des étiquettes, l'établissement du croquis provisoire et la clarification du croquis provisoire.

Nous ne nous étendons à nouveau pas ici sur la collecte des informations et le choix des entités relevantes et le rassemblement des événements, qui sont du travail sur dossier. L'élaboration des étiquettes est la première étape de l'analyse.

Il s'agit d'établir une structure (squelette des étiquettes) qui permette de contenir un certain nombre d'informations essentielles et qui sera utilisée systématiquement :

Description de l'événement			
4x4	§	Source	
Date	Heure	Index	

fig. 53 : Squelette d'une étiquette d'un diagramme chronologique

Il s'agit : de la description de l'événement, de l'évaluation de l'information (4x4<sup>230</sup>) et son type, de la source de l'information, de la date et de l'heure, de l'indexation et du no de page. Ces informations correspondantes se retrouvent dans le squelette de l'étiquette :

---

<sup>229</sup> MORRIS, Crime Analysis Charting, 1993

DUPONT sort de son véhicule à la Place de la Gare et entre dans le Café du Centre.		
C2	2	DUPONT Pierre
21/10/99	07:45	Aud 7/1

fig. 54 : Exemple de l'emplacement des informations dans le squelette des étiquettes

Chaque événement est saisi selon cette systématique dans des étiquettes. La représentation chronologique suit également certains standards.

Les axes de représentations sont les suivants :

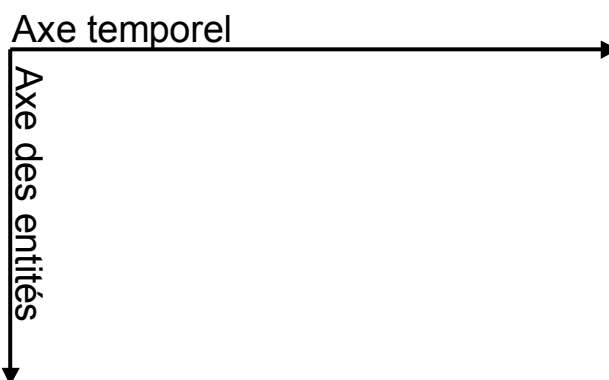


fig. 55 : Standard des axes représentation des schémas chronologiques

Un certain nombre de symboles sont utilisés pour la construction des lignes de temps :

<sup>230</sup> Le système dit « 4x4 » sert à l'évaluation de la qualité d'une information. Il est relativement répandu et se base sur deux questions : *Quelle est la qualité de la source ?* et *Quelle est la relation entre la source et l'information transmise ?* Les réponses possibles sont au nombre de 4 pour ces deux questions et une matrice 4x4 est établie. La qualité de la source est qualifiée de {A, B, C, X} dans un ordre dégressif le « X » signifiant inconnu. La relation de la source avec son information de {1, 2, 3, 4} si le témoignage est direct ou indirect avec quelques nuances.

		Source			
		Fiable: aucun doute raisonnable de confiance et de compétence.	Le plus souvent fiable: a rapporté en majorité des infos fiables.	Non fiable: a rapporté en majorité des infos non fiables.	Impossible de juger: nouvelle source d'infos, pas d'expérience.
Information		A	B	C	X
Certain: peut être considéré comme vrai sans aucun doute.	1	A1	B1	C1	X1
Observé par la source: en personne et rapporté à l'autorité compétente.	2	A2	B2	C2	X2
Entendu et confirmé: rapporté à la source et corroboré par d'autres éléments.	3	A3	B3	C3	X3
Entendu mais pas confirmé: rapporté à la source et pas corroboré.	4	A4	B4	C4	X4

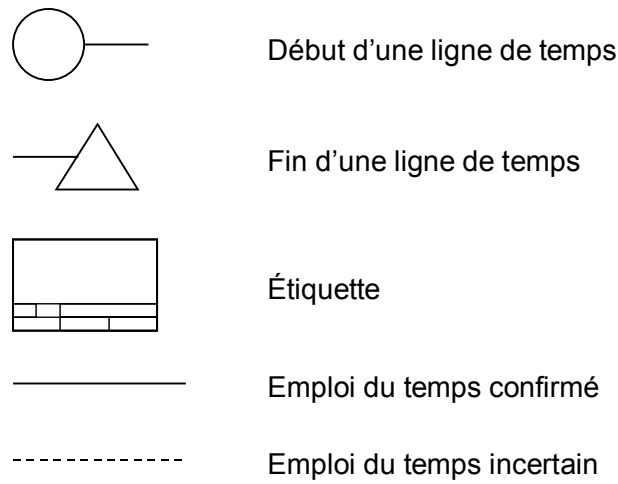


fig. 56 : Standards des symboles de représentation dans les schémas chronologiques

Ce qui peut donner l'exemple suivant :

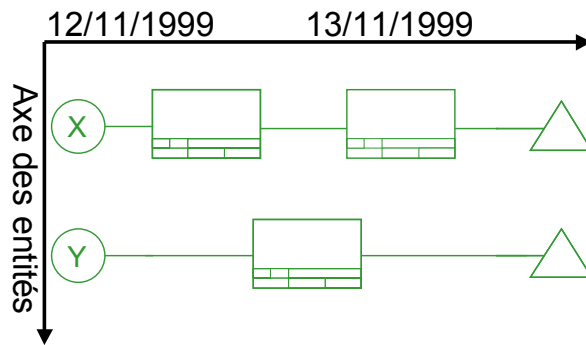


fig. 57 : Exemple de représentation chronologique standard

Lorsque des entités ont des parties de leur emploi du temps communes, il est nécessaire de clarifier le schéma en regroupant les lignes de temps. De même, la qualité de l'emploi du temps (certitude / incertitude) est symbolisée par l'emploi de pointillés.

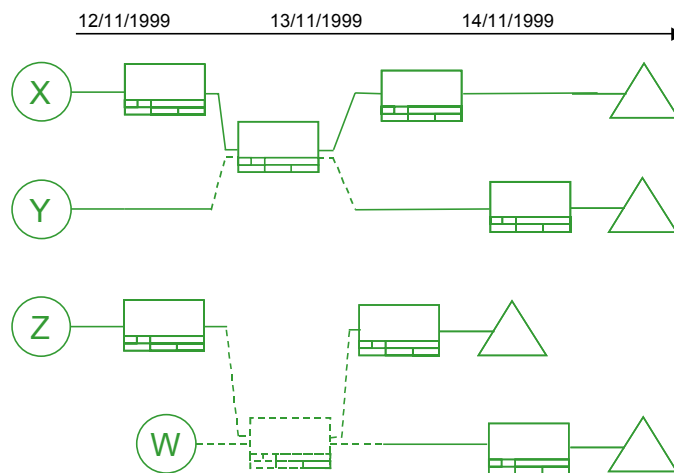


fig. 58 : Exemple de schéma chronologique standard clarifié

Les logiciels actuels n'apportent que peu de différences par rapport aux schémas originels. L'utilisation de couleurs permettait de rendre les schémas plus lisibles et l'informatique se chargeait de placer les événements par ordre chronologique.

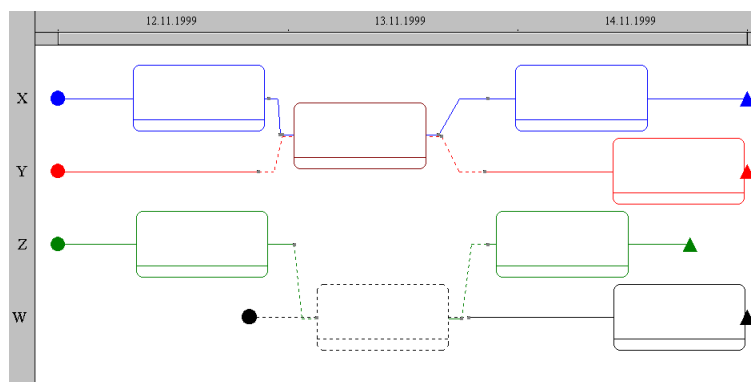


fig. 59 : Exemple de schéma chronologique avec les logiciels modernes

Une dernière version d'un logiciel de représentation graphique a réuni en un seul et même produit les représentations relationnelles et chronologiques. L'apparition des icônes dans les schémas chronologiques donne le résultat suivant :

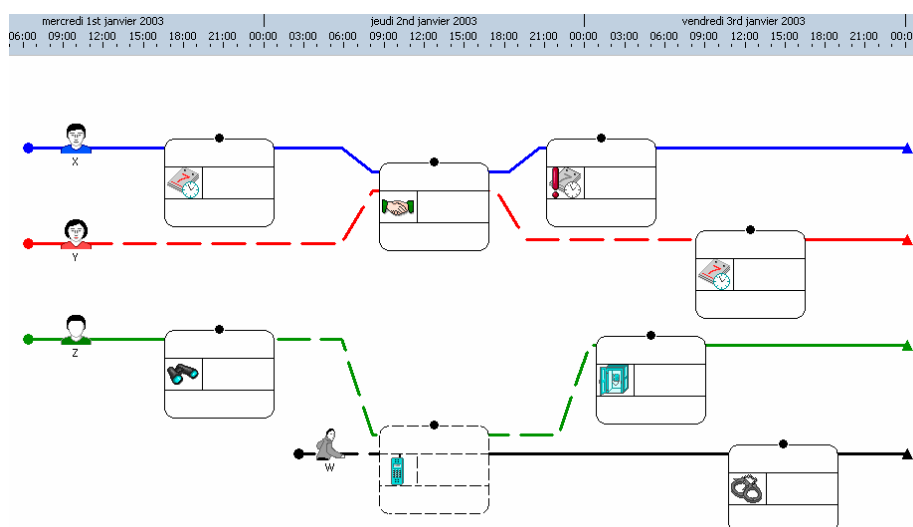


fig. 60 : Exemple de schéma chronologique avec les logiciels actuels

A l'instar des diagrammes relationnels, il est possible de représenter des flux de manière chronologique. Il s'agit de la même technique de représentation que le schéma de temps, mais avec l'indication du flux de biens, de marchandises ou d'informations représentés par une flèche entre les lignes de temps. Il s'agit de transactions de biens matériels ou immatériels, ou encore d'informations.

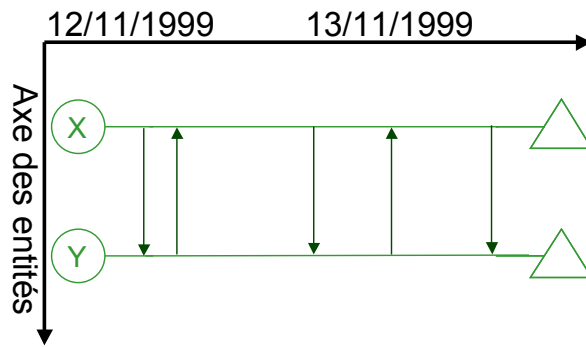


fig. 61 : Exemple de schéma de flux chronologique standard

Les schémas de flux chronologiques sont également très utiles pour l'analyse des contrôles techniques :

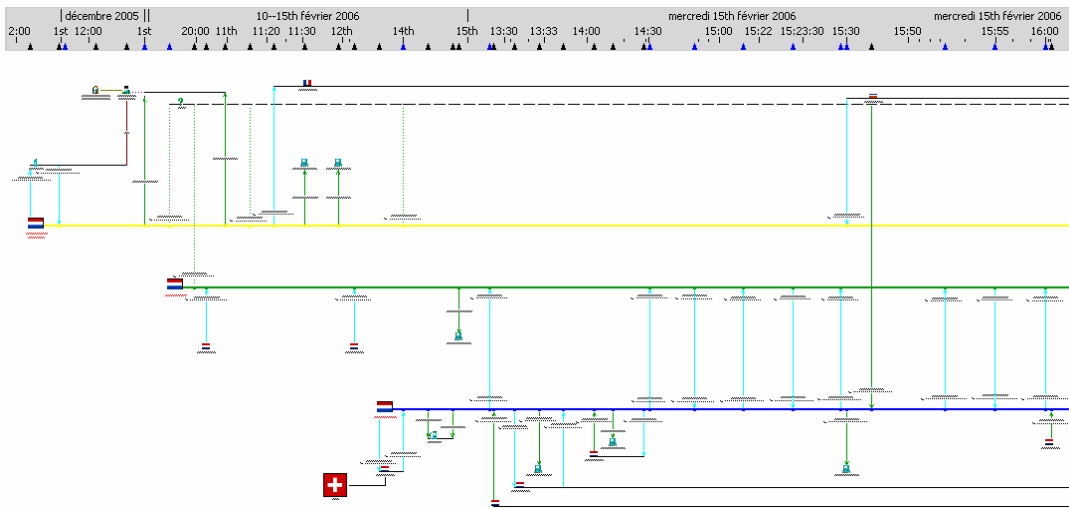


fig. 62 : Exemple de schéma de flux chronologique de connexions téléphoniques

Bien souvent, les schémas de temps comprennent une partie de flux. Il s'agit de schémas mixtes.

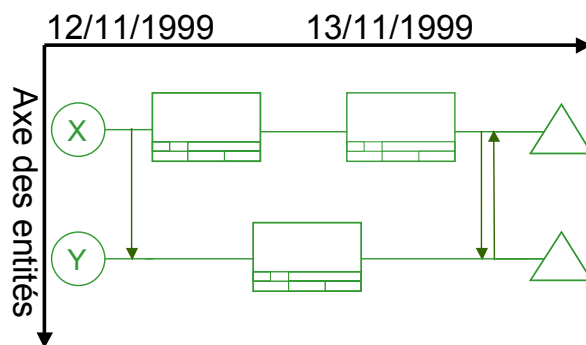


fig. 63 : Exemple de schéma chronologique mixte standard



Ce qui donne à l'aide des logiciels actuels :

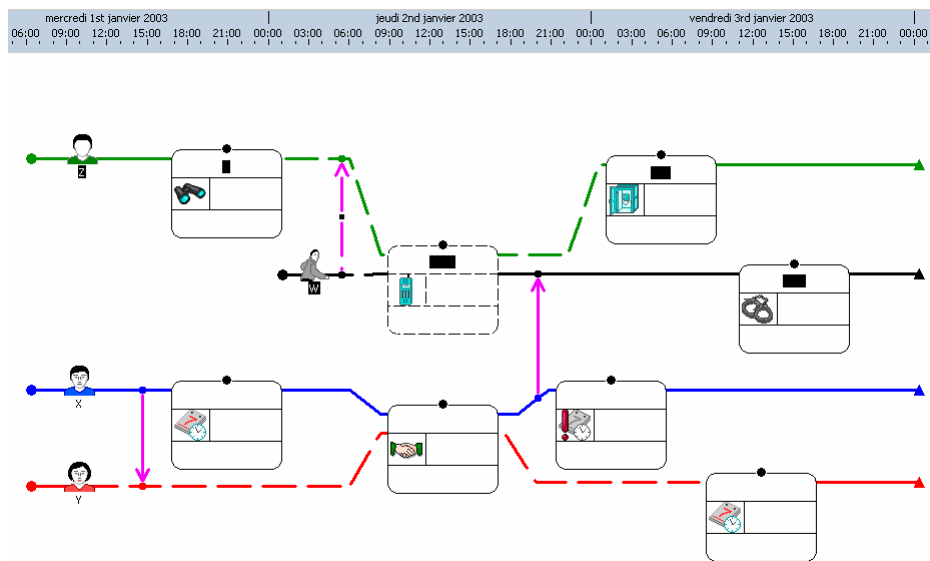


fig. 64 : Exemple de schéma chronologique mixte actuel

### 1.4.7 Synthèse

Dans cette dernière partie du chapitre 1, les techniques les plus utiles dans le contexte de la lutte contre la criminalité organisée ont été présentées. Mais, nous avons surtout voulu montrer que l'analyse criminelle se base sur un processus itératif du traitement de l'information, qui modélise un système d'apprentissage et qu'elle est ainsi liée à différents types de raisonnements, lorsqu'on synthétise des éléments ou qu'on les analyse.

Ce processus fondamental doit servir de base méthodologique pour construire notre réflexion sur le modèle du traitement de l'information dans le cadre de l'investigation en rapport avec la criminalité organisée. De plus, l'analyse criminelle se plaçant au sein de différents cadres qui l'influencent, il s'agit d'en tenir également compte dans nos réflexions.

Ainsi, nous disposons des éléments méthodologiques et contextuels qui nous permettent d'élaborer pragmatiquement, puis de proposer une organisation du flux de données et une architecture fondée sur deux composants informatiques constituant un système d'aide aux investigations criminelles dans le cadre de la lutte contre la criminalité organisée et constituant un véritable processus de renseignement criminel.

Le chapitre suivant pose différents postulats et hypothèses. Cela permettra de présenter dans le détail le projet de cette thèse qui vise à améliorer la lutte contre la criminalité organisée en Suisse en proposant un outil d'aide à l'enquête qui découle d'une méthode de travail explicite et qui s'inscrit dans des cadres organisationnels, structurels et légaux qui sont en mesure de le recevoir.



## 2 Le projet

Les sujets abordés au chapitre 1 ont montré que l'évolution de la société à la fin du siècle passé a eu des répercussions sur le crime en général. Par exemple, la plus grande mobilité des biens et des personnes a eu pour effet l'apparition de nouvelles formes de criminalité transfrontalière et internationale, parfois liée aux flux migratoires et aux déséquilibres économiques.

Les services de répression de la criminalité, que ce soit au niveau de la police ou de la justice, ont dû faire face à cette nouvelle criminalité qui s'organisait et dépassait les frontières de leur compétence géographique.

Les autorités ont alors rapidement constaté que dans la lutte contre la criminalité organisée on ne pouvait plus travailler efficacement sans partager l'information. Des systèmes d'information centralisés ont tenté de répondre à ce problème depuis le milieu des années 1990. Cependant, les efforts étaient encore trop souvent réduits à néant par des blocages légaux, économiques, structurels ou encore techniques produisant à chaque échelon des formes de *linkage blindness*, diminuant d'autant l'efficacité de l'ensemble.

Le rapport de situation 2000<sup>231</sup> de l'OFP constatait que la centralisation de l'information était nécessaire, mais qu'elle n'était pas suffisante et que sa conjonction avec les méthodes d'analyse criminelle n'avait encore que très rarement été utilisée. De ce fait, l'exploitation de l'information contenue dans les bases de connaissances n'était pas optimale et ne donnait que trop peu de résultats satisfaisants.

L'intégration des méthodes d'analyse criminelle dans un tel contexte doit passer par l'appréhension du processus de renseignement criminel dans sa globalité. L'intégration du cycle du renseignement à des systèmes d'aide à l'enquête peut s'apparenter aux démarches « qualité » qui ont été entreprises dans l'industrie et les services, lors de ces cinquante dernières années. Il convient donc de se s'assurer que le flux de données et les méthodes de travail s'intègrent dans les différents cadres politiques, légaux, économiques, ou encore structurels et qu'ils s'appuient sur des outils adéquats et rentables en terme d'utilisation.

Les outils d'analyse criminelle étant tributaires de l'information dont ils peuvent disposer, un système d'aide à l'enquête tel que proposé par cette recherche se doit d'être aussi proche que possible de la source principale des données. C'est pourquoi les bases de données d'enquête centralisées de la Confédération seront le point d'accrochage de ce projet.

Ce chapitre montrera que les architectures en exploitation jusqu'en 2005 ne permettaient pas réellement d'analyser les relations mises en lumière par les investigateurs, malgré d'importants efforts de gestion des liens.

---

<sup>231</sup> Voir chapitre 1.1.4

La transition sur un nouveau système de gestion de base de données qui était prévue devait servir de tremplin au projet, et si les revendications des analystes étaient prises en compte par les responsables du projet, sa réalisation devenait possible.

Les besoins des analystes, qui sont de disposer de données structurées et de suffisamment de souplesse logicielle afin de pouvoir intégrer les informations sans devoir tout ressaisir, puis de les analyser, pour pouvoir reconstituer petit à petit le puzzle, semblaient avoir été bien entendus par les responsables de la migration JANUS.

Il était illusoire de vouloir trouver dans le commerce, ou même de penser pouvoir créer un système unique qui réunisse en son seul sein les qualités nécessaires au partage national des informations en terme de sécurité et de gestion des droits d'accès, et qui offre suffisamment de souplesse aux analystes, tant les cahiers des charges sont différents et les besoins exprimés par chacun parfois même antinomiques.

Nous verrons plus en détail le projet de cette recherche qui était de proposer un modèle de flux d'informations suivant le cycle du renseignement et basé sur deux composants informatiques, dont le composant prototype de base de données d'analyse devait être créé et intégré afin qu'il puisse être couplé à la nouvelle base de données centralisée JANUS PV, cette dernière jouant le rôle de mémoire à long terme. Il s'agissait de trouver le bon équilibre pour le futur « sous-système »<sup>232</sup> JANUS PV entre les besoins des enquêteurs et des analystes, afin de permettre à cette base de données d'enquête centralisée d'une part de répondre rapidement et simplement aux interrogations de routine des enquêteurs, et d'autre part de disposer de données suffisamment structurées pour que les données puissent être exportées dans le composant externe et que des analyses puissent y être réalisées.

Dans ce deuxième chapitre, nous allons relever certains points critiques de la situation au début des années 2000 dans la gestion des liens se rapportant aux investigations sur la criminalité organisée.

En introduction, nous poserons trois postulats, qui définissent des stratégies et des méthodes de travail impératives et déjà rencontrées de manière récurrente dans ce type d'investigation criminelle. Afin d'illustrer nos propos, nous reprendrons une analogie, notamment faite par KIND<sup>233</sup>, entre le travail de reconstruction d'une situation par l'enquêteur et le jeu du puzzle, celui-ci étant, comme le relève cet auteur, assorti de quelques complications :

« In a sense the trial process is rather like assembling a jigsaw with the aid of a picture on the box, keeping in mind the possibility that pieces of jigsaw may have been stored in the wrong box. Consider now the position of the investigator. To use the same rather facile example, he is more in the position of someone who is assembling a jigsaw without the

---

<sup>232</sup> Le système JANUS se compose de plusieurs « sous-systèmes ». Voir chap. 1.3.4.

<sup>233</sup> KIND, *The Scientific Investigation of Crime*, 1987

aid of a picture. Like all similes the jigsaw one is not perfect. It could perhaps be refined by saying that the pieces are re-cut into random shapes and sizes each time the game is played, and that some pieces are always missing, and that the essential step is to elect whether the picture built up is sufficiently like some other picture to enable a proposition that they are the same. This represents the point where the investigator has to make up his mind if he has enough evidence to go to court. » (p.10)

Plus récemment, CHISUM et TURVEY<sup>234</sup> adeptes du courant *reconstructionniste* reprennent encore cette même allégorie et posent la question qui en découle naturellement :

« Crime reconstruction requires the ability to put together a puzzle using pieces of unknown dimensions without a guiding picture. The next logical question is only this: How? » (p.127)

Nous illustrerons donc les postulats par cette parabole, ainsi que par des expériences rencontrées jusqu'ici dans la pratique des investigations.

Suivra ensuite la description du projet pratique de cette recherche qui s'efforce de tenir compte de la spécificité des besoins de chaque acteur intervenant dans l'enquête (policier ou analyste).

Enfin, deux hypothèses découlant du projet seront posées. La première hypothèse portant sur la faisabilité d'un tel système d'aide à l'enquête et la seconde portant sur son utilité.

---

<sup>234</sup> CHISUM & TURVEY, Crime Reconstruction, 2007

## 2.1 *Postulat 1 – besoin de partager les informations*

**En matière d’investigation sur la criminalité organisée, le partage d’informations est devenu impératif. A l’heure actuelle, il doit notamment se faire grâce à des outils à haut potentiel qualitatif et quantitatif, comme une base de données *commune* aux unités d’enquête et *structurée* en fonction du but recherché.**

### 2.1.1 **Parabole du puzzle**

Imaginons la situation d’un groupe de joueurs qui a pour but commun de deviner et de décrire (si possible du premier coup et sans se tromper) une image représentée sur un puzzle. Au début du jeu, chaque joueur reçoit un nombre inégal de pièces du puzzle. Puis à chaque tour du jeu, pour obtenir des pièces supplémentaires, les joueurs doivent faire des hypothèses sur les pièces qui manquent, que ce soit sur leur contenu ou sur les liens qu’elles ont avec les pièces déjà posées. Quelle sera la meilleure stratégie que le groupe pourra adopter ?

#### 2.1.1.1 **Base de données commune**

Sans pièces, ou juste avec quelques-unes, il n’est pas possible de recomposer l’image du puzzle, ou alors d’une manière trop incertaine. La meilleure stratégie, est sans aucun doute de rassembler le plus grand nombre de pièces à disposition de chacun des joueurs, avant de se lancer dans une reconstruction commune du puzzle.

Dans le monde réel, les éléments de base sont *les données*. Les données récoltées constituent les pièces du puzzle.

La meilleure stratégie est donc de regrouper le plus grand nombre de données dès le départ. La mise en commun *a priori* des données ne peut se concrétiser que par la réalisation d’une *base de données commune*.

#### 2.1.1.2 **Base de données structurée**

Toujours par analogie avec le jeu décrit plus haut, chaque pièce du puzzle a des caractéristiques bien définies, soit :

- une signification (donnée par l’image partielle qui y est représentée),
- des relations (définies par ses bordures, elles-mêmes caractérisées par des formes convexes ou concaves qui permettent d’assembler les pièces).

Il est évidemment plus difficile de réaliser un puzzle dont le sujet est abstrait ou même inexistant en ne se basant que sur la forme des pièces. De même, si toutes les pièces sont exemptes de bordures caractéristiques (par exemple polygonales) il n’est plus possible de profiter de ces caractéristiques

pour tester l'hypothèse du bon positionnement d'une pièce par rapport aux autres. Afin que les puzzles soient réalisables, ils disposent (sauf exception) de ces deux caractéristiques.

Dans le monde réel, les informations de la base de données commune doivent disposer des mêmes caractéristiques, soit :

- une signification propre, (même si forcément partielle lorsqu'elle est sortie de son contexte),
- des relations (de différents types avec les autres informations).

Les possibilités de mise en relation doivent être, à l'image du puzzle, *simples* et *définies a priori*. La définition de la structure et des possibilités de mise en relation des informations doivent être prédéfinies et standardisées, donc *structurées*. Cette structure doit être motivée par le but recherché.

### 2.1.2 Situation actuelle

L'idée de la mise en commun des informations de police n'est évidemment pas nouvelle, puisqu'on en parlait déjà dans les années 1960. Toutefois, KREIS<sup>235</sup> met en évidence les énormes difficultés rencontrées sur près de trente ans, qui ont amené l'échec du KIS (*Kriminalpolizei Information System*)<sup>236</sup>.

Finalement, ce n'est qu'après l'affaire des fiches et une réorganisation importante au niveau de la Confédération que les premières bases de données d'enquête centralisées ont enfin abouti.

Dès lors, les bases de données que la Confédération avait mises en place pour la résolution d'enquêtes spécifiques ont évolué favorablement dans ce sens, aussi bien sur un plan technique que juridique (DOSIS, ISOK, FAMP, puis JANUS)<sup>237</sup>.

Même si l'utilisation du système JANUS n'est pas obligatoire et qu'il est exploité préférentiellement par les services de lutte contre le trafic de stupéfiants (qui sont à la base de son apparition), tous les cantons s'en servent avec plus ou moins d'assiduité.

Des statistiques de 2002<sup>238</sup> montraient que des informations de tous les cantons y figuraient. Si trois cantons et deux demi-cantons n'avaient rien saisi eux-mêmes en 2002, la Confédération avait comblé cette lacune.

Cette année là, sur les quelques 10'000 identités saisies dans le système, environ 7'000 l'avaient encore été par la Confédération. Les cantons les plus assidus étant Zurich (1200), Vaud (500), Genève (300), Saint-Gall (200) et Argovie (200).

Ces statistiques montrent bien qu'en 2002 la Confédération compensait encore largement le défaut de saisie des cantons. Il est à espérer qu'à l'avenir les cantons prennent à leur charge cette tâche et profitent ainsi eux-mêmes directement des avantages du système partagé et centralisé. A cet égard, des cours de sensibilisation sont dispensés depuis de nombreuses années à tous les niveaux

---

<sup>235</sup> KREIS, *op. cit.*, 1993

<sup>236</sup> Voir chapitre 1.3.3

<sup>237</sup> Voir chapitre 1.3.4

<sup>238</sup> Produites et aimablement transmises en 2003 par J.-D. HERITIER, premier chef DAO, BAAC - VD.

(enquêteur, spécialiste ou officier de police) lors des cours organisés sous l'égide de l'Institut Suisse de Police (ISP).

La nécessité d'une mise en commun des informations ne peut plus être remise en question. Ce constat, né il y a près de 50 ans, peine pourtant toujours à être mis en pratique. La principale difficulté est la nature fédéraliste de notre pays, qui complique les procédures lors de la réalisation, puis lors de l'exploitation de tels systèmes centraux. L'impression de redondance avec les systèmes cantonaux, sans mesurer le profit d'une telle démarche de mise en commun des informations, est malheureusement parfois encore bien présente dans les cantons.

Les premières expériences réalisées avec DOSIS ont été faites selon la perception des besoins et des connaissances d'enquêteurs. Elles ont amené une série de problèmes et de questions qui permettent aujourd'hui de faire des propositions concrètes sur des formes d'exploitation possibles et sur une structure des données (modèle conceptuel) plus élaborée et mieux adaptée aux nouvelles méthodes d'analyse criminelle opérationnelle.

Il existe bien entendu d'autres modèles distribués<sup>239</sup> possibles. Mais, celui d'une base de données comporte des avantages importants sur les plans quantitatifs (la quantité d'informations contenue dans le système), qualitatifs (la qualité des informations contenues, déterminée par la structure interne choisie), ainsi que sur les plans de la sécurité et de la pérennité des données, qui sont dans ce contexte particulièrement importants.

On acceptera donc le postulat qu'une telle base de données est nécessaire. Mais nous n'avons pas encore précisé le modèle sur lequel il convient de la faire fonctionner. C'est tout l'enjeu de ce travail, l'enquête judiciaire étant en effet peu formalisée. Il existe tout un éventail de stratégies d'enquête, certes empiriques, mais pragmatiques. Elles sont reprises au postulat suivant.

---

<sup>239</sup> Certains modèles distribués sont nés et ont pris de l'importance notamment avec l'apparition d'Internet, comme source d'informations.



## 2.2 *Postulat 2 – besoin de reconstruire une situation*

**Dans toute enquête criminelle, on cherche à reconstruire une situation passée ou présente, selon les trois dimensions de l'enquête (entités, temps et lieux). Dans le cas particulier de la criminalité organisée, la stratégie d'enquête passe par la détermination du rôle et de l'implication de chacun des protagonistes dans le groupement criminel apparaissant lors des investigations.**

### 2.2.1 **Parabole du puzzle**

Lorsque les joueurs disposent de plusieurs pièces d'un puzzle, il est naturel qu'ils cherchent à les assembler. C'est une étape indispensable. Pour pouvoir décrire l'image représentée, il est nécessaire d'y reconnaître les éléments principaux, d'identifier qui ils sont, ce qu'ils font, et de pouvoir dire où, quand et comment.

La construction du puzzle par le groupe de joueurs se passe en étapes successives et répétitives d'analyse. Par des raisonnements récursifs les joueurs recherchent l'image globale du puzzle alors que par des raisonnements progressifs ils testent et valident les hypothèses émises auparavant.

#### 2.2.1.1 **Besoin de mettre des personnes en relation**

Les pièces du puzzle ayant une signification et des possibilités de mise en relation, les joueurs vont rechercher, dans un premier temps, parmi celles qui sont à leur disposition, les pièces qui leur permettent de répondre à une première question : qui ? (ou éventuellement quoi ? si aucun individu est représenté), qui constitue l'élément central et essentiel à la description de l'image globale. Ensuite, ils vont tenter d'assembler petit à petit le reste du puzzle, afin de comprendre le contexte détaillé une fois que les pièces sont toutes mises ensemble.

Dans les enquêtes, il en est de même. La première préoccupation est de pouvoir identifier les personnes. S'il n'est souvent pas possible dans la phase préliminaire de les identifier « formellement », c'est-à-dire de connaître leur véritable identité, il est tout du moins nécessaire de pouvoir les différencier et les reconnaître durant la phase d'investigation discrète et de se donner les moyens de pouvoir les identifier *in fine*.

Parallèlement, pour tenter de savoir ce que font les membres d'une organisation criminelle, il est absolument indispensable de pouvoir établir quels sont les contacts entre les différents protagonistes.

Il s'agit donc de mettre en relation les éléments centraux des organisations que sont les personnes qui les composent. Le but est de pouvoir imaginer, par une démarche analytique qui y participe, pour y faire quoi, quand, où et comment.

### 2.2.1.2 Besoin de disposer d'éléments factuels

Les éléments principaux du puzzle sont rarement en interaction directe. Des éléments intermédiaires permettent de les lier. Ce sont ces mêmes éléments intermédiaires qui permettent de comprendre, puis d'expliquer ce qui lie les éléments centraux, comment et pourquoi. Les éléments intermédiaires ont un rôle important dans la reconstruction du puzzle. C'est grâce à eux, par exemple que les joueurs pourront générer et tester leurs hypothèses, puis plus tard valider celle qui leur semble être la bonne.

Dans le contexte judiciaire, les éléments factuels sont d'une extrême importance. Ces données que l'on peut aussi qualifier d'objectives, dans le sens qu'il s'agit de faits avérés et démontrables, constituent les prémisses des raisonnements analytiques ou déductifs.

S'il est satisfaisant de pouvoir comprendre qui sont les acteurs d'un trafic criminel, ou qui sont les auteurs de délits sériels, ce n'est de loin pas suffisant, en droit, si l'on ne peut l'expliquer, c'est-à-dire le démontrer, le prouver.

Ces éléments factuels sont ceux qui permettent de mettre des personnes en relation, selon les trois dimensions de l'enquête : *entités et leurs relations* (personnes et objets), *temps* et *lieux*<sup>240</sup>. Ainsi, dans la première dimension, on retrouvera par exemple les moyens de communication, de transport, ou la propriété, l'utilisation et le transfert de biens. Dans la deuxième dimension, on peut mentionner des événements qui lient des personnes, soit des rencontres, ou encore des événements spécifiquement judiciaires comme des crimes ou délits et les opérations de police qui peuvent intervenir dans les investigations. Enfin, la dernière dimension est composée des lieux géographiques<sup>241</sup>, souvent reliés à un événement particulier, impliquant une ou plusieurs personnes.

### 2.2.2 Situation actuelle

La base de données commune JANUS, constituée des deux « sous-systèmes » PV et JO, a été élaborée sur la base de DOSIS, elle-même créée par et pour des enquêteurs dans le cadre d'importantes affaires de trafic de stupéfiants. DOSIS était donc extrêmement pragmatique et semblait répondre assez fidèlement aux besoins spécifiques des enquêteurs.

Le « sous-système » PV se focalisait sur les personnes dont il faisait l'élément central et il permettait de contenir les informations associées à ces personnes, qui étaient constituées d'antécédents en texte libre. Dans ce texte libre, se trouvaient des renvois à d'autres entités, telles que d'autres personnes, objets, événements, moyens de communication, etc. Ces relations avec d'autres entités étaient effectuées à l'aide de marqueurs dans le texte et quelques règles de syntaxe. Il s'agissait des « sous-champs » des antécédents.

---

<sup>240</sup> Voir chapitre 1.2.2 – Les dimensions de l'enquête

<sup>241</sup> Sans oublier également ici l'espace virtuel qu'est aujourd'hui Internet et qui est un lieu de villégiature de la criminalité organisée. Cependant, les utilisateurs de cet espace global sont eux bien réels et il s'agira de les rechercher, de les localiser de les identifier.

Cette base de données était très utile afin de rechercher les liens entre les différents protagonistes (personnes) qui apparaissaient dans les diverses investigations en cours sur le territoire suisse. Nous avons vu qu'en 2002, les polices suisses avaient introduit environ 10'000 nouvelles personnes, dont une partie n'est d'ailleurs même pas établie dans notre pays.

Si un tel système centralisé est d'une extrême utilité quand il s'agit de rechercher des liens parmi cette masse d'informations (dans laquelle il faut compter les dizaines de milliers d'autres entités associées tels que des lieux, des objets ou encore des moyens de communication), il l'est beaucoup moins lorsqu'il s'agit d'interpréter la signification de ces liens.

L'existence d'un lien ne signifiant pas forcément toujours que deux personnes se connaissent réellement et encore moins qu'elles collaborent au sein d'un groupement criminel. Ainsi, deux personnes peuvent habiter à la même adresse ou avoir eu des contacts avec les mêmes interlocuteurs, sans même se connaître, et encore moins être complices d'actes délictueux.

L'interprétation de toutes ces relations nécessite une étape supplémentaire à part entière dans le traitement de l'information. Cette étape fait d'ailleurs partie de la panoplie d'outils proposés par l'analyse criminelle opérationnelle.

## **2.3 Postulat 3 – besoin d’analyser la situation**

**Le nombre et la complexité des relations en rapport avec une affaire particulière, ou par extension à plusieurs cas, nécessitent la mise en place d’un système d’analyse dynamique qui permette dans un premier temps d’apprécier une situation de départ et dans un second temps d’adapter son appréciation en fonction des nouveaux éléments.**

### **2.3.1 Parole du puzzle**

En poursuivant la mise en parallèle avec le jeu du puzzle avec des moyens mis à disposition début 2000 par les bases de données centralisées, on se retrouverait dans une situation où le maître du jeu aurait en fait pris et caché les pièces mises en commun par les joueurs, et il aurait construit le puzzle de son côté. Il donnerait les résultats de l’assemblage des pièces du puzzle aux joueurs par oral ou par écrit, soit ce qui est dessiné sur les pièces, quels en sont les contours, éventuellement les liaisons existantes. Les joueurs devraient donc se représenter mentalement la situation, émettre leurs hypothèses afin de rechercher des pièces supplémentaires et finalement jouer leur va-tout sur l’image qu’ils imagineraient être représentée par l’assemblage des pièces du puzzle. Il paraît ici évident que le jeu deviendrait vite difficile, voire impossible et qu’il nécessiterait bien plus de temps.

#### **2.3.1.1 Besoin d’un outil de représentation (visualisation graphique)**

Confrontés à cette nouvelle manière de jouer, certains joueurs vont rapidement vouloir représenter graphiquement les descriptions du maître du jeu, et en quelque sorte reproduire le puzzle selon un modèle qui leur sera propre. Ils pourront ainsi se libérer l’esprit de la charge de représentation mentale et augmenter ainsi la qualité de leurs hypothèses, en se basant sur des éléments qui seront moins déformés par des erreurs de mémorisation. Ils pourront également plus facilement expliquer à leurs camarades de jeu, par l’argumentation, leurs hypothèses ainsi formulées.

Dans le monde réel, l’enquêteur a également rapidement compris que des schémas peuvent lui venir en aide. Les méthodes d’analyse criminelle développées dans les années 1970 aux Etats-Unis vont dans ce sens. Différents types de représentations ont été rapidement identifiés comme étant la réponse appropriée à certaines situations récurrentes dans l’enquête policière. Ainsi, les schémas de relations et de temps se sont rapidement imposés.

#### **2.3.1.2 Besoin d’un outil évolutif (base de données)**

Le jeu se poursuivant, de nouvelles pièces vont se rapporter au puzzle, celles-ci étant à nouveau décrites aux joueurs par le maître du jeu. Ces derniers vont donc devoir adapter et faire évoluer leur représentation en regard de ces nouvelles informations. Certaines pièces peuvent soudain apporter

un éclairage totalement nouveau et remettre en question l'ensemble du dessin établi jusqu'ici. Disposer d'outils informatiques facilite désormais grandement la mise à jour des représentations graphiques. Les ressources nécessaires à la mise à jour des représentations ne sont toutefois pas négligeables. Disposer des outils et des connaissances appropriés est alors un élément stratégique déterminant.

Dans le monde policier, les nouveaux logiciels de visualisation graphique développés depuis les années 1990 fournissent enfin des fonctionnalités propres à faciliter la schématisation et la mise à jour des représentations. Cependant, la masse d'information, le niveau de détail et le rythme de l'enquête peuvent demander des ressources très importantes pour assurer le suivi. De plus, les schémas peuvent rapidement souffrir d'un surplus d'informations non pertinentes. Il est donc nécessaire de travailler avec des outils qui permettent de faire abstraction de certains éléments pour pouvoir se focaliser sur d'autres, tout en conservant le pouvoir de liaison des éléments momentanément ignorés. Les bases de données d'enquête couplées à des systèmes de représentation graphiques sont aptes à couvrir ce besoin.

### **2.3.1.3 Besoin d'un système d'analyse dynamique (base de données d'analyse)**

La taille des pièces représente le niveau de détail avec lequel on va devoir reconstituer le puzzle. Plus il y a de pièces, plus le puzzle est difficile et plus le jeu est long. Deviner le plus rapidement possible l'image représentée par un puzzle constitué de toutes petites pièces est effectivement un travail fastidieux et difficile. Il s'agira pour le groupe de joueurs d'élaborer des stratégies. Par exemple, ils peuvent décider de se focaliser sur des groupes de pièces hautement informatifs (représentant des personnes ou des choses) et de délaisser dans un premier temps des parties représentant des éléments moins informatifs (le ciel, le sol, etc.). Il s'agit pourtant de ne pas les oublier complètement, car c'est au regard de cet environnement que des hypothèses peuvent être écartées ou confirmées. Par exemple, une partie bleue peut représenter soit le ciel, soit la mer et influencer ainsi grandement l'image générale. Ou alors, les joueurs peuvent vouloir décomposer l'image en plusieurs sous-images et se partager le travail en se spécialisant et en analysant ensuite les implications relatives à leurs propres parties et à leur mise en commun pour s'en sortir à meilleur compte.

Sans décomposition en sous-problèmes, plus les informations de base sont détaillées, moins l'analyse générale de la situation sera fine. Or, dans le système judiciaire, l'appréciation des faits nécessite toujours un niveau de détail très important (les faits devant être démontrables pour avoir la qualité de preuve). Ce système impose donc, si l'on veut être compatible avec cette exigence, de travailler avec de très petites pièces, ce qui augmente, dans un premier temps la complexité du puzzle à reconstituer, et par la suite la difficulté de la lecture de l'image globale qu'il représente. La décomposition de l'enquête en parties spécifiques traitées par différents spécialistes dans un système commun peut être une clé de la réussite.

### 2.3.2 Situation actuelle

L'application de l'analyse criminelle dans le contexte de la criminalité organisée n'est également pas une idée novatrice, puisque c'est justement ce contexte qui l'a fait naître.

Nous avons vu que les outils utilisés dans l'analyse criminelle, particulièrement ceux qui permettent d'établir des schémas de relations correspondent très exactement à la problématique présente et que ceux-ci sont très souvent nécessaires à la résolution d'affaires complexes. Un constat de l'utilisation encore insuffisante de ces moyens était même déjà fait en Suisse en 2000<sup>242</sup>.

Mais, les outils seuls ne suffisent pas. L'analyse criminelle est une méthode qui doit être appliquée en adéquation avec les contraintes contextuelles. Elle ne doit pas se réduire à de simples outils de visualisation graphique. Jusqu'ici, une telle démarche n'a, à ma connaissance et dans ce contexte, jamais été entreprise en Suisse.

Une difficulté supplémentaire apparaît de manière critique lors de la première étape de l'enquête (recherche / identifier – localiser), lors de l'assemblage d'informations pour la reconstruction de la situation. Elle réside dans le fait qu'il manque très souvent un nombre important de pièces. Les données sont toujours incomplètes et bien souvent incertaines.

L'image globale donnée par ce drôle d'assemblage ne peut donc être ni certaine, ni univoque et le but de chacun est de trouver les bonnes pièces, de compléter le puzzle, pour finalement laisser la plus petite place possible au doute. Cette recherche intense d'éléments factuels complémentaires constitue le travail essentiel de l'investigation et occupe également une part prépondérante dans la seconde étape de l'enquête de police qui suit les interpellations (Enquêter / structuration de la preuve)<sup>243</sup>.

Afin de diminuer le risque d'erreurs, l'application systématique et rigoureuse de la méthode d'analyse criminelle, qui fonctionne selon le cycle du renseignement est un gage de sécurité.

Comment imaginer pouvoir réaliser un puzzle incomplet et dont certaines pièces sont floues, de plusieurs dizaines, centaines ou milliers de pièces en se rappelant la position de chacune des pièces relativement aux autres et en tirer l'image globale. Telle est la mission de l'investigateur qui est confronté à la criminalité organisée. Sans auxiliaire, cette mission est extrêmement difficile, si ce n'est impossible.

---

<sup>242</sup> Voir chapitre 1.1.4 – Survol de l'état de la lutte contre la criminalité organisée en Suisse

<sup>243</sup> Voir chapitre 1.2.4 – Les étapes du processus d'enquête

## 2.4 Description du projet

Nous allons maintenant présenter le processus de traitement de l'information et d'analyse qui constitue le concept du projet de ce travail de recherche, soit la gestion et l'analyse des liens dans le cadre de l'investigation criminelle sur la criminalité organisée.

Un point fondamental doit toutefois encore être pris en considération, avant de passer à la description du projet. Il s'agit des besoins des différents intervenants dans la lutte contre la criminalité organisée. Comme on l'a vu dans le chapitre qui traite de l'enquête<sup>244</sup>, la lutte contre la criminalité organisée est un travail d'équipe et à plus large échelle une collaboration de toutes les autorités de poursuite pénale. Cette constatation implique que différents types d'intervenants vont avoir leur rôle à jouer. Et chacun d'eux a des besoins bien différents.

### 2.4.1 Besoins de chaque intervenant

Parmi les intervenants qui vont interagir lors de l'investigation policière, nous en différencions sommairement deux, les *enquêteurs* et les *analystes*. Il peut très bien s'agir de la même personne poursuivant différents buts à un moment ou à un autre de l'enquête, que ce soit des actes purs d'enquête (recherches, contrôles, vérifications, etc.) ou d'autres actes d'analyse (appréciation d'une situation, élaboration d'hypothèses et de recommandations). Il endosse donc des *rôles* différents.

Lors de ces différentes activités, les besoins ne sont pas les mêmes. Par conséquent, les méthodes de travail sont développées par chacun dans le but de remplir sa mission au plus vite et au moindre coût. Il y a donc de grands risques que les méthodes et les moyens engagés par l'*enquêteur* et l'*analyste* divergent pour ne finalement plus être tout à fait compatibles, s'ils ne tiennent pas compte l'un de l'autre.

#### 2.4.1.1 Besoins de l'enquêteur

Les besoins de l'enquêteur découlent des tâches qu'il doit remplir. Mis à part le fait que l'enquêteur va choisir sa source en fonction de sa fiabilité<sup>245</sup>, également dans la mise à jour des informations qui y figurent, lorsque son activité est de rechercher des informations, de vérifier une identité dans une base de données, de contrôler un numéro d'immatriculation ou de téléphone, ses besoins se résument à quatre mots clés :

- Rapidité
- Simplicité

---

<sup>244</sup> Chapitre 1.2 – L'enquête

<sup>245</sup> Rappelons ici que l'évaluation de l'information elle-même est une étape à part entière du cycle du renseignement et que c'est non seulement la fiabilité de la source qui doit être évaluée, mais également le lien existant entre cette source et l'information qu'elle transmet, comme le préfigure par exemple le modèle d'évaluation 4x4.

- Centralisation<sup>246</sup>
- Exhaustivité

### Rapidité

Plus la recherche est rapide, plus le bénéfice est net. Les moyens informatiques actuels rendent la recherche extrêmement rapide par rapport à la masse d'information concernée par la requête. On ne peut plus se passer aujourd'hui de ces outils informatiques.

### Simplicité

Une recherche doit être simple. Là, de nouveau, les moyens informatiques permettent de rechercher simplement (sans se soucier du classement des informations, de leur inventoriage et de leur indexation). Cependant, il faut que les critères de recherche et que les formats de données soient précisément définis.

La simplicité d'accès aux informations joue également un rôle important. Si l'accès est rendu difficile par des mesures de sécurité<sup>247</sup> trop strictes, les utilisateurs trouvent, au mieux, des stratégies de remplacement (par exemple en déléguant le travail à de jeunes collègues ou à du personnel administratif), ou, au pire, ils délaissent l'outil.

### Centralisation

La disponibilité des données est un souci très actuel des politiques et par conséquent, à l'autre bout de la chaîne, des développeurs de bases de données de police<sup>248</sup>. Les outils informatiques d'aujourd'hui demandent à l'utilisateur beaucoup moins d'efforts de maintenance des données (classification, indexation, etc.). Les bases peuvent contenir des quantités d'informations toujours plus importantes et donc s'étendre à des ensembles géographiques beaucoup plus vastes<sup>249</sup>. Le

---

<sup>246</sup> Comme on l'a vu précédemment, le modèle de distribution de données par des systèmes de bases de données sécurisés et centralisés est celui qui correspond encore le mieux au contexte judiciaire et policier. Le mot « centralisation » doit être pris ici comme la *mise en commun d'informations provenant d'entités politiquement, légalement ou structurellement distinctes*.

<sup>247</sup> Par exemple, un rythme de changement de mots de passe plus rapide que la fréquence d'accès de l'utilisateur à la base de données provoque un blocage quasi perpétuel.

<sup>248</sup> Au niveau européen, l'espace Schengen dispose d'un index commun des personnes recherchées et des objets volés (SIS). La Suisse ayant accepté le référendum sur ce point en juin 2005, il est probable qu'elle intègre à ce système, par différentes passerelles, les données contenues dans la base suisse qui poursuit le même but (RIPOL).

<sup>249</sup> Au niveau suisse, on peut encore citer le projet *SuissePol-Index* qui a pour but de regrouper en un index les identités des personnes concernées par les registres de police cantonaux et par la police judiciaire fédérale. En une seule recherche, on devrait pouvoir vérifier si une personne est (ou a été) concernée par une procédure judiciaire en Suisse. Si le contrôle est positif, il faut alors s'adresser au corps de police concerné pour disposer des détails de la procédure. Le projet a démarré sa phase opérationnelle en été 2005. Il est prévu de réaliser cet index en trois phases : la première consiste en une recherche manuelle qui est assurée par la centrale d'engagement de la PJF dans ses propres données et dans les données cantonales ; la deuxième phase est semi-automatique, puisque les recherches dans les bases de la Confédération (JANUS et IPAS) seront automatiques alors que ce sera toujours manuel pour les bases cantonales ; enfin la troisième phase devrait être totalement automatique. Cette dernière phase ne devrait pas voir le jour avant 2010.



regroupement des données n'est en général plus limité par les ressources nécessaires à leur exploitation, mais par des normes légales ou des choix politiques qui ne sont pas toujours en phase avec les besoins opérationnels des autorités de poursuite pénale.

En Suisse, le regroupement des registres communaux au niveau cantonal, de même que les registres cantonaux au niveau national sont des démonstrations de ce souci de centralisation.

La centralisation de l'information permet donc de gagner du temps par une recherche unique et augmente ainsi la simplicité puisque l'on couvre un territoire plus grand, cela évitant des recherches et des contrôles répétés dans plusieurs registres locaux. D'un autre côté, elle peut dans certaines situations produire une masse de données pertinentes qu'il n'est plus possible d'apprécier simplement.

### Exhaustivité

L'exhaustivité de la recherche ou du contrôle veut dire qu'en une seule opération, l'action a porté sur l'ensemble des données contenues dans la base de données.

Par exemple, pour vérifier la présence d'une personne, s'il faut rechercher de manière répétitive dans plusieurs rubriques de la même base, il est vraisemblable que des utilisateurs occasionnels oublient les rubriques connexes qui peuvent pourtant potentiellement contenir l'information qu'ils recherchent. On parlera ici de problèmes structurels liés à la base de données elle-même. On résume souvent cette préoccupation de l'utilisateur par la phrase « Tout devrait apparaître en un seul clic » !

Les moteurs de recherche que l'on trouve sur Internet<sup>250</sup> sont un excellent exemple de systèmes qui correspondent aux critères énoncés ci-dessus : le moteur de recherche est rapide. Il contient un index de milliards de pages Internet.

D'accès aisé, des fonctions de recherches simples sont proposées par défaut, l'accès à des moyens de recherche avancés se faisant sur requête de l'utilisateur.

La portée d'un tel moteur de recherche est telle qu'on la considère souvent comme quasiment illimitée. Il centralise les informations du monde entier. A un tel point que les systèmes doivent maintenant permettre de limiter la portée de la recherche à une langue ou à un pays précis, afin de ne pas être submergé par un trop grand nombre d'occurrences positives.

Le moteur de recherche regroupe par son indexation des informations qui peuvent être contenues dans des supports de types différents, comme les pages web ou les documents mis en ligne (\*.pdf, \*.doc, etc.). En une seule recherche, on couvre donc une grande partie de l'information mise en ligne.<sup>251</sup>

---

<sup>250</sup> Les cinq moteurs les plus utilisés dans le monde en 2005 étaient *Google, AOL, Yahoo, MSN* et *Ask Jeeves*.

<sup>251</sup> Il existe toutefois une très grande partie du web qui n'est en fait pas indexé par les moteurs de recherche traditionnels. Il s'agit de ce qu'on appelle le *Invisible Web*, qui est constitué du *Deep Web* (essentiellement du contenu dynamique ou programmé) et du *Black Web* (côté obscur d'Internet composé de sites interlopes qui cherchent justement

### 2.4.1.2 Besoins de l'analyste

Lorsqu'une personne a besoin d'analyser les informations qu'elle a retrouvées, les critères changent. Reprenons l'exemple d'une requête effectuée à l'aide d'un moteur de recherche sur Internet.

Le résultat est bien souvent des centaines, voire des milliers (ou même beaucoup plus) de documents contenant le critère recherché. Si l'on veut analyser tous les éléments qui apparaissent lors de cette recherche, le travail devient vite démesuré.

L'analyste a des besoins spécifiques qui peuvent se résumer par les points suivants :

- Précision
- Structuration
- Décomposition
- Individualisation

#### Précision

La précision de la recherche est primordiale, il ne peut pas y avoir de flous ou d'ambiguïtés. Les éléments doivent être, au début, extrêmement bien définis, de manière très précise, afin que l'on puisse se baser sur des entités connues et reconnaissables comme telles.

#### Structuration

Les faits doivent être structurés, de manière à ce qu'ils permettent de retrouver chaque type d'information à sa place et que les connexions possibles entre les différentes entités soient prédéfinies afin de rendre une recherche ciblée possible.

#### Décomposition

Chaque information doit être décomposée en un maximum d'entités individuelles. Grâce à la structuration et à la précision des données, ces décompositions doivent toujours permettre le processus inverse, soit leur recombinaison dans les phases d'analyse ou de synthèse des informations.

#### Individualisation

Chaque entité doit être individualisable, c'est à dire unique, afin de ne pas faire de fausses inférences et ainsi mettre en péril les fondements de toute analyse que sont les faits.

L'exemple type d'architecture qui répond assez exactement aux critères détaillés ci-dessus est la base de données objet-relationnelle. Grâce à un modèle relationnel, il est possible d'y chercher des éléments clairement identifiables dans ses tables et de la sorte d'en retirer ses connexions avec d'autres données contenues dans d'autres tables. Il est ainsi beaucoup plus aisé d'apprécier

---

à rester discrets aux yeux du grand public et qui dispose de ses propres moteurs de recherche spécifiques [p. ex. *Astalavista*], comme les moteurs traditionnels répugnent à les indexer).

l'élément recherché par rapport à son contexte. L'objet permet l'introduction de pointeurs invariants pour chaîner les objets entre eux. On peut ainsi parcourir rapidement des suites d'associations, par navigation dans la base. Il permet aussi de supporter des objets complexes au sein du modèle. Des recherches multicritères portant sur des éléments contenus dans différentes tables ne doivent en outre plus faire l'objet de développements d'outils spécifiques.

### 2.4.1.3 Compromis

Il appert donc que les besoins des *enquêteurs* et des *analystes* ne sont pas les mêmes. Les structures et organisations des données que nécessitent leurs travaux respectifs sont même franchement opposées.

Comme le fondement de toute analyse est l'information factuelle, il faut aller la chercher là où elle se trouve, et ne pas développer un système indépendant, même performant, qui souffre chroniquement du manque d'informations. Il s'agit donc de trouver le bon compromis afin de permettre à chaque intervenant, d'une part de réaliser des contrôles rapides, simples, exhaustifs et de manière centralisée et d'autre part, de permettre l'analyse de données précises, structurées, suffisamment décomposées et individuelles.

Avant l'été 2005, le système JANUS PV ne répondait qu'en partie à ce compromis. Il était clairement orienté vers les besoins de l'enquêteur. Il permettait par sa structure hiérarchique de rechercher rapidement et assez simplement de nombreuses informations centralisées. L'exhaustivité dépendait grandement des directives internes des différents partenaires utilisant le système quant aux données qu'ils faisaient figurer dans JANUS PV. Bien que ce système fût mis à la disposition des cantons, il n'y avait que très rarement des règlements internes qui obligeaient les intervenants à saisir leurs informations dans JANUS, sous une forme standardisée, comme c'était le cas depuis 2002 dans le canton de Vaud.

Les possibilités que laissait entrevoir JANUS PV pour l'analyse des données étaient intéressantes, et elles ont fait partie des préoccupations du groupe de référence qui devait préparer sa nouvelle version. Les comparaisons automatiques<sup>252</sup>, même incomplètement réalisées, ont permis de faire comprendre aux *enquêteurs* l'utilité des besoins des *analystes*.

Les possibilités de visualisation graphique pour l'analyse des données étaient malheureusement quasiment nulles dans l'ancien sous-système. Ce qui a débouché sur les problèmes que l'on découvrira plus loin.

La situation n'était par ailleurs globalement pas satisfaisante pour plusieurs raisons qui ont été détaillées au chapitre 2.3.2. Il s'agissait donc de faire évoluer le futur système JANUS PV 2.0 en

---

<sup>252</sup> Fonction déjà présente dans DOSIS et qui a perduré qui permet de comparer automatiquement les « sous-champs » entre-eux, au niveau d'un antécédent ou d'une identité.

une base de données reflétant le bon compromis entre les besoins des *enquêteurs* et ceux des *analystes*.

## 2.4.2 Concept

Le concept de ce projet de thèse est une organisation du flux de données qui se base sur un système d'aide à l'enquête en deux composants informatiques interconnectés. Ces composants ont les fonctions de mémoire à long terme pour le premier (système de gestion des données centralisés au niveau fédéral – JANUS PV 2.0<sup>253</sup>) et de base(s) de données d'analyse ou de travail (système prototype à créer) pour le second. Chaque investigation devant exploiter sa propre base de données d'analyse, celles-ci étant issues du même modèle conceptuel.

Les interconnexions doivent permettre d'assurer les *flux de données descendants* pour l'analyse et les *flux de données montants* pour réalimenter la mémoire à long terme.

Le schéma suivant résume ce processus général :

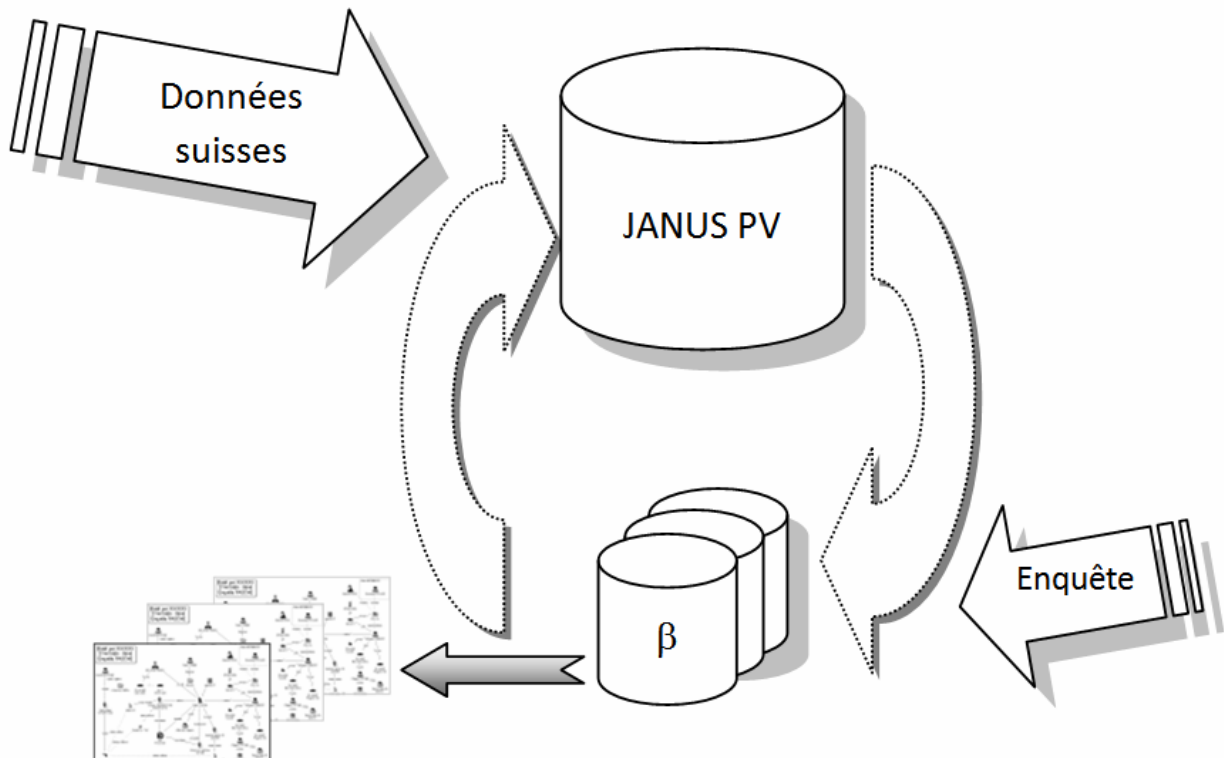


fig. 65 : Concept du projet de thèse

Le flux de données itératif préconisé consiste à intégrer continuellement un maximum de données au niveau de JANUS PV 2.0, et de proposer un outil d'exploration et de visualisation des données ponctuel mais performant, qui aide à analyser les informations connues de JANUS PV et de

<sup>253</sup> Le groupe de référence pour le renouvellement de JANUS PV en JANUS PV 2.0 a été constitué de 2002 à 2005.

disposer aussi d'un composant externe assez souple pour intégrer les données supplémentaires nécessaires à la résolution opérationnelle d'investigations.

### 2.4.3 Système basé sur deux composants

Nous allons décrire ici dans le détail les deux composants qui vont entrer en jeu dans le flux des données relatives aux investigations liées à la criminalité organisée. La base des données JANUS mise à disposition de tous les cantons par la police judiciaire fédérale constitue la mémoire à long terme ; un composant externe disposant d'une plus grande souplesse devant être développé, afin de pouvoir garantir une flexibilité et une qualité d'analyse suffisantes.

#### 2.4.3.1 Base de données d'enquête centralisée (JANUS PV 2.0)

Les bases de données de la Confédération constituent un impératif dans l'organisation du flux de données. Comme nous l'avons mentionné à l'axiome 1<sup>254</sup>, le facteur déterminant de toute analyse est l'accès à l'information par sa mise à disposition par les différents acteurs de la lutte contre la criminalité organisée en Suisse.

Grâce aux bases de données JANUS, les autorités de poursuite pénale et leurs agents disposent d'un outil de mémoire à long terme qui remplit parfaitement le cahier des charges d'une partie des étapes du cycle du renseignement. Ces bases de données permettent effectivement de collecter, d'intégrer, et d'évaluer les informations recueillies à l'échelle de la Suisse. De plus, l'intégration de la notion de lien, bien qu'imparfaitement implantée dans les versions antérieures des bases de données confédérées, permettaient déjà de générer automatiquement des relations entre les différents protagonistes en présence.

Par contre, l'orientation de cette base de données axée principalement sur les besoins de l'*enquêteur* et liée à des contraintes logicielles obsolètes, ne permettait pas d'obtenir une image facilement appréciable d'une situation plus ou moins complexe. Par ailleurs, les contraintes légales liées à la protection des données personnelles sensibles, ne permettent pas d'utiliser JANUS comme unique composant du système d'aide à l'enquête.

La nouvelle architecture du sous-système PV (JANUS PV 2.0) devra intégrer une réelle composante relationnelle, sans toutefois tomber dans l'excès inverse avec son lot de désavantages, comme une saisie trop stricte ou une navigation peu aisée<sup>255</sup>.

---

<sup>254</sup> Axiome 1: A l'heure actuelle une base de données commune et structurée est impérative en matière de lutte contre la criminalité organisée.

<sup>255</sup> Lors de la migration de JANUS JO à JANUS+ JO, une structure stricte de base de données relationnelle a été choisie et les conséquences ont été un système trop contraignant pour l'utilisateur final. JANUS JO 3.0 a rejoint en 2007 le nouveau système JANUS PV 2.0 mis en fonction en été 2005. Ensemble ils constituent à nouveau un système cohérent et compatible, comme ce fût le cas avant 2002, mais avec des outils plus modernes.

Certains nouveaux outils disponibles sur le marché s'inspirent grandement des méthodes d'analyse du renseignement<sup>256</sup>. Il sera primordial de soutenir les efforts consentis dans ce sens et de s'en inspirer pour les développements de la nouvelle version.

C'est pourquoi un composant d'analyse externe est nécessaire, afin de pouvoir ainsi faciliter le travail d'analyse, la diffusion et la réévaluation des informations et ainsi de terminer le cycle du renseignement.

#### **2.4.3.2 Bases de données d'analyse**

Il s'agit ici de créer un composant encore inexistant permettant d'améliorer l'intégration des diverses données d'enquête et de libérer du temps et de l'énergie pour le réel travail d'analyse, actuellement principalement entrepris par le personnel des cellules d'analyse criminelle opérationnelle au sein de la police judiciaire fédérale et des polices judiciaires des cantons suisses.

Le travail de ces spécialistes consiste en grande partie à la réalisation d'analyses opérationnelles sur mandat des enquêteurs, le gros du travail restant encore souvent le traitement des données (saisie, formatage, etc.). Dans les rares cas où la quasi-totalité des informations se trouve déjà dans les bases de données centralisées, comme pour le trafic illicite de stupéfiants (qui disposait déjà de quelques années de fonctionnement), les liens générés à l'aide des bases de données JANUS doivent être ressaisis dans des systèmes de visualisation pour pouvoir être ensuite analysés et le renseignement qui en découle finalement transmis.

Cette situation n'est que peu satisfaisante. On se rend bien compte du potentiel des systèmes, mais la manutention des données est encore trop lourde et limite par là l'utilisation de l'analyse criminelle et de ses futurs développements.

#### Outils

A nouveau, dans ce contexte, il ne s'agissait pas de partir de zéro, mais d'utiliser les outils préexistants et déjà bien implantés, qui permettent une exploitation plus rapide et une intégration assurée.

Les outils nécessaires au développement du prototype de base de données d'analyse sont donc constitués des logiciels d'analyse criminelle distribués largement dans les corps de police en Suisse et soutenus comme standards par l'Organisation Internationale de Police Criminelle (OIPC - Interpol). Il s'agit des logiciels commercialisés par le fabricant britannique *i2 Ltd*<sup>257</sup>.

La famille des logiciels *i2 Ltd* se divise en différents outils, au même titre que la suite *Office*<sup>TM</sup> de *Microsoft*<sup>TM</sup>, par exemple.

---

<sup>256</sup> Particulièrement le produit *RsCASE*<sup>TM</sup> de la société ROLA GmbH ([www.rola.com](http://www.rola.com))

<sup>257</sup> *i2 Limited*, The Visual Space, Capital Park, Fulbourn, Cambridge, CB1 5HX, GB, [www.i2group.com](http://www.i2group.com)

Les outils principaux de ce fabricant, présentés comme étant directement inspirés du cycle du renseignement (voir figure suivante), sont les suivants :

- *Analyst's Notebook™* : Logiciel phare. Utilisé par plus de 1200 organismes dans plus de 60 pays différents. Permet la visualisation des liens et la reconstitution chronologique.
- *iBase™* : Logiciel de base de données, développé pour être couplé à l'*Analyst's Notebook™* en ce qui concerne la visualisation des données contenues dans la base.
- *Chart Reader™* : Utilitaire permettant d'afficher et d'imprimer les schémas, sans avoir recours à l'*Analyst's Notebook™*, qui est protégé par une clé physique. Fonctionne de manière similaire à l'*Acrobat Reader™* d'*Adobe™*.
- *Analyst's Workstation™* : Logiciel regroupant de nombreuses fonctionnalités de représentation graphique de données numériques et de représentation cartographiques en lien avec les logiciels *MapInfo™* ou *ArcView™*.
- *TextChart™* : Logiciel permettant de récupérer semi-automatiquement des données textuelles pour les représenter graphiquement, sur le modèle de l'*Analyst's Notebook™*.
- *iBridge™* : Logiciel d'administration pour interconnecter les systèmes de gestion de bases de données préexistants avec l'*Analyst's Notebook™*.
- *Chart Explorer™* : Logiciel d'indexation de toutes les données contenues dans les visualisations produites à l'aide de l'*Analyst's Notebook™* et disponibles sur un espace disque commun, par exemple.

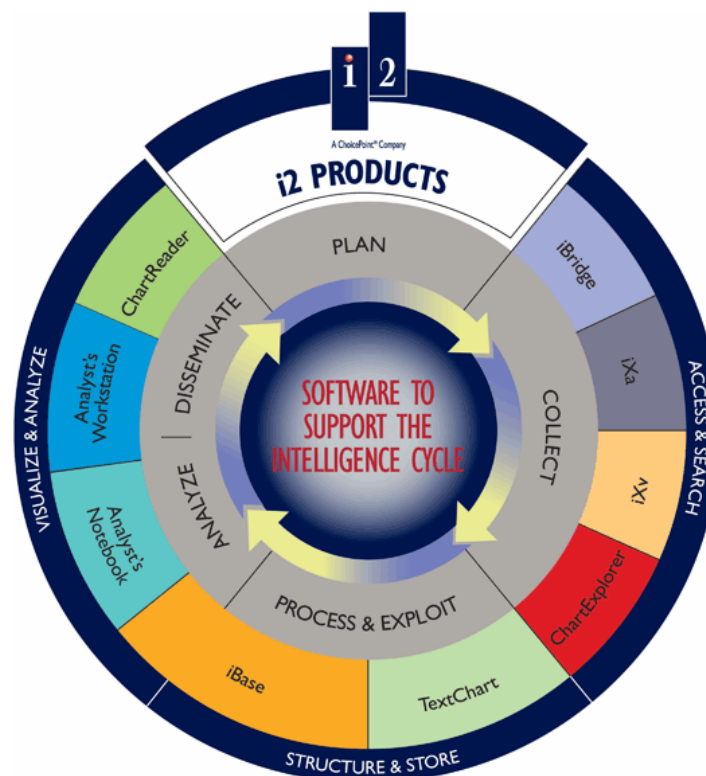


fig. 66 : Suite logicielle de i2 – mars 2008 - source [www.i2inc.com](http://www.i2inc.com)

## Elaboration

L'élaboration du prototype à l'aide des outils définis ci-dessus doit se faire en respect strict de la compatibilité descendante des données (exportation de JANUS PV 2.0) en provenance des bases de données centralisées et avec l'espoir d'atteindre une compatibilité montante (importation dans JANUS PV 2.0) des informations complémentaires qui seraient apparues durant l'analyse de la situation de départ et de l'évolution au long de l'enquête.

Il s'agira donc dans un premier temps de traduire la structure des données de JANUS PV 2.0 et d'y ajouter par la suite les éléments supplémentaires nécessaires à une analyse plus fine de la situation et au suivi de cette dernière tout au long de l'enquête préliminaire, ou après les interpellations et perquisitions qui s'y rapportent.

Les logiciels qui seront utilisés sont principalement l'*Analyst's Notebook*<sup>TM</sup> pour la visualisation des données et *iBase*<sup>TM</sup> pour leur gestion.

### **2.4.4 Composants interconnectés**

Les deux composants constituant le système d'aide à l'enquête doivent impérativement être interconnectés entre eux, afin de permettre la fluidité des données.

L'extraction de données du composant de mémoire à long terme (JANUS PV 2.0) en direction du composant d'analyse (prototype *iBase*<sup>TM</sup>) est une condition *sine qua non* à la réalisation du projet. La ressaisie manuelle des informations serait dans le cas contraire beaucoup trop lourde à assumer, n'aurait aucun sens aux yeux de l'utilisateur final et ne ferait finalement que peu évoluer la situation préexistante.

Les efforts entrepris auprès des personnes en charge du projet JANUS PV 2.0 à la police judiciaire fédérale et au sein du service informatique du Département fédéral de justice et police nous laissaient penser que les possibilités de connexion du composant d'analyse des données faisaient partie intégrante du cahier des charges du nouveau sous-système. Nous verrons par la suite ce qu'il en est advenu.

#### **2.4.4.1 Possibilités de flux de données descendant pour l'analyse**

Le sous-système le plus intéressant pour l'analyse des données est le sous-système PV, contenant les *personnes* et leurs *antécédents*, le sous-système JO étant normalement cloisonné selon les juridictions. En 2002, la Confédération pensait pouvoir mettre en exploitation un nouveau système JANUS + PV dès 2004. Le cahier des charges avait été préétabli et le groupe de travail regroupant les différents partenaires fédéraux et cantonaux avait été formé. L'auteur de cette recherche a pu rejoindre le groupe de travail susmentionné dès le départ, soit courant mai 2002.

Les possibilités de flux descendant pour l'analyse ne devaient pas poser juridiquement de problème, car l'ordonnance idoine<sup>258</sup> prévoyait déjà cette éventualité.

---

<sup>258</sup> RS 360.2 – Ordonnance sur le système informatisé de la Police judiciaire fédérale (JANUS)



Il s'agissait de prédéfinir les modalités et interfaces d'exportation des données de JANUS PV 2.0. On a pu penser à un moment que le choix du chef de projet se porterait sur le produit *RsCASE*<sup>TM</sup> de la société germano-suisse ROLA GmbH, les possibilités d'interconnexions avec les produits d'analyse étaient pré-intégrés et permettaient d'envisager les exportations avec confiance. Cependant, le système *RsCASE*<sup>TM</sup> ne permettait pas de gérer la complexité des droits d'accès pour un système confédéré de 27 entités différentes et d'un service de contrôle. Une base de données développée en interne devenait la seule issue possible et l'interconnexion redevenait un point central.

#### 2.4.4.2 Possibilités de flux de données montant pour alimenter la mémoire à long terme

Contrairement à l'exportation de données des systèmes JANUS, qui sont réglées dans l'ordonnance s'y référant, l'importation d'informations n'y est pas traitée.

Les possibilités techniques semblaient exister et n'étaient *a priori* pas hors de question.

Les modalités d'importation de données étaient déjà à l'ordre du jour en 2002, au vu des possibilités de développements conjoints des projets METAMORPHOSE<sup>259</sup> et JANUS PV 2.0, dans le but d'éviter la ressaisie des informations techniques des conversations surveillées (numéro appelant, numéro appelé, date, heure, type et durée de la connexion).

A nouveau, les modalités et interfaces d'importation des données du module d'analyse étaient à définir en fonction de l'avancée des travaux dans les deux composants du système.

#### 2.4.5 Synthèse

Ce projet repose sur une organisation du flux de données et propose une architecture fondée sur deux composants informatiques constituant un système d'aide aux investigations criminelles dans le cadre de la lutte contre la criminalité organisée.

Ceci essentiellement pour les raisons suivantes :

- 1<sup>er</sup> postulat : Il répond à un besoin de mettre les données relatives aux enquêtes criminelles en commun, ce type de criminalité dépassant presque assurément les frontières cantonales, régionales et même nationales, celles-ci régissant le cadre légal et son principe de territorialité. Ce système repose donc sur un composant pérenne et commun qui répond spécifiquement à ce besoin.
- 2<sup>ème</sup> postulat : L'enquête criminelle cherche à reconstruire une situation passée ou présente selon trois dimensions : *les entités et leurs relations* (personnes ou choses), *le temps* et *les lieux*. Dans le cadre des investigations sur la criminalité organisée, il est primordial de pouvoir apprécier le rôle joué par les protagonistes au sein du groupement criminel,

---

<sup>259</sup> Projet de digitalisation et centralisation des « écoutes téléphoniques » au service des tâches spéciales du DETEC

notamment en se basant sur les relations déterminées par des liens factuels. Ce système propose pour les deux composants du système un modèle conceptuel générique qui cherche à reproduire le réel.

- 3<sup>ème</sup> postulat : La complexité des données recueillies, notamment par leur nombre, leurs types, leur qualité, nécessite de disposer d'un moyen d'analyse dynamique. Ce système repose sur un second composant spécifique externe et ponctuel qui répond à ce besoin (base d'analyse).

De plus, ce modèle organisationnel du flux et de gestion de données constitué d'un système bi-composant permet de séparer les données d'enquête établies qui peuvent être partagées avec d'autres autorités d'instruction (dans le composant « base de données d'enquête centralisée » JANUS PV 2.0), de celles, qui ne le sont pas encore et qui reposent sur de simples soupçons ou proviennent par exemples d'informateurs, mais qui sont nécessaires à la résolution de l'affaire particulière et qui doivent être intégrées au second composant (« base de données d'analyse »).

Ce modèle permet ainsi d'être le plus efficace possible durant l'enquête, mais également comme le moteur du renseignement criminel dans le cadre de la lutte contre la criminalité organisée, JANUS étant une base de connaissance propice à la recherche et à la production de renseignements adéquats dans la première phase des investigations.

## 2.5 Hypothèse 1 – faisabilité du projet

**Il est possible de coupler aux bases de données centralisées un composant d'analyse externe évolutif qui intègre des systèmes de représentation graphique, dans le but d'analyser les relations complexes de la criminalité organisée.**

Cette première hypothèse porte sur la faisabilité de la réalisation pratique du système d'aide à l'enquête bi-composant tel qu'imaginé dans cette recherche.

Si une fonction de visualisation graphique des données avait déjà été développée pour un des sous-systèmes<sup>260</sup> JANUS afin d'aider l'investigateur dans l'analyse des données, elle ne portait que sur la partie traitant des contrôles téléphoniques (JANUS JO). Une plus grande souplesse est nécessaire pour une analyse plus fine, plus en profondeur et qui se prolonge dans le temps. C'est pourquoi un composant d'analyse de groupe d'auteurs à part entière doit remplir la fonction de base de données d'analyse. Ce composant doit être exploité par l'analyste lui-même ou par le groupe d'investigateurs en charge de l'affaire.

Ce composant doit, de plus, permettre d'inclure des éléments supplémentaires en cours d'enquête, qui ne pourraient pas légalement figurer dans la base de données centralisée, ou qui ne correspondent simplement pas à la structure de son modèle conceptuel.

Cet auxiliaire doit, encore et c'est primordial, pouvoir faire facilement évoluer l'image de la situation en fonction des nouvelles informations, que ce soit encore dans une phase préliminaire ou après les interventions.

### 2.5.1 Bases de données d'enquête centralisées

On a vu que le cadre législatif<sup>261</sup> avait évolué favorablement durant les années 1990 et qu'il s'agissait de s'attarder sur les contraintes économiques, organisationnelles, méthodologiques et enfin les outils à disposition des praticiens<sup>262</sup>.

Les systèmes d'aide à l'enquête de la Confédération (DOSIS, ISOK et JANUS) ont vécu une transition technologique permanente. Il s'agissait de profiter d'une de ces transitions nécessaires (contrainte économique partiellement levée) des systèmes déjà en place et éprouvés (contrainte organisationnelle presque entièrement levée) pour faire valoir les besoins des analystes (cadre méthodologique) à leur juste valeur et adapter enfin les outils.

<sup>260</sup> Voir chapitre 1.3.4.1 – Les bases de données centralisées JANUS

<sup>261</sup> Voir chapitre 1.3.4 – Les bases de données de police judiciaire

<sup>262</sup> Voir chapitre 1.4.3 – Cadre de l'analyse criminelle

L'architecture de l'ancien système DOSIS (actuellement JANUS) était toujours utilisée au début des années 2000, en ce qui concernait le sous-système PV lors de l'élaboration de ce projet. L'autre partie du système JANUS, le sous-système JO, était encore disponible sous son ancienne forme pour la consultation, mais une nouvelle version JANUS+ JO était opérationnelle depuis peu.

### 2.5.1.1 JANUS PV (Personnes et antécédents)

Ce sous-système, appelée JANUS PV (*Personen und Vorgänge*), est *a priori* ouvert, c'est-à-dire que les informations qui s'y trouvent sont par défaut partagées avec l'ensemble des utilisateurs autorisés, à moins que l'on y apporte les restrictions d'accès particulières, que se soit au niveau de la typologie des infractions ou de l'appartenance juridictionnelle des utilisateurs.

Jusqu'en 2005, il fonctionnait selon une architecture de type hiérarchique. À la base, on retrouvait la fiche de la personne physique ou morale, identifiée ou non, à laquelle correspondait un certain nombre d'antécédents judiciaires.

L'intérêt particulier de ce système résidait dans la définition de marqueurs dans le texte, des « sous-champs », qui permettaient de créer des relations entre les différentes fiches personnes.

Ces « sous-champs » étaient prédéfinis. Ils regroupaient les types de liens les plus communs que l'on pouvait retrouver dans une analyse de groupe d'auteurs.

La liste suivante décrit les codes de « sous-champs » qui étaient introduits comme marqueurs dans le corps de texte de l'antécédent lié à la fiche personne pour résumer l'événement judiciaire la concernant. Ces marqueurs n'apparaissaient toutefois pas à l'impression.

- ABO> Numéros de téléphones vérifiés, avec abonné ;
- ADR> Adresses,
- AUT> Numéros minéralogiques non-encore vérifiés ;
- CPT> Comptes – bancaire ou postal ;
- DET> Numéros minéralogiques vérifiés, avec détenteurs ;
- FTQ> Transaction financière - source ;
- FTZ> Transaction financière - but ;
- HOT> Hôtels (seulement lorsque la personne principale y séjourne) ;
- OBJ> Objet en relation avec une infraction ;
- ORG> Organisation criminelle ;
- PAS> Papiers d'identité ;
- REL> Personnes en relation avec l'identité principale ;
- RTG> Routings ;
- SOC> Sociétés ;
- TEL> Numéros de téléphones non-encore vérifiés ;
- URL> Site Internet, adresse e-mail ;
- VER> Mesures de contraintes ;

La syntaxe des informations dépendait du type de marqueur utilisé. Par exemple, pour une personne en relation, on mentionnait : REL>NOM/Prénom/Date\_de\_naissance/nationalité. Toutefois, il ne s'agissait là que de recommandations et elles étaient plus ou moins bien suivies.

Le schéma suivant résume les « sous-champs » définis dans le système JANUS PV et les relations entre deux fiches personnes qui en découlaient. Il s'agissait donc de relations directes ou indirectes prédéfinies.

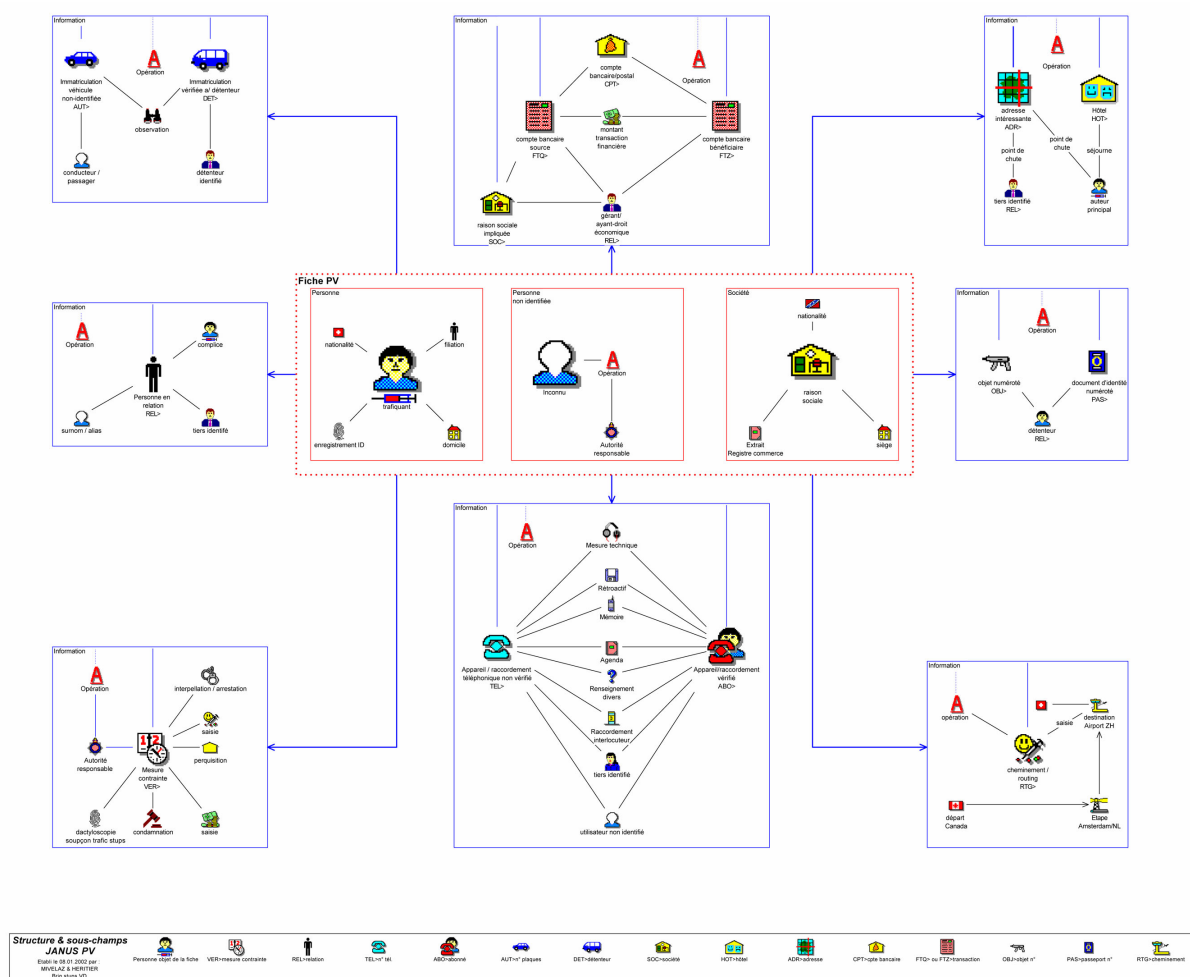


fig. 67 : Possibilités de liens définis par « sous-champs » dans le système JANUS PV<sup>263</sup>

On remarque à ce niveau que malgré la quantité de « sous-champs », un seul type de relation directe était défini (entre deux personnes, physique ou morale). Par ailleurs, les différents liens indirects<sup>264</sup>

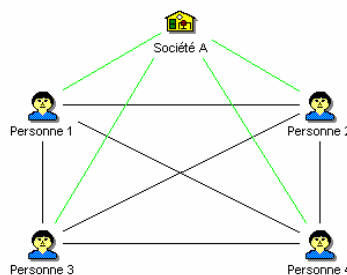
<sup>263</sup> Etabli par F. MIVELAZ et J.-D. HERITIER, police de Sûreté vaudoise, janvier 2002. Ce schéma se trouve également à l'Annexe I – Figures de grande taille.

<sup>264</sup> Le point 2.5.2.8 montre en détail que les « sous-champs » pouvaient contenir en fait plusieurs liens. La syntaxe de certains « sous-champs » empêchait que la décomposition des données objectives soit totale. Ces faits perdaient alors leur capacité à créer des liens.

n'étaient pas pris en compte, comme on le verra en détail plus loin. Cela n'était évidemment pas satisfaisant pour conduire une analyse fine d'une situation.

Un autre gros problème de JANUS PV était que la composante relationnelle des informations décrites n'était pas transposée au niveau informatique, qui se traduisait par une navigation entièrement hiérarchique dans le système et une recherche des liens par des *comparaisons*<sup>265</sup> gourmandes en ressources système. L'exploitation des entités et de leurs relations n'était donc possible qu'au prix d'un traitement nécessitant des ressources informatiques importantes et du temps. Un temps qui n'était pas toujours pris par les utilisateurs du système qui ne se préfiguraient donc pas forcément la plus-value de la saisie précise des informations à l'aide des marqueurs de « sous-champs ». Cette négligence a eu pour effet que certains mentionnaient par exemple dans toutes les fiches des personnes concernées par un même événement l'entier de l'information sans distinction de la personne concernée en titre. Ce qui créait une énorme redondance d'information et ruinait tout espoir de représentation relationnelle automatique des faits.

Bien que pour l'enquêteur ce ne soit pas singulièrement faux, puisqu'il lui était possible de retrouver les éléments écrits relatifs à chacun sur toutes les fiches, il fallait alors encore et toujours être en mesure d'apprécier mentalement la situation. Car si l'on représentait automatiquement et directement les informations à disposition, on risquait fort de se trouver dans la situation totalement fautive où tous les éléments étaient interconnectés entre eux !



*fig. 68 : Exemple de représentation fautive où tout est lié à tout*

Alors que la situation décrite dans le texte en tant que tel aurait pu être la suivante :

---

<sup>265</sup> Les comparaisons sont des recherches automatisées de liens entre les personnes présentes dans le système par l'intermédiaire des « sous-champs ». Elles n'ont finalement pu être implémentées que pour certains « sous-champs ».

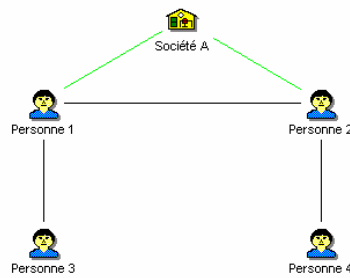


fig. 69 : Exemple de représentation correcte où les liens sont différenciés

### 2.5.1.2 JANUS JO

De manière générale, ce sous-système peut accueillir les données d'enquête de tous les cantons, sans restriction de lien avec la criminalité organisée, ou avec les autres types d'infractions de la compétence de la Confédération. C'est pourquoi il est *a priori* fermé. Les données introduites sont donc visibles et exploitables uniquement par les membres de l'autorité qui les ont saisies, à moins que celle-ci autorise la mise à disposition de ses données à d'autres partenaires. De fait, le *linkage blindness* dans ce sous-système, même centralisé, est très grand, et il ne sera pas forcément possible de le diminuer, le cadre légal étant strict sur ce point.

Le sous-système nommé JANUS JO (*Journal*), qui avait subi une mise à jour importante en 2002 (JANUS+ JO), bénéficiait déjà d'une structure informatique relationnelle stricte. Cela permettait de résoudre partiellement le problème évoqué juste précédemment, car la base de données elle-même forçait l'utilisateur à penser en entités propres (personnes, choses, lieux, etc.) et en relations (parent, abonné, détenteur, domicile, etc.). Par contre, elle avait comme désavantage d'être en contrepartie évidemment beaucoup plus contraignante lors de la saisie des informations. JANUS+ JO rendait la saisie des liens problématique pour l'opérateur qui ne disposait pas d'auxiliaire graphique. La précision avec laquelle les informations étaient introduites était évidemment primordiale pour la représentation automatique des données.

Afin de ne pas trop perturber les utilisateurs avec une interface purement relationnelle, une navigation thématique avait été conservée. Ainsi, les informations étaient subdivisées en différents actes d'enquêtes tels que les contrôles téléphoniques, les journaux d'enquête et d'observations judiciaires. On trouvait aussi un index des numéros de téléphone et des personnes s'y référant. Les droits d'accès étaient liés aux opérations de police qui régissent l'ensemble des actes enregistrés dans le sous-système JANUS JO.

La gestion thématique d'une structure relationnelle a posé bien des problèmes aux concepteurs, puis aux enquêteurs qui souffraient chaque fois qu'ils utilisaient ce sous-système<sup>266</sup>.

Des surprises sont apparues lors de l'établissement du schéma suivant. Par exemple, dans ce sous-système JANUS JO, qui était indépendant de JANUS PV, l'entité « véhicule » identifiée par le numéro d'immatriculation ne pouvait apparaître que dans le thème de saisie « Observation » et il n'était pas possible de le rattacher à une personne. Ceci était une erreur de conception manifeste, qui a été corrigée lors d'une mise à jour ultérieure. Un thème supplémentaire a également été ajouté à notre demande. Il s'agissait des « mains courantes d'enquête », journaux auxquels on pouvait lier également des personnes physiques ou morales.

Ce schéma représente la structure thématique de navigation (rectangles) et les entités définies, ainsi que les liens qui les mettent en relation.

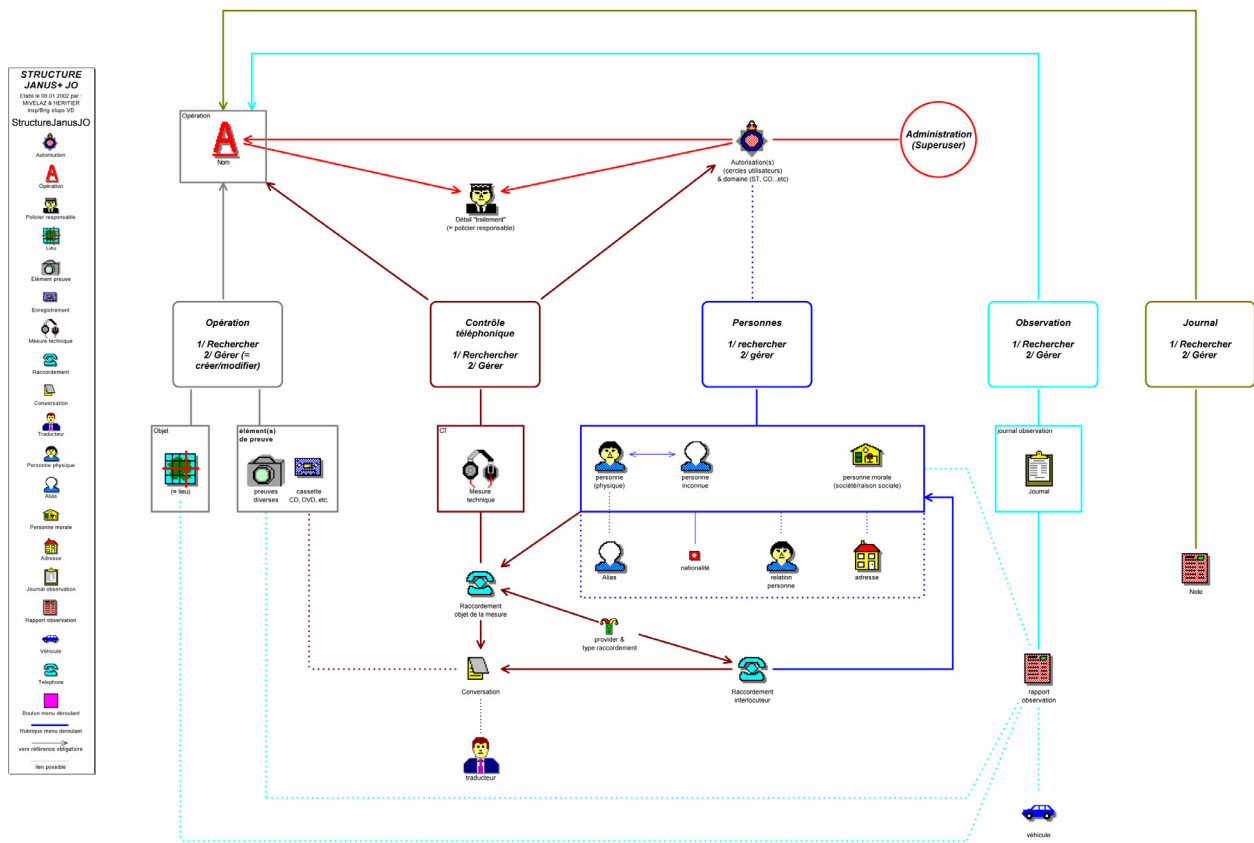


fig. 70 : Possibilités de liens définis par dans le système JANUS+ JO (version évaluation)<sup>267</sup>

<sup>266</sup> Une nouvelle version a été déployée en 2007. Elle gomme les difficultés de navigation précédentes et se greffe à la plateforme du nouveau JANUS PV. Cette réunion forme le système JANUS 3.

<sup>267</sup> Etabli par F. MIVELAZ et J.-D. HERITIER, police de Sûreté vaudoise, janvier 2002 Ce schéma se trouve également à l'Annexe I – Figures de grande taille.



### 2.5.1.3 Synthèse

Le sous-système JO ne correspond pas aux besoins qui sont énoncés dans le premier postulat, puisqu'il est *a priori* fermé. La réduction du *linkage blindness* ne serait donc pas effective en situation normale. Cependant, des moyens simples de visualisation de certaines informations contenues dans la base de données centralisée existaient déjà, comme les contrôles téléphoniques. Ces visualisations permettent aux investigateurs d'analyser plus facilement les métadonnées des surveillances téléphoniques et saisies dans JANUS JO.

Le sous-système PV, par contre, est lui *a priori* ouvert et il supprime ainsi grandement le *linkage blindness*.

JANUS PV n'avait jamais disposé d'une fonction de visualisation des liens, mais il le compensait par sa fonction de *comparaison*, qui permettait de rechercher si des informations contenues dans des « sous-champs » se retrouvaient ailleurs dans la base de données dans des « sous-champs » du même type. Il y avait donc une fonction d'aide à la recherche des liens, mais le résultat produit par le système était très peu digeste.

Le sous-système JANUS PV est donc bien la base de données d'enquête qui devrait permettre de rechercher, de gérer et d'analyser les liens entre les protagonistes du tissu criminel organisé actif dans notre pays.

Mais, était-il possible d'extraire et de représenter les informations telles qu'elles étaient structurées dans la base de données JANUS PV ?

## 2.5.2 Structure détaillée de JANUS PV

Le but ici est de relever, dans le détail, les principales caractéristiques de la base JANUS PV qui était utilisée avant juillet 2005 et qui posaient problème pour la réalisation du projet de cette recherche. Ces problèmes découlaient principalement de la structure hiérarchique du système de gestion de la base de données et de l'astuce qui consistait au stockage des liens sous la forme de texte libre marqué et plus ou moins formaté (« sous-champs »). JANUS PV avait un autre gros désavantage technique, qui était l'impossibilité d'importer ou d'exporter des données de la base centrale avec des composants d'analyse comme nous désirions le développer dans ce projet.

### 2.5.2.1 Modèle conceptuel : personnes et antécédents (Personen und Vorgänge – PV)

S'agissant d'un système pensé par et pour des enquêteurs, effet de la formalisation ou empilement d'expériences particulières, JANUS PV était centré sur l'élément principal de l'enquête, c'est-à-dire la personne. Il était structuré hiérarchiquement de fiches *personnes*, qu'il s'agisse de personnes physiques, morales ou encore d'inconnus, et de leurs *antécédents*, soit les informations les concernant, répertoriées par ordre chronologique inverse (les plus récentes en premier). Ces antécédents étaient, par exemple, des ouvertures d'enquêtes suite à des mises en cause, des identifications par empreintes digitales ou ADN, des mesures de contraintes (comme une mise sous

contrôle technique, une arrestation, une visite domiciliaire, une saisie ou un séquestre), des renseignements complémentaires en cours d'enquête, ou enfin des résumés des rapports destinés aux magistrats instructeurs. Plusieurs autorités pouvaient saisir des antécédents pour la même personne.

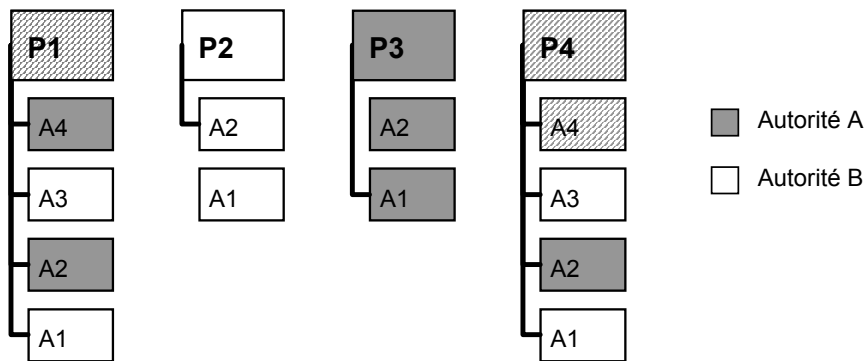


fig. 71 : Structure hiérarchique des personnes et des antécédents de JANUS PV<sup>268</sup>

C'est à l'intérieur des antécédents que l'on pouvait retrouver dans le texte libre explicatif les fameux « sous-champs », permettant de générer des liens entre les différents *antécédents*, et par voie de conséquence entre les différentes *personnes*.

Comme dans toute base de données, les informations qui y figurent sont structurées selon un modèle conceptuel défini au départ. Ce modèle initial a une importance capitale, puisqu'il déterminera ce qu'il sera possible de faire avec les jeux de données contenus lors de l'exploitation de la base de données.

Les principales rubriques vont maintenant être passées en revue et analysées en regard des notions nécessaires à la définition d'un modèle conceptuel de la base de données, soit :

- les entités et leurs attributs (faits, personnes ou objets),
- l'attribut identifiant (tout ou partie de l'élément qui permet de l'individualiser),
- leurs connexions possibles (ce qui peut être lié à quoi et comment).

Suit la structure des principaux éléments de JANUS PV (Personne « identité », liens « sous-champs » et « événements ») :

<sup>268</sup> Adaptée d'une présentation de N. DEWHIRST, père de DOSIS, OFP, 1999

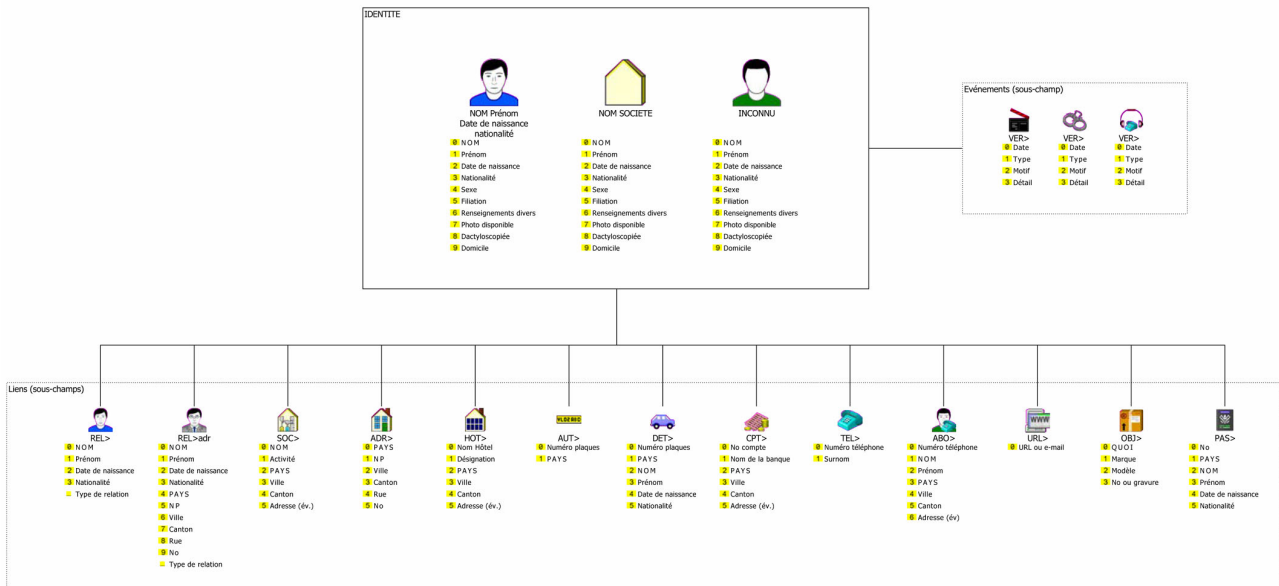


fig. 72 : JANUS PV : Détail des rubriques principales de l'identité et des « sous-champs »<sup>269</sup>

Finalement, nous schématiserons les représentations qui résultent de la structure qui avait été adoptée pour JANUS PV. Nous ne tiendrons pas compte des champs nécessaires au fonctionnement logique du système tels que la « date de saisie de l'information », le « code utilisateur de la personne réalisant le saisie », etc.

### 2.5.2.2 IDENTITE

La notion IDENTITE utilisée ici était la traduction du terme allemand *Stamm* (tronc). Ce terme imageait bien que c'est sur cette entité que le système était centré. L'IDENTITE représentait une *personne* qui faisait l'objet d'un enregistrement dans JANUS PV, et dont l'identité (au sens propre) était justement enregistrée dans le système. Une personne qui figurait dans le système comme IDENTITE devait posséder au moins un antécédent qui expliquait les raisons de son enregistrement. Il arrivait parfois que l'utilisateur ne puisse accéder à cet antécédent, car il concernait une juridiction ou un domaine de la criminalité pour lequel il ne disposait pas de droit d'accès. Tel que défini dans l'ordonnance JANUS, il pouvait alors voir qu'un antécédent avait été saisi, à quelle date, par qui et pour quel domaine de la criminalité, mais sans accéder aux détails.

Voici certaines informations qui devaient figurer sur l'identité d'une *personne* dans JANUS PV:

<sup>269</sup> Ce schéma se trouve également à l'Annexe I – Figures de grande taille.

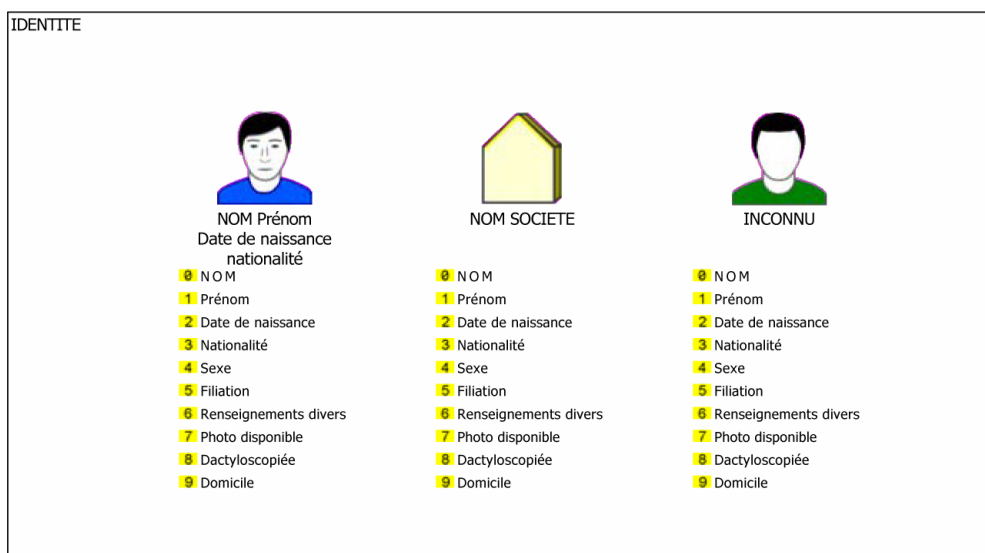


fig. 73 : JANUS PV : Détail des champs de l'IDENTITE

### Entité

Il s'agissait ici de l'élément principal du système : la *personne*. Cette entité pouvait être définie comme une personne physique, morale ou inconnue. Dans tous les cas, les champs étaient les mêmes et n'étaient pas toujours spécifiques à chaque type, par exemple le « sexe » pour une *personne morale*, ou la « date de naissance » pour un *inconnu*). Des organisations criminelles reconnues (*Sacra Corona Unita, Hell's Angels, etc.*) pouvaient également être mentionnées en tant que type particulier de personne morale (*organisation criminelle*).

Le choix d'utiliser la même entité pour des personnes physiques, morales, inconnues ou même des organisations criminelles a certainement été pragmatique.

### Identifiant

Les champs principaux que nous avons sélectionnés (hors données logistiques) étaient au nombre de dix<sup>270</sup>.

Dans ce cas, le champ « NOM » ne pouvait pas constituer pas à lui seul l'identité de la personne. Une identité complète (pour le policier) comprend également les informations « Prénom », « Date de naissance », « Nationalité », « Sexe », ainsi que la « Filiation ».

Mais, ces données ne sont pas toujours disponibles et sont malheureusement rarement saisies à chaque fois que l'on mentionne une *personne*, on doit donc raisonnablement restreindre la qualification de l'identité à trois critères : « NOM », « Prénom » et « Date de naissance ». De la sorte, on optimise les chances de trouver automatiquement des identités communes, en diminuant le risque de faire de faux liens sur le seul « NOM ». Il faudrait donc disposer d'un identifiant qui reprenne les rubriques 0, 1 et 2 au moins, et pas seulement le champ Ø.

<sup>270</sup> Nous utiliserons, par convention, dans cette description le champ Ø (zéro) comme étant l'identifiant de l'entité. En effet, le champ Ø était utilisé pour produire les comparaisons qui recherchaient automatiquement les « sous-champs » de même type ayant le même champ ø, générant par là-même des liens par les entités mentionnées en tant que « sous-champs ».

Dans le cas de l'entité *personne*, et comme il s'agissait de l'élément central, le système faisait appel à une référence informatique propre. Cette clé unique dans le système JANUS PV était le *numéro TED*, qui référençait les *personnes* (IDENTITES) et les *antécédents*. Il s'agissait comme souvent d'un code alphanumérique. Or, comme on va le voir plus bas, cette clé unique n'était pas reprise dans le « sous-champ » REL>.

### 2.5.2.3 REL>, REL>adr (relations interpersonnelles)

Voici les informations qui pouvaient figurer dans les « sous-champs » REL> et REL>adr que nous avons distingués sciemment, car l'un faisait mention en sus de l'adresse de la relation.

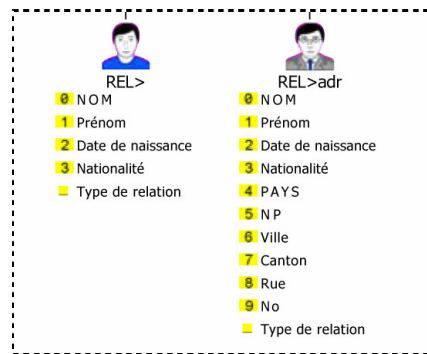


fig. 74 : JANUS PV : Détail REL> et REL>adr

#### Entité

Il s'agissait à nouveau de *personnes* (uniquement physiques cette fois-ci). On retrouvait pour ces deux « sous-champs » la même structure des rubriques 0 à 3, puis l'élément REL>adr, mentionnait en sus aux champs 4 à 9 l'adresse de la relation *personne*. Nous avons là une seconde entité (l'adresse) incluse dans la première (la personne). Il s'agissait d'un enchâssement d'entités de types différents, ce qui montre que la décomposition des informations connues était incomplète et par conséquent que certains liens ne pouvaient pas se faire automatiquement.

Pour atteindre cette décomposition complète, il aurait alors fallu que la relation (REL>) soit elle-même élevée au rang de *personne* à part-entière en IDENTITE à laquelle on puisse attribuer des « sous-champs ». Or, pour des raisons légales ou pragmatiques, il n'était pas toujours possible et nécessaire d'établir des IDENTITES pour toutes les *personnes* apparaissant dans une enquête. Bien que le regroupement de la personne et de son adresse soit utile, l'adresse de la relation perdait sa capacité à générer des liens. Il en allait de même avec le dernier champ qui qualifiait le type de relation, et qui n'avait qu'une fonction informative.

### Identifiant

Nous nous trouvions dans la même situation que pour l'IDENTITE de la *personne*. Mais en plus, les « sous-champs » de PV devaient posséder une syntaxe bien particulière et très contraignante. Par exemple :

Si nous désirions mentionner un complice, soit : Toto LEHERO, né le 1<sup>er</sup> janvier 1970, de nationalité française, le « sous-champ » était : REL>LEHERO/Toto/01.01.1970/F/complice ; .

Et, si nous désirions encore mentionner son adresse à l'avenue de la Gare 1, à 1006 Lausanne, le « sous-champ devenait le suivant : REL>LEHERO/Toto/01.01.1970/F/CH/1006/Lausanne/VD/avenue/de/la/Gare/1/complice ;

Les rubriques des « sous-champs » étaient séparées par des barres obliques « / », et pour que le « sous-champ » ne soit pas anormalement sectionné par le système, il ne devait pas contenir d'espaces ou de caractères spéciaux. Le sectionnement des informations était ainsi rendu difficile et la génération de liens pouvait s'en trouver faussée ! Par exemple, prenons le « NOM » (champ Ø) de l'exemple ci-dessus : LEHERO. L'opérateur de saisie avait la possibilité de fractionner la particule de différentes manières : REL>LE/HERO/Toto/... ou REL>HERO/LE/Toto/... .

De plus, il n'était pas toujours possible d'obtenir et de pouvoir mentionner toutes les informations prévues. Dans ce cas, on ne les faisait pas apparaître. Par exemple, si on ne connaissait pas la date de naissance ou la nationalité, cela donnait simplement : REL>LEHERO/Toto/CH/1006/Lausanne/VD/avenue/de/la/gare/1/complice ;

Or ici, il y a un problème car on ne mentionnait pas explicitement les informations manquantes, ce qui rendait impossible toute restructuration automatique des données<sup>271</sup> ! Il aurait fallu écrire : REL>LEHERO/Toto///CH/... .

### Connexion

Le type de lien était une relation *personne - personne physique* et aurait pu être codée ainsi (p. ex. avec une couleur particulière). Cependant, la qualité de la relation (confirmée ou non) n'était définie nulle part et l'information complémentaire qui décrivait la nature de celle-ci (en toute fin de « sous-champs ») n'était pas récupérable car elle était facultative et elle dépendait du nombre d'informations précédentes (prévue par la syntaxe, certaines étant présentes et d'autres pas).

---

<sup>271</sup> Pour preuve, lors de la migration de JANUS PV à JANUS PV 2.0 en 2005, la grande majorité des « sous-champs » ont dû être restructurés manuellement ou laissés en l'état.

### 2.5.2.4 SOC> (société)

Le « sous-champ » SOC> permettait de mentionner des liens avec des personnes morales.

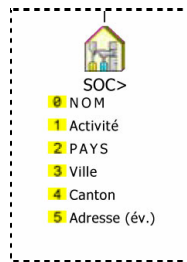


fig. 75 : JANUS PV : Détail SOC>

#### Entité

Cet élément nous renvoyait également à une entité qui pouvait figurer en IDENTITE. Mais ici, la différence entre l'élément de lien (« sous-champ ») et l'élément de l'IDENTITE est encore plus flagrante que pour les personnes physiques.

#### Identifiant

La première rubrique du « sous-champ » SOC> contenait le nom de la personne morale concernée. De nombreux problèmes apparaissaient plus particulièrement ici à cause des noms composés. De plus, de nombreuses personnes morales possèdent des noms aux parties initiales identiques. Par exemple, toutes les « Société de ... » ou les « Fondations pour ... », ou encore les références historiques ou géographiques.

De la sorte, une société qui s'appellerait « International Bank Trade » basée à Londres (SOC>International/Bank/Trade/banque/GB/Londres ;) n'était pas différenciable, sur la base du premier mot du nom composé, de la « International Association of Law Enforcement Intelligence Analysts » du New-Jersey, (SOC>International/Association/of/Law/Enforcement/Intelligence/Analysts/association/US/New/Jersey ;) , alors qu'elles n'ont rien à voir !

#### Connexion

Bien que le type de relation fût déterminé par le code du « sous-champ » SOC>, le détail de la relation manquait cruellement. Le degré d'implication et le rôle de la personne mentionnée dans l'IDENTITE n'étaient pas indiqués dans ce « sous-champ ».

### 2.5.2.5 ADR>, HOT> (adresse, hôtel)

Les relations d'adresse de la personne concernée dans l'IDENTITE étaient mentionnées de la sorte :

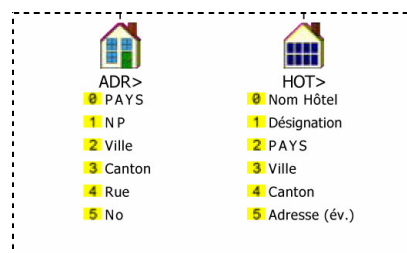


fig. 76 : JANUS PV : Détail ADR> et HOT>

## Entité

Il s'agissait ici de lieux, que ce soit des résidences privées, professionnelles, ou des lieux particuliers. Le concepteur de JANUS PV avait fait la différenciation entre une adresse (ADR>) et un hôtel (HOT>), pour des raisons qui nous sont encore obscures. La structure des rubriques de ces deux « sous-champs » était, de plus, complètement différente, ce qui rendait leur comparaison automatique impossible<sup>272</sup>.

## Identifiant

Le « sous-champ » ADR> comportait le code pays en position Ø. Ce qui voulait dire que l'identification du lieu ne pouvait se faire automatiquement que sur la base du pays ! Suivaient les indications dans un ordre respectant à peu près un travelling-avant géographique, soit : le numéro postal et la ville, le canton (comme complément de la ville), la rue et le numéro. Ce qui donne, par exemple : ADR>CH/1006/Lausanne/VD/avenue/de/la/Gare/1 ;

En ce qui concerne les hôtels, le « sous-champ » HOT> était identifié par le nom de l'hôtel, puis suivaient une désignation du type, et, comme pour l'adresse, le pays, la ville (sans le numéro postal !), le canton et l'adresse, éventuellement. A nouveau, on était confronté avec des noms composés, qui constituent la grande majorité des noms d'hôtels. L'exemple suivant illustre ce problème : HOT>LA/CROIX/FEDERALE/Pension/CH/Lausanne/VD/boulevard/de/Grancy/1 ;

Ici l'identifiant était le mot « LA », ce qui n'était, on en conviendra, pas très concluant !

Il faut toutefois admettre que la génération et la gestion des liens de *lieux* sont une des grandes difficultés dans l'environnement informatique. Cela requiert une très grande structuration des données et une qualité de saisie très élevée. Or, le système de « sous-champs » en exploitation ne revêtait aucune de ces deux qualités. Ce défi est si difficile à relever que dans bien des cas, les informations de *lieux* sont utilisées à des fins informatives uniquement et non pas dans le but de générer automatiquement des liens. Il n'y a alors pas d'identifiant défini. Le géocodage de ces données peut sans aucun doute constituer une des voies à suivre pour leur inférence<sup>273</sup>.

## Connexions

Les connexions sont ici identifiables par les codes de « sous-champs » ADR> et HOT> comme des relations entre *personnes* et *lieux* et pouvaient être codées en conséquence.

---

<sup>272</sup> C'est un indice supplémentaire que la comparaison automatique des « sous-champs » n'a été implémentée qu'une fois que la base de données était déjà en fonction.

<sup>273</sup> Avec l'arrivée des SIG (Système d'Information Géographique), les lieux sont désormais codés par les systèmes de coordonnées (latitude-longitude ou coordonnées suisses), ce qui les rend uniques et visualisables. Se pose alors encore la question de la base de référence des données géocodées qui doit être standardisée.



### 2.5.2.6 AUT>, DET> (automobile, détenteur)

Ces deux « sous-champs » étaient prévus pour signaler des véhicules en relation avec l'IDENTITE.

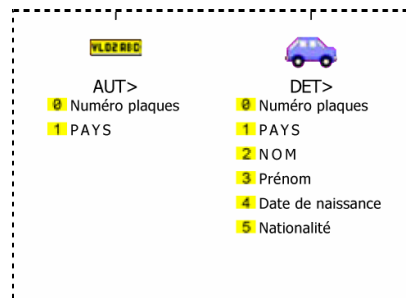


fig. 77 : JANUS PV : Détail AUT> et DET>

#### Entité

Il s'agissait de *moyens de transport*, tels qu'un véhicule privé dont l'IDENTITE est propriétaire ou qu'elle utilise. Le véhicule devait toutefois disposer d'un numéro d'immatriculation.

#### Identifiant

En position Ø, on trouve justement ce numéro d'immatriculation. En Suisse, les propriétaires de véhicules immatriculés gardent souvent leur numéro d'immatriculation lorsqu'ils changent de véhicule. Cette coutume nous aide, car il y a une plus grande stabilité dans le lien qui unit un propriétaire de véhicule à son numéro d'immatriculation. Dans la plupart des pays qui nous entourent, l'immatriculation suit le véhicule tout au long de sa « vie », malgré les changements de propriétaires. Ceci rend ce type de relation moins stable et du coup moins intéressant dans certaines enquêtes. Ici, l'identifiant ne pose pas de problème majeur, pour autant qu'un standard soit adopté pour la mention de l'indication cantonale. Par exemple, AUT>VD123456/CH ; et non pas AUT>123456/VD/CH ;. Il en était de même avec les plaques minéralogiques étrangères : AUT>1234XYZ75/F ; et pas AUT>1234/XYZ/75/F ; .

Comme pour le cas de la relation *personne – personne avec adresse*, si on avait la mention du détenteur, il ne pouvait pas être reconnu comme une *personne physique ou morale* à part entière et ne pouvait pas servir à la génération de liens. Il s'agissait d'une donnée uniquement informative. Le « sous-champ » avait la syntaxe suivante : DET>VD123456/CH/LEHERO/Toto/01.01.1970/CH ;.

#### Connexion

Le type de connexion : *personne - moyen de transport* était identifiable par le code AUT> ou DET>. Cependant, la propriété ou l'utilisation n'étaient pas mentionnées expressément.

### 2.5.2.7 CPT> (comptes)

Le « sous-champ » suivant permettait de mentionner des comptes bancaires.



fig. 78 : JANUS PV : Détail CPT>

### Entité

Il s'agissait de *biens (argent)*, et plus particulièrement les comptes bancaires. On pouvait imaginer également détourner quelque peu le sens strict de ce « sous-champ », en mentionnant aussi des chèques ou papiers valeur numérotés.

### Identifiant

L'identifiant en position Ø était le numéro de compte ou du papier valeur. A nouveau, une grande rigueur était nécessaire, d'autant plus que les numérotations financières sont souvent alphanumériques et peuvent comporter des indications complémentaires comme par exemple le numéro de clearing d'une banque (code de la banque pour les transferts bancaires) ou à l'inverse des codes de subdivisions d'un même compte.

Prenons l'exemple suivant : Monsieur LE HERO est titulaire d'un compte (123-456789.XYZ) à la BCV à Lausanne. La syntaxe du « sous-champ » devait être la suivante (123 étant le clearing de la banque) : CPT>456789XYZ/BCV/CH/Lausanne/VD/Place/St/François ; et non pas : CPT>123/456789/XYZ/BCV/...<sup>274</sup>.

### Connexion

Le code CPT> indique une relation *personne - bien (Argent)*. Il manquait toujours la mention plus précise de la qualité des liens, qui sont multiples dans le monde de la finance (titulaire, bénéficiaire, procuration, ...).

#### **2.5.2.8 TEL>, ABO> (téléphone, abonnement)**

Les « sous-champs » TEL> et ABO> ont une syntaxe similaire aux données concernant les véhicules (AUT> et DET>).

---

<sup>274</sup> Aujourd'hui, il est possible de travailler avec le code IBAN. Cette nouvelle structure se base sur les principes de la norme internationale EBS 204 IBAN (International Bank Account Number), ce qui garantit une identification unique à tout compte bancaire. En Suisse, il totalise 21 positions. Ces dernières déterminent sans équivoque les trois principales caractéristiques nécessaires à l'identification d'un compte bancaire : pays, établissement financier et numéro de compte. Un chiffre de contrôle est également inclus afin de garantir une détection optimale des erreurs de saisie. Exemple :



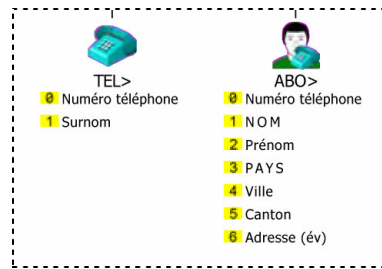


fig. 79 : JANUS PV : Détail TEL> et ABO>

## Entité

Ces « sous-champs » TEL> et ABO> permettaient de faire des liens grâce aux *moyens de communication*, principalement de la téléphonie.

Le « sous-champ » TEL> faisait référence à un numéro de téléphone (fixe ou mobile) qui n'était pas un abonnement et dont l'utilisateur ne pouvait être trouvé dans un annuaire. Cette catégorie de numéro téléphone était très courante, car les criminels utilisent préférentiellement des téléphones mobiles avec des cartes prépayées complètement anonymes ou acquises sous de fausses identités.

## Identifiant

En position Ø, on trouvait le numéro de téléphone, et il était possible pour le « sous-champ » TEL> d'ajouter ensuite le nom ou le surnom de l'utilisateur, entendu lors d'une écoute téléphonique ou relevé dans un répertoire papier ou électronique, comme c'était le cas dans la mémoire des téléphones mobiles. Cela donnait par exemple : TEL>0791234567/Toto ; . Il était très important que le numéro de téléphone soit saisi sans caractères spéciaux et sans espaces. Il était aussi admis de mentionner le numéro de série d'un appareil de téléphonie mobile, car des échanges de cartes SIM et de téléphones mobiles étaient fréquents dans certains réseaux criminels. Il était demandé de mentionner après le code la mention IMEI, soit : TEL>123456789012345/IMEI/Toto ; .

Le « sous-champ » ABO> permettait, tout en conservant le numéro de téléphone comme identifiant, de mentionner les nom et prénom de l'abonné du raccordement en question et encore éventuellement son adresse. Il s'agissait pour le nom d'un lien indirect (niveau 2) et si on rajoutait encore l'adresse, celle-ci devenait un lien second indirect (niveau 3) ! A nouveau, ces deux informations ne permettaient pas de générer des liens et n'étaient présentes qu'à des fins informatives. Voici un exemple complet, avec nom, prénom et adresse du « sous-champ » ABO> :

ABO>[0211234567](tel:0211234567)/[LEHERO/Toto](#)/[CH/1006/Lausanne/VD/avenue/de/la/gare/1](#) ;



### Connexion

Le type de connexion était facilement définissable par les codes de « sous-champs ». Cependant, comme on le verra plus loin il n'était pas possible de mentionner dans quel cadre un raccordement apparaissait dans des antécédents d'une IDENTITE. Il pouvait s'agir des propres raccordements de l'IDENTITE ou de numéros de téléphone d'autres personnes avec lesquelles elle était en contact. Soit dans le premier cas de figure, on était en présence d'un lien direct avec l'IDENTITE et dans le second, d'un lien indirect de niveau 1. Cela ne ressortait pas dans le contenu des « sous-champs » et posait des problèmes d'interprétation. Il était alors nécessaire de dépouiller les *comparaisons* avec soin dans le but de retrouver des liens directs, bien plus intéressants que les liens indirects qui pouvaient être nombreux et légitimes, comme par exemple par la présence de sociétés de services (gérances, taxis, etc.), de communications (prestataires de services de téléphonie mobile, fixe ou surtaxée) ou encore simplement d'administrations.

#### **2.5.2.9 URL> (adresse Internet)**

L'URL> est un « sous-champ » qui n'était pas très développé.

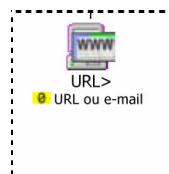


fig. 80 : JANUS PV : Détail URL>

### Entité

Ce « sous-champ » permettait de mentionner un nouveau *moyen de communication*, soit Internet et le courrier électronique (e-mail). Les adresses des sites Internet (www.xyz.com) ou les adresses e-mail (toto.lehero@mail.net) y étaient mentionnées.

### Identifiant

Comme il n'y a qu'une seule rubrique en position Ø, elle faisait forcément office d'identifiant. On avait donc la situation suivante : URL> www.xyz.com; ou URL>toto.lehero@mail.net ; .

## Connexion

Le type de relation était défini par le code de « sous-champ », mais à nouveau, à part le nom de l'adresse, aucune information n'était disponible pour qualifier le lien.

### 2.5.2.10 OBJ> (objet)

Voici le détail du « sous-champ » objet :



fig. 81 : JANUS PV : Détail OBJ>

## Entité

Ce « sous-champ » entre dans la catégorie des *biens (choses)*. Il pouvait être utilisé pour mentionner l'utilisation ou la propriété sur des biens divers. A l'origine, ce « sous-champ » avait été prévu principalement pour des armes à feu.

## Identifiant

Malheureusement, on trouvait en position Ø la réponse à la question « Quoi », qui servait à décrire le type d'objet auquel on avait à faire. Alors qu'en position 3 on demandait le numéro de série ou la gravure (en référence aux armes à feu) qui sont des identifiants. Par exemple, si on voulait mentionner une carte de crédit, on trouvait le « sous-champ » suivant : OBJ>carte/de/crédit/VISA/UBS/540412345678901 ; . Or dans ce cas, la mise en relation se faisait sur le mot « carte » ! Il aurait suffi de mettre le numéro de série en position Ø et le problème aurait été résolu : OBJ>540412345678901/carte/de/crédit/VISA/UBS ; .

## Connexion

Nous nous trouvons toujours ici en présence d'un code de relation identifiable par le code de « sous-champ », mais également toujours sans aucun détail sur le type et la qualité de la relation.

### 2.5.2.11 PAS> (passeport)

Enfin, les concepteurs de JANUS PV avaient créé un « sous-champ » spécial pour les documents d'identité, dont voici le détail :



fig. 82 : JANUS PV : Détail PAS>

## Entité

Il s'agissait ici de pouvoir créer des liens sur la base des papiers d'identité. Cette catégorie spéciale avait sans doute été implémentée dans le but de pouvoir inférer grâce à des documents contrefaits dont en général on ne modifie pas le numéro de série, mais auquel on substitue simplement la photo. Or, dans la pratique, il semble que les documents d'identité n'étaient introduits dans la base JANUS que lorsqu'ils étaient séquestrés et déclarés falsifiés. Dès lors, le lien avec un document original n'était pas généré dans cette base et ce « sous-champ » perdait son utilité. De plus, si le nom du titulaire avait été modifié, un contrôle par le numéro de série auprès des autorités étrangères compétentes permettait de retrouver le titulaire original<sup>275</sup>.

## Identifiant

Cette fois-ci, le numéro du document d'identité se trouve en position Ø. Il devait permettre de faire des relations avec d'autres documents d'identité, s'il apparaissait dans plusieurs affaires. Voici un exemple de la mention du passeport de Monsieur LE HERO :

PAS>1234567/EU/COVER/Harry/01.10.1969/GB ; . Une limitation subsiste toutefois encore, puisque le code du pays n'est mentionné que dans la rubrique 1, ce qui fait que tous les passeports ayant le même numéro, mais provenant de différents pays provoqueraient des faux positifs.

## Connexion

Il n'était toujours pas prévu de mentionner par exemple le détail du lien entre l'IDENTITE et le document, ni s'il s'agissait d'un faux ou d'un document authentique. La problématique des documents d'identité n'était donc pas vraiment facilitée par ce « sous-champ ».

### **2.5.2.12 VER> (arrestation)**

Finalement, nous en arrivons au dernier type de « sous-champ » que nous avons sélectionné pour cette description détaillée.

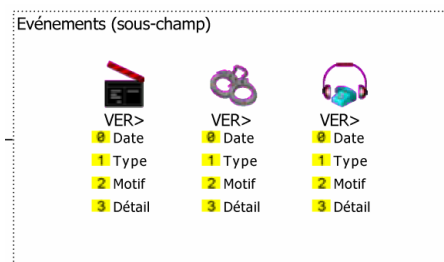


fig. 83 : JANUS PV : Détail VER>

<sup>275</sup> Des bases de données spécifiques existent, qui plus est au niveau fédéral.

### Entité

Ce « sous-champ » était prévu pour recenser les *événements* et plus particulièrement les mesures de contraintes à l'encontre de la *personne* mentionnée dans l'IDENTITE. Normalement, on ne devait pas retrouver plus d'une mesure de contrainte par antécédent, chacune d'elle devant justement entraîner la saisie de l'information correspondante dans le système JANUS PV. On pouvait citer comme mesures de contrainte : une arrestation, une visite domiciliaire, une saisie, un séquestre, ou encore un contrôle technique (mesure de surveillance des télécommunications).

### Identifiant

La date de la mesure de contrainte était mentionnée dans la position Ø. Donc, toutes les mesures de contraintes qui avaient eu lieu à la même date auraient été liées lors d'une comparaison, ce qui était évidemment peu satisfaisant. Dans ce cas précis, il n'était pas nécessaire de définir un identifiant et d'utiliser ce « sous-champ » comme moyen d'inférence. Comme il s'agissait en quelque sorte d'inventorier les mesures qui avaient été prises par l'autorité judiciaire et qui ne dépendaient pas de la personne suspecte, ce « sous-champ » pouvait revêtir un caractère uniquement informatif.

Néanmoins, la syntaxe de ce « sous-champ » un peu particulier était la suivante, pour M. LE HERO qui aurait été l'objet d'une mise sous écoute le 1<sup>er</sup> février 2003 puis arrêté le 15 mars 2003 :

VER>01.02.2003/mise/sous/écoute/soupçons/trafic/stupéfiants sur le TEL>0791234567 ; puis pour son interpellation : VER>15.03.2003/arrestation/trafic/stupéfiants/lors/livraison/50gr/cocaïne ;

### Connexion

Ici, comme il s'agit d'inventorier des mesures de contraintes, le codage du lien par un unique code de « sous-champ » VER> était insuffisant, puisqu'il ne permettait pas de différencier leur type.

## **2.5.3 Organisation détaillée de JANUS PV**

Nous venons de voir en détail la structure de JANUS PV telle qu'elle existait jusqu'en été 2005. Ce fichier de *personnes* dont les informations étaient structurées hiérarchiquement en événements (les *antécédents*), permettait néanmoins de générer des liens par la comparaison dirigée de chaînes de caractères spécifiques, reconnaissables par des marqueurs appelés « sous-champs », inclus au corps du texte de l'antécédent.

Les problèmes liés aux informations qui devaient servir d'identifiant aux entités potentiellement liées mentionnées en « sous-champs » ont débouché sur une mise en service très partielle du mécanisme de comparaison automatique. En effet, seuls quelques « sous-champs » (TEL>, ABO>, SOC> et REL>) étaient réellement comparés. Les autres « sous-champs » n'étaient finalement utilisés que pour faciliter des recherches ciblées.

Les solutions proposées par le système original DOSIS ont été développées en fonction de situations réelles rencontrées, d'intérêts imaginés (URL>), mais elles ne se fondaient pas sur un

modèle formel correspondant plus à des problématiques ponctuelles qu'à une véritable stratégie globale d'aide à l'enquête.

Néanmoins, le potentiel des *comparaisons* (recherches automatiques) a été rapidement identifié par les policiers et mis à profit principalement avec les « sous-champs » TEL> et ABO>, qui possédaient un identifiant valide<sup>276</sup> et qui devaient en fait constituer jusqu'en 2005 la très grande majorité des « sous-champs » de JANUS PV.

### 2.5.3.1 Situation illustrative

Voyons maintenant, par un exemple fictif, comment ces informations étaient organisées, si on prenait le temps de faire une représentation graphique des IDENTITES et des « sous-champs » qui leur étaient liés dans les antécédents en se basant sur les identifiants et quelles en étaient les conséquences.

Dans l'exemple présenté à la figure 84, les données comportent trois IDENTITES, une *personne inconnue*, une *personne physique*, une *personne morale*. Chacune des *personnes* a subi une mesure de contrainte et l'enquêteur leur a correctement créé à chacune une IDENTITE dans JANUS PV.

Pour chaque IDENTITE, on retrouve un certain nombre d'informations (faits objectifs) permettant de faire des liens. Celles-ci sont structurées comme prévu sous la forme de « sous-champs », organisés normalement comme des liens directs de chaque IDENTITE.

Jusqu'ici, il n'y avait pas d'erreur manifeste de mise en relation de tout avec tout<sup>277</sup>. Certains problèmes subsistaient toutefois.

---

<sup>276</sup> Comme les numéros de téléphone n'étaient pas saisis selon un standard prédéfini, soit avec ou sans l'indicatif international, utilisation du 00 à la place du code +, une correction logicielle a fait que seuls les 7 derniers chiffres étaient pris en compte lors des comparaisons : +41211234567 = 0041761234567 = 781234567. Ceci a créé de fausses relations. Ce critère a été par la suite encore corrigé et augmenté aux 9 derniers chiffres, ce qui permettait d'ignorer le formatage international et fonctionnait correctement pour les numéros suisses.

<sup>277</sup> Voir chap. 2.3.1.1



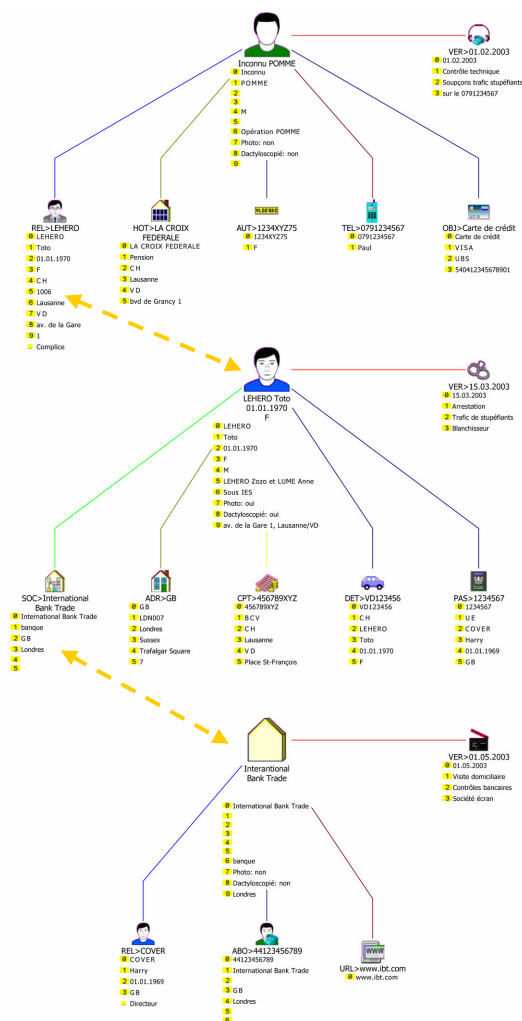


fig. 84 : JANUS PV : Exemple de l'organisation des données IDENTITE – « sous-champs »<sup>278</sup>

### Problème structurel IDENTITE – « sous-champs »

Les flèches en orange sur la figure ci-dessus montrent que ces trois *personnes* ne génèrent pas de liens alors que les « sous-champs » mentionnaient des relations avec certaines IDENTITES. C'est le problème structurel qui différencie une IDENTITE d'un « sous-champ ». La représentation correcte aurait dû être telle que représentée à la figure 85.

Les trois *personnes* apparaissent désormais désormais comme liées. Mais, cette correction devait être apportée *a posteriori*, ce qui aurait nécessité une étape supplémentaire (automatisée ou manuelle) de recherche des IDENTITES et « sous-champs » concordants.

<sup>278</sup> Cette figure est reproduite à l'Annexe I – Figures de grande taille

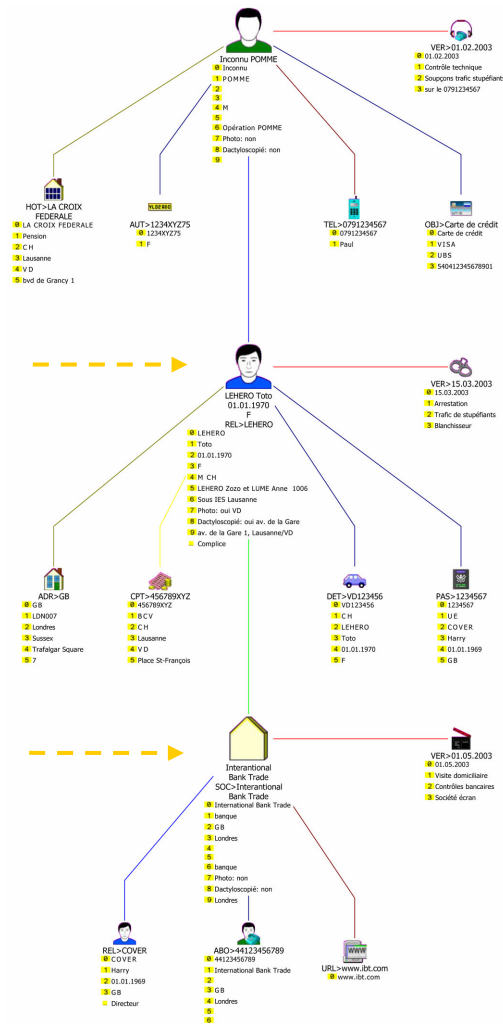


fig. 85 : JANUS PV : Correction de l'organisation des données IDENTITE – « sous-champs »<sup>279</sup>

### Problèmes dus à la structure des « sous-champs »

Une difficulté supplémentaire apparaissait lorsque l'on mentionnait dans un antécédent tous les raccordements qui avaient été en contact avec la *personne* en IDENTITE, par exemple lors d'une mesure de surveillance technique<sup>280</sup>.

Si l'on complète pour l'exemple le schéma précédent avec des données issues d'une mesure technique sur le raccordement de la *personne inconnue*, on obtient un résultat tel qu'illustré à la figure 86.

<sup>279</sup> Cette figure est reproduite à l'Annexe I – Figures de grande taille

<sup>280</sup> Habituellement, ces contrôles créent des listes allant d'une dizaine à plusieurs centaines, voire exceptionnellement plusieurs milliers d'interlocuteurs différents.

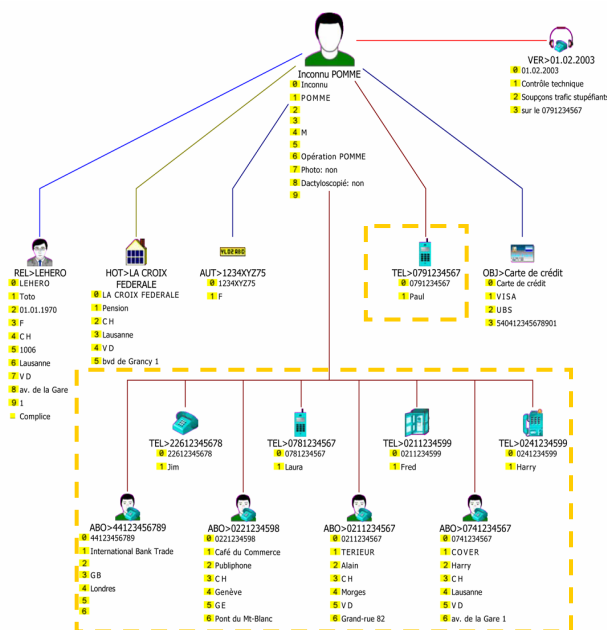


fig. 86 : JANUS PV : Mention des contrôles techniques dans des « sous-champs »<sup>281</sup>

Mais, rien ne différenciait le propre raccordement de l'Inconnu des autres numéros qui, en fait, avaient été en contact avec celui-ci. Il s'agissait d'une représentation fautive, car la structure de la base de données JANUS PV ne pouvait gérer que des liens indirects de premier niveau. Or, il aurait fallu, dans une représentation plus conforme à la réalité, connecter les raccordements apparaissant dans la mesure technique au raccordement de la *personne inconnue*, soit dans l'exemple le TEL>0791234567 et non pas à l'IDENTITE elle-même.

Cette correction n'était pas possible directement dans la base JANUS PV car un « sous-champ » ne pouvait pas contenir d'autres « sous-champs ». Il aurait donc fallu corriger cette erreur d'organisation manuellement dans les visualisations produites.

Néanmoins, si des numéros de téléphones étaient communs à d'autres antécédents, le système reconnaissait ces raccordements comme identiques et signifiait un lien lors des *comparaisons*.

<sup>281</sup> Cette figure est reproduite à l'Annexe I – Figures de grande taille

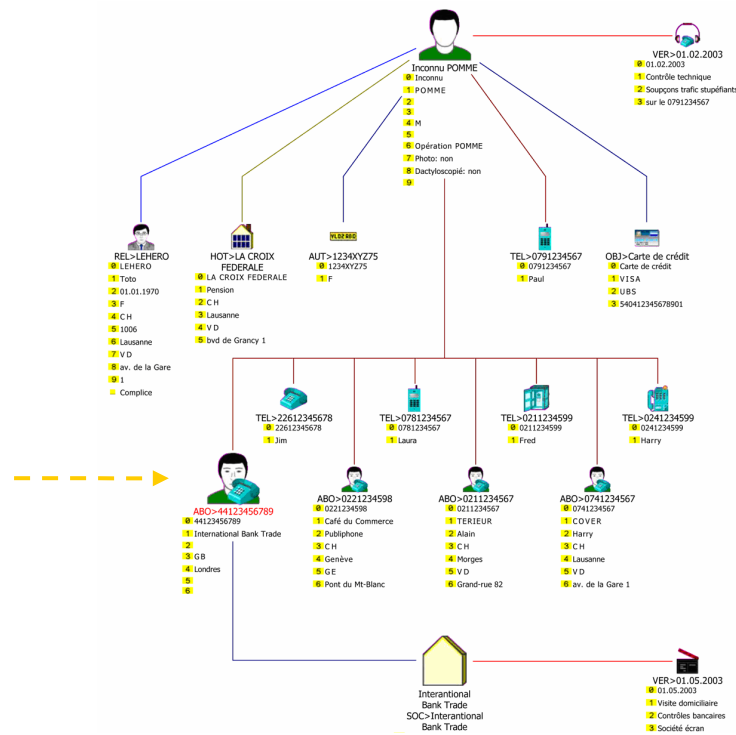


fig. 87 : JANUS PV : Connexion automatique des « sous-champs »<sup>282</sup>

Un second problème structurel des « sous-champs » venait du fait que des informations enchâssées figuraient à l’intérieur de ceux-ci, mais ne permettaient pas de faire des liens car il s’agissait de liens indirects de niveau 2 ou 3. Par exemple, l’identité mentionnée sur le passeport retrouvé sur Toto LEHERO, ou encore le raccordement de l’abonné Harry COVER sont des liens indirects de niveau 2.

Alors que précédemment la représentation était fautive avec les liens indirects de niveau 1, le potentiel de génération de lien était préservé. Ici, la représentation était correcte, bien que la décomposition des entités n’ait pas été complète, donc le potentiel de génération des liens était perdu.

La figure 88 montre ces trois « sous-champs » faisant référence à cette personne « Harry COVER » qui permettraient de générer deux liens supplémentaires. La lecture d’un schéma aussi simple permettait de trouver visuellement des liens potentiels non réalisés, mais lors de la recherche automatique de liens dans l’ensemble de la base de données, c’était impossible ! Il fallait faire des recherches en texte libre et reconstituer ensuite manuellement les liens découverts.

<sup>282</sup> Cette figure est reproduite à l’Annexe I – Figures de grande taille

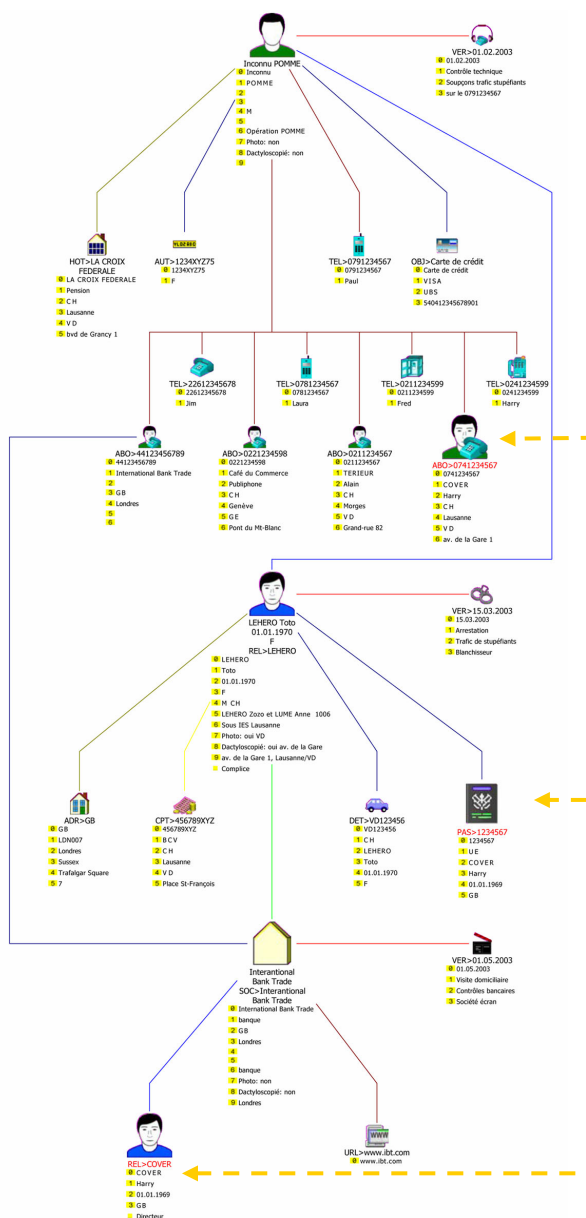


fig. 88 : JANUS PV : Perte du potentiel de liaison des « sous-champs » avec des liens indirects de niv. 2<sup>283</sup>

Représentation correcte

La représentation réelle de la situation, après la correction manuelle des liens indirects de niveau supérieur à 1 (2 ou 3) est la suivante :

<sup>283</sup> Cette figure est reproduite à l'Annexe I – Figures de grande taille

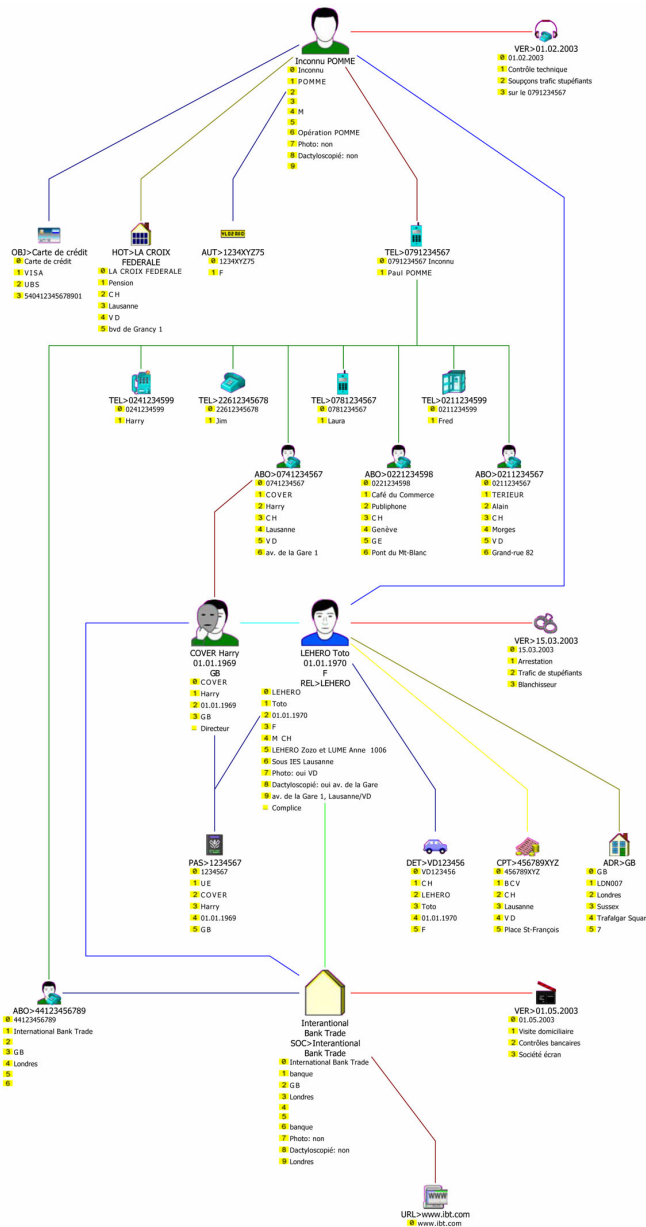


fig. 89 : JANUS PV : Schéma définitif sur la base du schéma provisoire issu de la base de données<sup>284</sup>

## 2.5.4 Synthèse

La base de données d'enquête centralisée qui souffrait le plus d'un manque de composant d'analyse était JANUS PV. Ce « sous-système » JANUS présentait l'avantage d'être ouvert et centré sur la *personne*, soit l'entité principale et de disposer d'un système de génération de liens basés sur d'autres types d'entités, soit des événements, des lieux, des moyens de communication, des choses, etc. Elle s'intégrait ainsi à une stratégie d'enquête qui consistait à partir de personnes pour découvrir leurs activités illicites, les mécanismes et les groupements criminels, ainsi que les complices impliqués. Cette base de données présentait toutefois des problèmes liés à sa structure hiérarchique et à la manière dont ces entités étaient enregistrées dans les antécédents.

<sup>284</sup> Cette figure est reproduite à l'Annexe I – Figures de grande taille

C'est pourquoi, le système disposait en dehors des *comparaisons*, de fonctions qui permettaient de générer des « listes de travail », qui résumaient l'ensemble des « sous-champs » d'une IDENTITE. Cette liste devait encore être retravaillée manuellement, mais elle permettait de produire une représentation graphique simple.

Il faut toutefois concéder que lors de la conception initiale de DOSIS, dont la structure allait être utilisée jusqu'en 2005 pour JANUS PV, les logiciels de visualisation graphique en étaient encore à leurs débuts et leur intégration en Suisse à ses balbutiements.

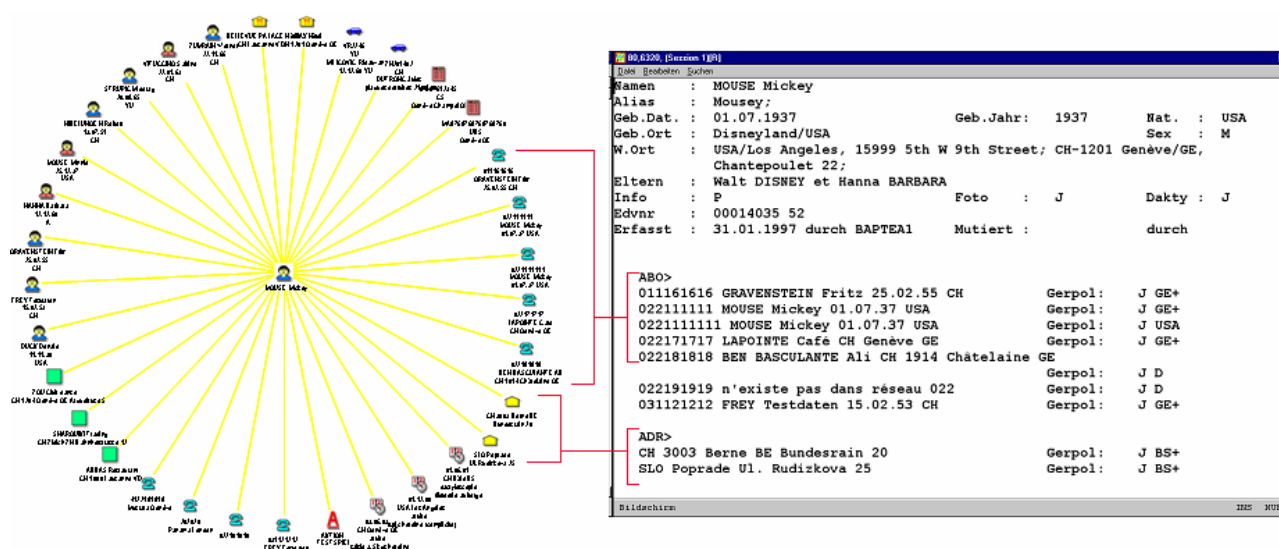


fig. 90 : Exemple de la visualisation manuelle d'une « liste de travail »<sup>285</sup>

Cependant, comme les outils de visualisation ne font que représenter l'information sur la base d'un modèle, cela montre bien que DOSIS et par extension JANUS jusqu'en 2005, ne permettait pas vraiment de raisonner « naturellement ». Ici, par exemple, toutes les entités étaient directement liées à l'entité principale, ce qui rendait toute interprétation difficile, voire carrément impossible. La plus-value de la visualisation par rapport à la « liste de travail » était donc minime.

Il était également possible de générer une « liste de travail spéciale » qui permettait de sélectionner le type de « sous-champs » apparaissant dans une opération de police et que l'on désirait lister.

<sup>285</sup> Figure tirée d'une présentation de N. DEWHIRST, OFP, 1998

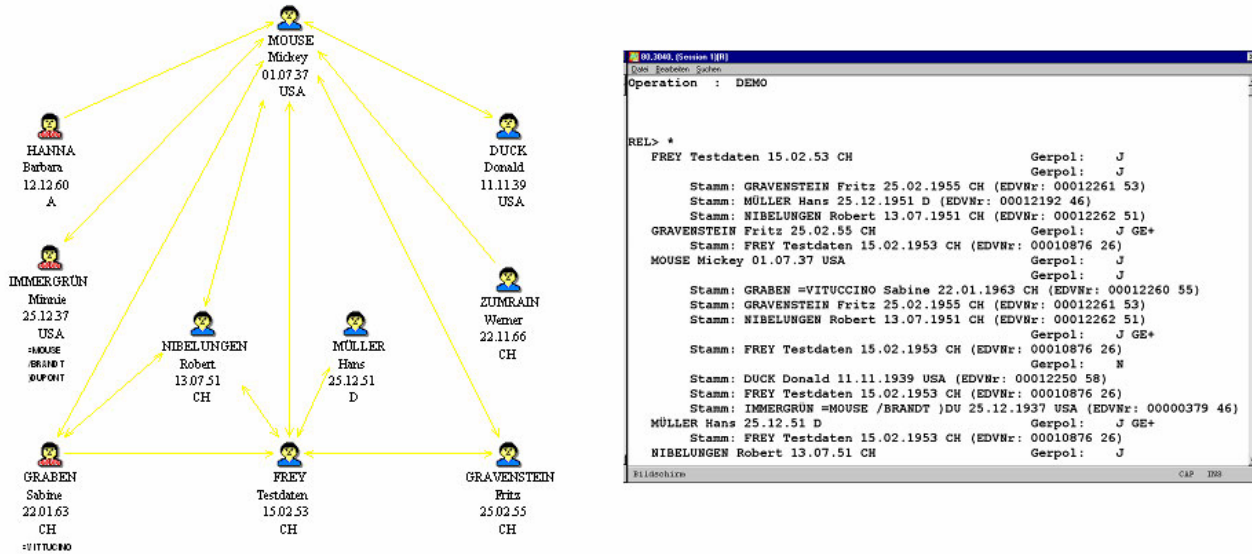


fig. 91 : Exemple de la visualisation manuelle d'une « liste de travail spéciale »<sup>286</sup>

Là encore, comme le montre la figure précédente, le niveau de détail était pauvre et si la saisie des données n'avait pas été faite avec le plus grand soin, en pensant déjà pouvoir profiter d'une visualisation graphique (qu'il aurait été plus aisé de réaliser sans DOSIS ou JANUS, d'ailleurs), le risque était grand de se retrouver avec des antécédents redondants et donc des entités complètement reliées entre elles.

### 2.5.4.1 Potentialités des systèmes centralisés de la Confédération

La situation technique qui a duré jusqu'au milieu de 2005, ne permettait de générer automatiquement des liens (par *comparaison*) que pour certains types d'entités, alors qu'un plus grand nombre avait été prévu au départ.

Le problème résidait essentiellement dans trois points structurels et organisationnels des données :

1. La structure déficiente des « sous-champs » qui caractérisaient les entités (identifiants pas ou mal définis) ;
2. La décomposition incomplète des « sous-champs », faisant perdre du coup le potentiel d'inférence des entités enchâssées ;
3. L'impossibilité de différencier une entité directement ou indirectement liée à une *personne* mentionnée en IDENTITE.

Le constat était le suivant : la version en vigueur avant juillet 2005 ne permettait pas d'analyser pleinement les données pourtant centralisées, même à l'aide des techniques d'analyse criminelle, ou

<sup>286</sup> Figure tirée d'une présentation de N. DEWHIRST, OFP, 1998



alors au prix d'un effort conséquent pour l'établissement manuel d'un état de la situation par un analyste détaché.

#### **2.5.4.2 Développements possibles**

Depuis 2002, la Confédération, plus particulièrement la division *planification et engagement*, par son commissariat Polsys (systèmes informatique de police) a projeté de faire évoluer le sous-système PV à l'instar de ce qui avait été réalisé l'année précédente avec le sous-système JO devenu JANUS+ JO.

Afin de ne pas répéter certaines erreurs de conception dues à un trop grand éloignement du concepteur de l'utilisateur final, un groupe de référence était mis sur pied. Celui-ci était constitué des membres du commissariat Polsys, des informaticiens du Département de justice et police (*CSI-DFJP*) et de membres volontaires des polices cantonales et fédérales (une dizaine de cantons ayant répondu à l'appel).

Le renouvellement de la technologie de JANUS PV était l'opportunité à saisir pour corriger tout ou partie des problèmes rencontrés avec la version précédente et tenter de réaliser le projet de cette recherche.

## 2.6 Hypothèse 2 – utilité du projet

**L'intégration d'un composant d'analyse externe couplé aux bases de données d'enquête centralisées et par conséquent compatible avec la structure des informations qui y sont contenues, est utile à l'investigation dans le cadre de la lutte contre la criminalité organisée.**

Lors des premières applications pratiques des méthodes d'analyse criminelle opérationnelle dans les enquêtes de police judiciaire, la plus-value a été particulièrement remarquée pour :

- l'appréciation de la situation par les investigateurs,
- le partage de l'information entre tous les acteurs de l'instruction (enquêteurs, spécialistes, magistrats, etc.),
- l'assurance de la qualité du travail effectué,
- l'aide à la compréhension lors de la préparation des dossiers pour la suite du processus judiciaire.

Les outils en exploitation au moment des premiers essais pratiques *in situ* demandaient un travail de ressaisie des données très important au détriment du travail de réflexion et d'analyse proprement dit. Il n'était donc pas envisageable de poursuivre l'exploitation de ces méthodes en routine au niveau de l'analyse de données centralisées. Une systématisation du traitement de l'information était donc nécessaire et une meilleure intégration des données de base était impérative.

Il s'agissait donc d'implémenter un système d'analyse là où se trouve déjà le centre de gravité de l'information, c'est à dire au sein des bases de données d'enquête de la Confédération.

Un certain nombre de questions peuvent être formulées dans le but de pouvoir plus facilement mesurer l'utilité du système. Nous en traiterons trois :

1. Le système apporte-t-il un gain d'informations ?
2. Le système apporte-t-il un gain de temps ?
3. Le système apporte-t-il un gain de capacité d'analyse ?

Et comme dans toute évolution en général, chaque nouvelle situation apporte de nouveaux problèmes. Donc, subsidiairement, le système apporte-t-il de nouvelles problématiques ?

C'est à ces quelques questions que nous tenterons de répondre dans la discussion de ce travail.

## 2.6.1 Méthodologie de test

Il sera difficile de pouvoir tester cette seconde hypothèse autrement qu'en se basant sur un certain nombre d'expériences pratiques. Voici toutefois sommairement comment nous envisageons de répondre aux trois premières questions que nous venons de nous poser.

### 2.6.1.1 Test du gain d'information

Il s'agira de mesurer aussi fidèlement que possible quatre améliorations prévues et les avantages qui devraient en découler sur la base d'un certain nombre d'indicateurs. Le gain d'information devra se faire dans le réservoir d'information, soit la base de données centralisée JANUS PV 2.0.

#### Système plus facile d'accès → Plus d'adhérents ?

Une première amélioration de JANUS PV 2.0 vient du fait que l'accès à cette base de données, ainsi qu'aux autres applications mises à disposition par la Confédération, devait se faire par l'intermédiaire d'un portail sécurisé unique. L'utilisateur une fois connecté à ce portail pouvait accéder aux bases de données sans avoir à se légitimer à nouveau.

Ce système d'accès devait permettre de surmonter les réticences des utilisateurs occasionnels qui se trouvaient neuf fois sur dix bloqués par les standards de sécurité, notamment sur la durée de validité des mots de passe, trop vite oubliés. Ainsi, le niveau d'adhésion des intervenants judiciaires devait logiquement augmenter et par voie de fait la quantité d'information pouvant être transmise par ces mêmes enquêteurs.

#### Système plus performant → Plus d'intérêt ?

Les technologies actuelles permettent de partager plus de ressources en un temps toujours plus réduit. Des fichiers multimédias (photos) devaient pouvoir ainsi être inclus aux fiches *personnes*. De plus, les recherches complexes et les *comparaisons* devaient être beaucoup plus rapides et concerner tous les « sous-champs ».

De la sorte, l'intérêt des utilisateurs devait augmenter, le système offrant plus de possibilités et répondant mieux et plus vite à leurs requêtes.

#### Système plus convivial → Plus de participants ?

Il s'agissait sans doute du point noir du système JANUS PV qui a fonctionné jusqu'en 2005. Alors que les systèmes d'exploitation graphiques fêtaient allégrement leur première décennie, les bases de données hiérarchiques, dont la navigation se fait par codes de fonction, passaient pour des dinosaures d'un autre âge.

JANUS PV 2.0 sous sa nouvelle forme devait se muer en un système correspondant aux nouveaux standards de navigation par arborescence et par onglets. Il devait aussi s'agir d'un système graphique qui s'adapte automatiquement à la résolution de l'écran. Ainsi, la participation générale devait augmenter, le système devant faire l'unanimité sur le plan de la convivialité.

### Système plus précis → Plus de données structurées ?

Enfin, les données objectives permettant de générer des liens devaient être plus précisément saisies dans le système. La précision des données enregistrées devait aller de pair avec l'augmentation de la structuration de celles-ci. Tout cela entraînant un avantage direct pour l'analyse ultérieure des informations.

#### **2.6.1.2 Test du gain de temps**

Le gain de temps devrait être mesurable tant au niveau de la base de donnée centralisée qu'au niveau des outils d'analyse. Des gains de temps peuvent intervenir en simplifiant les processus et en donnant accès aux données aux personnes qui en ont directement besoin.

### Système plus simple → Moins de saisies intermédiaires ?

Jusqu'en été 2005, dans le canton de Vaud, le système JANUS PV était de manière générale trop difficile d'accès et trop compliqué pour la saisie correcte d'informations pour l'ensemble des utilisateurs. C'est pourquoi un mode de saisie intermédiaire (fichier interface), sous la forme d'une formule MSExcel, appelée « Communiqué JANUS PV », avait été distribuée depuis 2002.

Désormais, le système étant plus simple, il est vraisemblable que cette formule interface, qui était transmise par l'enquêteur à du personnel dédié à la saisie, soit caduque et que l'enquêteur soit capable de saisir lui-même les informations dont il dispose.

### Système plus ouvert → Moins de double saisie ?

Disposer de systèmes qui prévoient des passerelles pour l'importation ou l'exportation de données est un très grand avantage lorsque l'on pratique l'analyse criminelle. Jusqu'en été 2005, comme il a déjà été mentionné, les données analysées étaient toutes ressaisies dans les logiciels d'analyse criminelle idoines.

Les possibilités d'interfacer les systèmes entre eux devaient radicalement diminuer les double ou triple saisies et ainsi gagner un temps très important.

### Système plus intégré → Moins de manipulations ?

L'intégration de données à tous niveaux est une autre de nos principales préoccupations. Les langages utilisés pour le transfert de données intègrent aujourd'hui les informations concernant les données elles-mêmes. On peut citer le langage XML<sup>287</sup>, qui devait être utilisé pour l'exportation et l'importation de données de JANUS PV 2.0.

Le système mieux intégré devait permettre au final aux intervenants de diminuer les manipulations nécessaires à l'exploitation des données dans les différents systèmes et ainsi gagner du temps.

---

<sup>287</sup> XML : *eXtensible Markup Language*. Le format XML, qui est de plus en plus répandu, est un métalangage, puisqu'il contient les données elles-mêmes, mais également la structure de ces données.

### Système plus précis → Moins de formatage ?

Une des principales manipulations des données est le reformatage. En effet, presque chaque système définit son propre standard. En informatique aussi, la normalisation et la standardisation sont plus que nécessaires. De plus en plus de normes ISO sont définies dans ce secteur. Les données sont globalement plus précisément définies selon les standards internationaux, ce qui diminue le reformatage des données, une fois que le même standard a été adopté par les différents systèmes et leurs utilisateurs. Le temps investi au départ devait très vraisemblablement être rentabilisé par la suite.

### **2.6.1.3 Test du gain de capacité d'analyse**

En ce qui concerne l'analyse, la situation est moins prévisible que pour le gain d'information et le gain de temps. En effet, des améliorations logicielles ont déjà eu lieu dans d'autres domaines et un raisonnement « non démonstratif » nous permet d'entrevoir ce que l'avenir devrait nous réserver. Pour le travail pur d'analyse, nous entrons dans une dimension nouvelle, qui n'a été explorée jusqu'ici que dans des situations ponctuelles et particulières. Nous pouvons toutefois imaginer quels pourraient être les amorces d'améliorations.

### Gain d'intégration → L'analyste analyse ?

Les systèmes étant mieux intégrés, le temps que passe l'analyste sur son cas devait être en beaucoup plus grande partie du travail d'analyse plutôt que de traitement de données.

L'analyste va-t-il analyser une situation plus vite et pouvoir ainsi traiter plus de cas, ou va-t-il pouvoir traiter les cas en plus grande profondeur ?

### Gain de précision → L'analyse est meilleure ?

Les systèmes étant plus précis, la décomposition des informations et les inférences devaient servir de base solide à l'analyse. Celle-ci devait logiquement s'en trouver renforcée et sa qualité devait augmenter. Cependant, en compensation sa complexité devrait, elle aussi, augmenter proportionnellement. Une analyse plus précise et plus complexe est-elle forcément meilleure ?

### Gain de décomposition → L'analyse est plus fine ?

La décomposition des informations devait être plus importante, ce qui devait permettre à l'analyste d'apprécier plus finement la situation. Mais à nouveau, le niveau de détail de l'analyse est intimement lié à la portée de celle-ci et à sa complexité. Une analyse plus fine et moins globale est-elle également meilleure ?

### Gain de structuration → L'analyse est plus standardisée ?

Enfin, les éléments devaient être plus structurés et les procédures mises en œuvre pouvaient par conséquent être plus facilement standardisables. Des procédures d'analyses standardisées sont-elles un gain de qualité ou une perte de créativité ?

#### **2.6.1.4 Recherche des problèmes persistants ou nouveaux**

Une fois le système fonctionnel, il a fallu rechercher activement les problèmes qui ont persisté et ceux, nouveaux, qui ont apparus. Seul le bilan du lot d'améliorations par rapport aux nouvelles problématiques permettra de trancher sur un éventuel progrès.

### 3 Réalisation

Dans ce troisième chapitre qui décrit la réalisation du projet de recherche, cinq points seront abordés.

La définition d'un modèle de base de données qui sera repris pour l'établissement des deux composants du système est discutée dans la première partie. Cette démarche méthodologique a également été suivie lors de la réalisation pratique du projet, dans le but de s'intégrer aux conditions cadres supérieures (contraintes politiques, légales, économiques, structurelles, et organisationnelles<sup>288</sup>) et tenter de les influencer lorsque cela était encore possible. Une fois le modèle fixé, il a fallu transmettre au sein du groupe de référence utilisateurs du nouveau système JANUS PV la méthode de travail qui était envisagée, afin qu'ils puissent en mesurer la portée et qu'ils puissent intégrer certaines requêtes spécifiques au cahier des charges de la nouvelle version. C'est donc naturellement que ce chapitre débute par une étude préliminaire devant déboucher sur la proposition d'un modèle de bases de données pouvant soutenir une analyse appropriée et qui corresponde aux stratégies et aux méthodes de travail des enquêteurs dans le contexte de la lutte contre la criminalité organisée. Des choix déterminants ont été faits à ce moment de la recherche et s'ils sont très souvent empiriques, ils ont été dictés par les meilleures pratiques connues. Ils sont évidemment discutables et les raisons de chacun de ces choix sont exposées textuellement.

Les trois parties suivantes de ce troisième chapitre sont les descriptions formelles des deux composants du système proposé, soit de JANUS PV 2.0 tel qu'il a été réalisé en été 2005, du composant de base de données d'analyse compatible, que nous avons baptisé *Prototype  $\beta$* , et des interconnexions entre les deux composants, puisqu'elles influencent grandement la faisabilité et l'efficacité du projet et qu'elles constituent une condition de sa réalisation.

Enfin, quelques expériences faites avec ces nouveaux composants constituant le système d'analyse bi-composant seront décrites dans la dernière partie.

#### 3.1 *Modèle méthodologique*

Le contexte de la criminalité organisée nous offre pléthore de situations différentes dans lesquelles les investigateurs doivent pouvoir évoluer. Que l'on s'intéresse à divers trafics, des montages financiers ou des séries de délits contre le patrimoine (cambriolages ou escroqueries), les enquêteurs doivent pouvoir traiter et gérer l'information à leur disposition d'une manière adéquate.

---

<sup>288</sup> Voir chapitre 1.4.3 – Cadre de l'analyse criminelle

Nous faisons donc un premier choix qui est de proposer un modèle de base de données d'analyse qui puisse s'appliquer au plus grand nombre de situations possibles. Il s'agit de généraliser au maximum le modèle. Il est, en outre, toujours plus aisé d'intégrer des éléments spécifiques à un modèle général que le contraire. La spécialisation sera d'ailleurs toujours possible par l'intermédiaire de composants d'analyse externes, disposant d'un degré de liberté au niveau de leur structure et de leurs fonctionnalités spécifiques<sup>289</sup>.

La structure du graphe, soit les entités, éléments factuels objectifs récoltés (structure du modèle), leurs connexions (organisation du modèle) et le degré de détail (niveau d'agrégation du modèle) nécessaire à sa réalisation sont décrits maintenant.

### **3.1.1 Entités**

La collecte d'éléments factuels est à la base de tout travail d'investigation. Il s'agit de faits avérés ou probables qui sont portés à la connaissance des autorités et qui présentent une utilité dans la recherche de la vérité. Ces éléments doivent être structurés de sorte à représenter ou modéliser aussi fidèlement que possible une situation réelle. La structure générale de ce modèle se fonde donc sur un modèle universel et « réaliste ».

Dans le cadre des investigations menées en rapport avec la criminalité organisée, nous avons vu que la stratégie d'enquête est, outre la démonstration de la commission d'infraction(s), de pouvoir replacer chaque protagoniste au sein du groupement criminel, afin de pouvoir déterminer son rôle et son influence. Ainsi, le modèle « réaliste » proposé devra permettre d'évaluer les relations interpersonnelles (qu'elles soient directes ou indirectes). Ces relations doivent pouvoir être établies sur la base de faits (comme des connexions téléphoniques, la présence de données personnelles de tiers, le partage ou le transfert de biens ou d'argent, etc.). Comme nous le verrons plus loin dans ce chapitre, la définition initiale du niveau de détail du modèle adopté est très importante car il est encore très difficile de naviguer entre les différents niveaux d'agrégation. Enfin, ce modèle doit permettre de remonter les raisonnements analytiques non-démonstratifs, qui ont été utilisés pour formuler les hypothèses, en synthétisant les éléments disponibles, en démontrant progressivement un état de fait. Ce qui consiste simplement en l'application de la méthode hypothético-déductive, utilisée abondamment lors des deux premières étapes de l'enquête qui sont de rechercher, puis de structurer la preuve. Cette dernière condition va grandement influencer le choix du niveau de détail.

#### **3.1.1.1 Type**

Les entités doivent être regroupées en différents types génériques. Nous nous tiendrons, par souci de simplicité et d'universalité, à des types qui sont le moins spécifiques possible. La mise en

---

<sup>289</sup> Voir par exemple des bases de données d'analyse spécifiques à une problématique précise. Telle que les escroqueries par Internet (Nigerian Connection), voir SCHIFFER *et al.*, 2004 et BIRRER *et al.*, 2005.



relation de ces entités, qui font partie des trois dimensions de l'enquête, doit permettre de reconstruire l'image de la situation et répondre aux questions fondamentales : qui, quoi, quand, où et comment<sup>290</sup>.

Les types d'entité que nous avons choisis sont au nombre de huit, soit :

- Personne
- Lieu
- Moyen de communication
- Moyen de transport
- Biens (choses)
- Biens (argent)
- Événement
- Forensique

Chaque type d'entité ci-dessus peut se subdiviser en différentes catégories, chacune ayant une spécificité. Cependant, les éléments d'un même type, bien que de catégories différentes, peuvent être immédiatement comparés entre eux, alors que des entités différentes n'ont pas cette capacité intrinsèque.

Voici ci-après le détail des huit types d'entités de notre modèle générique, avec leurs catégories.

### Personne

Il s'agit de l'entité centrale du modèle. Il n'y a pas vraiment d'alternative à ce choix, qui est imposé par le contexte judiciaire. Les autorités de poursuite pénale cherchent à comprendre et à analyser le fonctionnement d'organisations criminelles, dont les éléments sont des personnes. De plus, ce sont ces mêmes personnes qui vont devoir, en fin de compte, répondre de leurs actes devant la justice. Ce premier type d'entité peut revêtir plusieurs formes plus spécifiques :

#### *Personne physique*

La personne physique est la pierre angulaire du modèle d'investigation. Mais, pour pouvoir revêtir cette qualité, il faut qu'elle remplisse plusieurs conditions, qui ne sont pas toujours évidentes, lorsque l'on travaille avec des données imparfaites. Il faut que cette entité soit qualifiable d'humain et qu'elle soit identifiable au minimum par ses nom, prénom et date de naissance<sup>291</sup>.

#### *Personne morale*

Nous plaçons la personne morale au même niveau que la personne physique, bien qu'il s'agisse réellement d'un organisme « artificiel » administré par des personnes physiques. La raison pour laquelle la personne morale est placée dans le même type d'entités provient du fait que celle-ci peut

---

<sup>290</sup> Voir axiome 2

<sup>291</sup> En termes policiers, l'identité d'une personne comprend encore sa filiation et le lieu de sa naissance.

se comporter juridiquement comme une personne physique, et qu'elle peut également constituer un lien indirect entre des personnes physiques. Dans d'autres modèles génériques, les personnes morales constituent un type à part entière. Nous avons décidé de ne pas emprunter cette voie, considérant que celle-ci complique en fin de compte le modèle inutilement comparativement au bénéfice que l'on peut retirer de cette spécification<sup>292</sup>.

A nouveau, cet élément doit être identifiable comme tel au moins par son nom et sa raison sociale<sup>293</sup>.

#### *Personne inconnue*

Il est très important de considérer la personne inconnue comme une catégorie à part entière. Il s'agit d'un élément qui, s'il n'est pas apprécié au stade de la conception, peut poser de nombreux problèmes ultérieurs lors de l'analyse et de l'interprétation des données. La personne inconnue devrait idéalement constituer un état intermédiaire dans le processus d'investigation. Celle-ci devrait se transformer en cours d'enquête en une personne physique. Cette transformation est grandement simplifiée par le fait que ces catégories font partie du même type d'entité.

Il faut encore veiller à considérer les personnes inconnues comme uniques et différentes dans chaque situation où elles ne sont justement pas identifiables, et ne pas utiliser une seule et même personne « inconnue », reprise chaque fois. Il faudra donc leur donner des identités temporaires « d'investigation » afin de pouvoir les différencier, par exemple en les numérotant ou en leur donnant des surnoms.

#### Lieu

Ce deuxième type regroupe les lieux, identifiables comme tels parce qu'ils représentent une entité géographique et qu'ils constituent une dimension à part entière de l'investigation. Dans la réalité, il existe une multitude de types de lieux. Le but ici n'est pas de faire la liste exhaustive des catégories de lieux possibles, mais de les grouper en deux catégories spécifiques et une dernière qui servira d'entité universelle.

#### *Résidence privée*

La résidence privée est le lieu d'habitation d'une personne physique. Il s'agit d'un ou plusieurs lieux privilégiés pour cette dernière. La résidence privée est importante à plusieurs titres, puisque les autres personnes s'y trouvant ont une relation significative avec la personne d'intérêt. La résidence privée est caractérisée en général par une adresse (pays, canton, localité, rue et numéro).

---

<sup>292</sup> Concrètement, dans des listings, les personnes physiques et morales sont amalgamées avec notre modèle, alors qu'avec une spécification, cela ne serait pas le cas. De plus, dans ce modèle générique, il est nécessaire de définir des standards de saisie dans les champs *NOM* et *Prénom* utilisés pour la personne morale. Cependant, l'organisation de notre base est quasiment deux fois plus simple en regroupant ces deux catégories de personnes au même type d'entité.

<sup>293</sup> Pour la personne morale commerciale, il existe des registres commerciaux qui permettent d'identifier plus précisément une société, par un numéro d'enregistrement, par exemple.

*Résidence professionnelle*

Le lieu de travail est peut-être moins privilégié que la résidence privée, s'il est partagé par un grand nombre de personnes. Mais, d'un autre côté, il s'agit du lieu de résidence des personnes physiques. Là également, l'adresse est l'élément caractérisant.

*Lieu particulier*

Bien qu'il s'agisse ici de l'élément lieu universel, il est appelé « lieu particulier » puisqu'il s'agit d'une dénomination plus facilement compréhensible dans l'investigation. En effet, seuls les lieux revêtant un intérêt particulier sont utiles à l'investigation criminelle, qu'il s'agisse du lieu du crime, d'une rencontre ou de la commission d'une activité particulière.

Moyen de communication

Les moyens de communications prennent une part de plus en plus importante dans les investigations actuelles pour plusieurs raisons. Premièrement, ils se diversifient, se simplifient et surtout se démocratisent. Il est désormais aujourd'hui possible d'entrer en contact avec d'autres personnes dans le monde entier, sans aucun système onéreux, et quasiment sans délai grâce à la téléphonie mobile, notamment.

Par ailleurs, les données recueillies auprès des fournisseurs de service de communications lors des enquêtes permettent, dans la limite des contraintes légales, de récupérer des informations souvent déterminantes dans les investigations sur des réseaux criminels. Nous avons choisi de différencier trois catégories de moyens de communication.

*Courrier postal*

Il ne faut malgré tout pas oublier les moyens traditionnels comme le courrier postal, qui permet la transmission d'informations écrites ou de biens via les résidences privées, professionnelles ou simplement postales (case postale). Le courrier postal peut être adressé à une personne (physique ou morale) et à un lieu précis (adresse).

*Courrier électronique & Internet*

Il s'agit ici de la transmission de données pouvant être écrites, multimédia (sonores, graphiques, audiovisuelles) ou autres, le tout pouvant être protégé contre la surveillance par des processus de cryptage<sup>294</sup>. La transmission des données se fait par des adresses e-mail ou via le protocole IP (adresses IP).

*Téléphonie (fixe & mobile)*

La téléphonie peut être l'outil de travail de certains criminels, notamment des réseaux de trafiquants en tout genre. La téléphonie est aujourd'hui un moyen d'échange d'informations orales, écrites et aussi multimédia (fax, SMS, MMS, etc.). L'élément caractérisant un raccordement est en général un

---

<sup>294</sup> La grande liberté dont jouissent les Internauts et les possibilités très limitées des autorités de poursuite judiciaires sur Internet et/ou le courrier électronique, à cause du principe de territorialité, en font sans aucun doute le système de communication aujourd'hui le plus difficile à intercepter légalement. Néanmoins, il est parfois encore possible de retrouver des informations échangées via ce médium, en particulier lors des perquisitions ou de visites domiciliaires.

numéro d'appel, mais avec l'avènement de la téléphonie IP, des pseudonymes ont désormais aussi fait leur apparition.

### Moyen de transport

Les moyens de transport sont, tout comme les lieux, extrêmement divers. Cependant, certains d'entre eux présentent un intérêt particulier : ce sont les moyens de transport privés. Les autres revêtent un intérêt plus circonstanciel.

#### *Véhicule (privé)*

Il s'agit du véhicule d'une personne physique ou morale. Celui-ci est identifiable par des caractéristiques groupales (marque, modèle, etc.) et individuelles (immatriculation, numéro de châssis). Il sera également nécessaire de différencier le propriétaire et l'utilisateur d'un tel moyen de transport.

#### *Transport particulier*

Il peut s'agir d'un moyen de transport public ou privé intéressant puisqu'il aurait servi de lieu de rencontre ou d'un autre événement particulier.

### Biens (choses)

Les biens ou les choses permettent souvent de créer des liens entre les personnes, ces biens matériels pouvant changer de propriétaire ou d'utilisateur. Deux catégories ont été définies.

#### *Objets divers*

Cette catégorie d'objet est difficile à définir. Il peut potentiellement s'agir de toute chose permettant de faire un lien indirect entre des personnes. Un problème supplémentaire est souvent l'absence d'élément identifiant permettant d'individualiser l'objet en question. On se limitera donc normalement à des objets identifiables (présentant des numéros de séries) comme des cartes de crédit ou bancaires, des appareils électroniques, ou autres objets numérotés (produits de luxe, bijoux, armes, etc.).

#### *Papiers d'identité*

Les papiers d'identité méritent de figurer de manière spécifique dans les bases de données d'analyse. Ces derniers sont, par définition, rattachés à une personne physique précise et lorsqu'ils sont falsifiés, ils permettent de gérer les alias des criminels.

### Biens (argent)

A l'instar de la catégorie précédente, les biens en argent permettent également de générer des liens entre des personnes dans certaines conditions. C'est le cas lors de transactions identifiables, via des bordereaux d'organismes bancaires ou financiers, ou par l'intermédiaire de papiers valeurs numérotés, tels que les chèques. Les transactions en cash ne sont que très rarement identifiables. Ce n'est par exemple le cas que lors de rançon car les numéros de série des billets de banque sont relevés.

*Compte bancaire*

Le compte bancaire peut relier plusieurs personnes physiques ou morales. Généralement, il est identifié par un numéro et la banque qui le gère.

*Chèque & papier valeur*

Le chèque est un moyen de transaction identifiable puisqu'il porte un numéro et qu'il permet de relier plusieurs personnes entre elles lors de sa transaction.

Événement

Les événements font partie d'une catégorie particulière. Il s'agit de circonstances immatérielles qui revêtent une grande importance dans l'investigation. Les événements doivent autant que possible être identifiables par un aspect temporel précis, ainsi que par un lieu de commission. Notre modèle comporte quatre catégories, dont trois font référence au contexte judiciaire.

*Événement & rencontre*

Nous utiliserons cette entité pour tous les événements non-spécifiques et en particulier les rencontres de plusieurs personnes physiques. Cette entité permet généralement de faire une relation directe entre des protagonistes.

*Infraction*

Événement délictuel qui permettra de lier les suspects à des activités criminelles avérées.

*Arrestation*

Il s'agit d'un événement particulier dans la carrière criminelle d'un délinquant. Une arrestation signifie pour l'enquêteur qu'une quantité d'informations non négligeable doit se trouver auprès de l'autorité qui l'a effectuée.

*Condamnation*

Enfin, les criminels condamnés vont conserver une trace de leur(s) condamnation(s) dans les registres idoines. Ces condamnations peuvent signaler un récidiviste et ainsi orienter les recherches de police.

Forensique

Enfin, un dernier élément a droit à sa place dans le processus judiciaire. Il s'agit des éléments factuels de type forensique (souvent des traces), qui serviront de preuves lors du jugement. Ces éléments doivent figurer en bonne place dans le processus de renseignement, puisqu'ils auront une importance particulière en finalité. Ils permettent de lier quasiment toutes les autres entités entre elles. Le problème principal dans une base de renseignement de ce type de fait est bien souvent l'absence d'un identifiant connu. Seules les traces permettant l'identification formelle de personnes (empreintes digitales, ADN) disposent de codifications uniques et standardisées grâce à leur utilisations dans les bases de données nationales idoines.

### 3.1.1.2 Identifiant

La présence d'un identifiant pour chaque entité devrait être une condition *sine qua non* à sa mention dans une base d'analyse. Il n'est, en effet, pas possible de faire des liens directs ou indirects entre des personnes sans que les entités liantes ne soient clairement identifiables et individualisables. Autrement dit, sans cette condition, il n'est pas possible de gérer des liens objectifs, qui doivent rester démontrables. Ou pire, une utilisation incorrecte et insuffisamment précise de l'identifiant peut amener à des erreurs d'agrégation, ce qui entraînera de fausses interprétations qui peuvent être extrêmement dommageables.

Les criminels l'ont bien compris, puisqu'ils en jouent intentionnellement, par exemple, en prenant de faux noms ou en changeant fréquemment de téléphone, ce qui pose passablement de problèmes. Il s'agit alors de pouvoir gérer les alias et les relations personnes – objets de manière très précise et systématique !

Comme on l'a déjà vu dans la critique de la situation actuelle et en particulier lors de l'analyse de la structure de JANUS PV, l'identifiant peut regrouper plusieurs données brutes, soit au moins les « NOM », « Prénom » et « Date de naissance » pour des personnes.

Il s'agit de déterminer, pour chaque entité, quels sont les éléments nécessaires et suffisants à l'établissement d'une identité qu'il s'agisse d'une personne ou d'une autre entité.

Il faut toutefois trouver le juste équilibre. L'individualisation ne doit pas être trop contraignante. Par exemple, si on ajoute encore le lieu de naissance et la filiation (noms des parents) aux éléments cités ci-dessus afin de déterminer l'identité d'un individu dans une base d'analyse (qui ne va pas contenir des dizaines ou centaines de milliers d'individus), cela demandera trop d'efforts de collecte de données lors du travail de saisie usuel. Si par contre, il s'agit d'une base d'archives judiciaires, il est tout à fait nécessaire que les critères pour la définition d'une identité soient plus étendus et comprennent aussi le lieu de naissance et la filiation, afin de limiter au maximum les risques de confusion de personnes.

En fin de compte, le choix doit se faire entre individualisation et efficacité. On peut se dire que dans l'absolu, on préférera éviter tout risque de confusion en optant pour la solution la plus sûre et la plus complète, mais c'est sans compter sur un facteur pratique qu'est la « flemmardise naturelle » des utilisateurs. Ceux-ci, à défaut d'informations connues, emplissent souvent les champs obligatoires des bases de données de valeurs vides de sens, du genre « inconnu », « indéterminé », etc. Cette saisie approximative augmente en fait le risque de confusion puisque des éléments prévus comme étant discriminants deviennent récurrents.

L'étude de JANUS PV (version qui a été utilisée jusqu'en 2005) nous a aussi montré que les entités et leurs identifiants doivent être pris en compte dès le début du processus de création des bases de données, sous peine de voir leur capacité de liaison fortement diminuée, à cause d'erreurs initiales de conception difficilement corrigibles une fois le système en exploitation.

Très souvent, les systèmes de gestion de bases de données (SGBD) relationnelles utilisent des identifiants alphanumériques propres à leurs tables. Ils sont nécessaires à leur fonctionnement et ont l'avantage d'être constitués d'un champ unique. Cependant, ils n'ont aucune signification réelle et ne peuvent pas être synchronisés entre différents SGBD. Pour cette raison, si de tels identifiants doivent être utilisés, ce n'est que pour compléter une identification ou à titre de référence d'une base dans l'autre.

### 3.1.1.3 Représentation graphique des entités

La représentation des entités par des dessins facilement reconnaissables a été rendue possible ces dernières années grâce aux logiciels de visualisation utilisant l'iconographie<sup>295</sup>. Nous allons passer en revue les possibilités qui sont offertes actuellement par ces logiciels.

Le tableau ci-dessous propose une iconographie correspondant à notre modèle générique.

#### Iconographie

Types	Catégories	Icônes (exemples)
<b>Personne</b>	Personne physique	
	Personne morale	
	Inconnu	
<b>Lieu</b>	Résidence privée	
	Résidence professionnelle	
	Lieu particulier	
<b>Moyen de communication</b>	Courrier postal	
	Courrier électronique & Internet	
	Téléphonie (fixe et mobile)	
<b>Moyen de transport</b>	Véhicule privé	
	Transport particulier	
<b>Biens (choses)</b>	Objets divers	
	Papiers d'identité	
<b>Biens (argent)</b>	Compte bancaire	
	Chèque & papier valeur	

<sup>295</sup> Nous entendons par là une symbolologie particulière qui est l'utilisation de pictogrammes.















Types (suite)	Catégories	Icônes (exemples)
<b>Événement</b>	Événement & rencontre	 
	Infraction	    
	Arrestation	
	Condamnation	
<b>Forensique</b>	Trace	    

fig. 92 : Exemple d'iconographie actuelle<sup>296</sup>

On remarque que les possibilités actuelles d'iconographie sont très étendues et qu'il est même possible de trouver plusieurs icônes dans les diverses catégories de chaque type.

Tant que cela tombe sous le sens commun, il n'y a pas de problème à les détailler. Cependant, il s'agit ici de fixer leur utilisation selon le niveau de détail adéquat, et de ne pas tomber dans l'excès d'esthétique, ce qui a pour conséquence de décrédibiliser le schéma. Si un interlocuteur dit à l'analyste que son schéma est « joli », il n'y voit souvent plus que le côté « cosmétique » et ne cherche visiblement pas à comprendre réellement la situation représentée.

### 3.1.2 Connexions

Le lexique de notre nouveau langage commun a maintenant été établi. Il s'agit désormais d'en définir la syntaxe, soit les règles qui permettent d'arranger, de connecter les éléments entre eux, afin de donner un sens à l'ensemble.

#### 3.1.2.1 Types

La syntaxe des visualisations est composée par différents types de connexions. Notre modèle centré sur la personne nous permet de diviser les connexions en deux types principaux. Il y a d'une part les relations directes entre les personnes et les relations indirectes, elles-mêmes décomposables en différents niveaux, en fonction des entités intermédiaires. Le contenu de l'information qui permet de faire le lien est utilisé comme légende dudit lien. Ce contenu peut être prédéfini en listes de choix, ce qui permet d'en standardiser la saisie.

##### Relations directes

Il s'agit ici de relations inter-personnes directes, que ce soient des personnes physiques, morales ou inconnues. Dans les enquêtes pénales, ces relations ne sont pas toujours évidentes à démontrer et ne doivent être mentionnées que lorsqu'elles sont sans équivoque, ou alors de manière hypothétique, en attente de leur confirmation. Elles ne seront donc pas fréquentes. La combinaison des différentes catégories de personnes de notre modèle sont les suivantes :

<sup>296</sup> Les icônes ont été tirées de la version 6 de l'*Analyst's Notebook™* de i2 inc.



*Relation Personne physique – Personne physique*

Les relations de ce type doivent pouvoir être formellement établies. Par exemple, on pourra mentionner des liens de parenté, de mariage ou de concubinage, ou encore des liens déjà établis par une enquête précédente et dont la nature a été confirmée par les protagonistes eux-mêmes ou par d'autres éléments factuels indirects, ceci par souci de simplification. Il est, en effet, inutile de répéter *ad aeternam* le détail des relations indirectes avérées.

*Relation Personne physique – Personne morale*

La relation entre une personne physique et une personne morale peut être de plusieurs ordres. Il s'agira ici de mentionner les liens forts comme la fonction de directeur ou d'employé dans l'organisme. Le simple contact avec une personne morale ne devrait être mentionné que s'il apporte un éclairage particulier à l'enquête (par exemple si la société est lésée).

*Relation Personne physique – Personne inconnue*

Il sera fréquent de trouver des liens entre des personnes physiques et des personnes inconnues. De cette manière, on pourra gérer simplement les inconnus ainsi que les noms d'emprunt ou les alias. Une personne dont la fausse identité a été constatée devrait être représentée par une personne inconnue avec son faux nom et reliée par alias à son identité réelle.

*Relation Personne morale – Personne inconnue*

Les relations entre les inconnus et les personnes morales devraient être moins fréquentes, mais elles doivent suivre les règles des relations entre les personnes physiques et les personnes morales. Le statut d'inconnu devant être temporaire.

*Relation Personne morale – Personne morale*

Deux personnes morales peuvent être en relation, par exemple contractuellement. Dans d'autres cas de figure, on préférera passer par une représentation indirecte du lien, notamment par des personnes physiques ayant un rôle particulier dans plusieurs sociétés, par exemple au sein d'organes de direction ou des conseils d'administration.

*Relation Personne inconnue – Personne inconnue*

Ces relations devraient être exceptionnelles, les relations directes entre des personnes physiques devant être avérées et vérifiées. On peut imaginer cependant d'user de ce lien pour mentionner que deux suspects inconnus seraient complices d'une ou plusieurs infractions.

Relations indirectes

Il s'agit des relations indirectes entre deux personnes, dans le sens que des entités intermédiaires se trouvent intercalées. Ces relations ont pour but de relier des personnes entre elles par le biais d'entités démontrant le lien. Il n'est pas nécessaire que les relations indirectes soient complètes dès le début. Elles peuvent être saisies de proche en proche en fonction de leur relation directe avec une personne. Les inférences indirectes entre les personnes se construisent d'elles-mêmes, de manière fortuite ou délibérée, lorsque les entités sont individualisables.

*Relation Lieu – Personne*

Relation Résidence privée – Personne

Cette relation peut être décrite comme le lieu de résidence d'une personne physique ou morale, soit son adresse principale ou encore ses résidences secondaires.

Relation Résidence professionnelle – Personne

Parallèlement aux résidences secondaires, il est possible de relier une personne physique directement à son adresse professionnelle, si le rôle de cet employeur ou raison individuelle n'intervient pas directement dans l'affaire.

Relation Lieu particulier - Personne

Il s'agit ici simplement de mentionner le lien entre une personne et un lieu particulièrement intéressant pour les investigations. Il s'agit d'une relation générique.

*Relation Moyen de communication - Personne*

Relation Courrier postal – Personne

Dans ce cas de figure, il peut être nécessaire de mentionner un ou plusieurs courriers qui sont échangés entre des personnes. Des éléments découverts lors d'une surveillance postale peuvent s'avérer très importants. Ce lien doit définir qui est l'émetteur ou le récepteur des envois (direction).

Relation Courrier électronique – Personne

Un échange de messages électroniques ou via tout autre système basé sur le réseau Internet (Chat, IRC, *peer to peer*, etc.) peut revêtir un intérêt particulier. Il est alors nécessaire de mentionner les différents utilisateurs de ces médias.

Relation Téléphonie – Personne

L'abonnement et/ou l'utilisation de la téléphonie doivent également être enregistrés. Ils sont une source de renseignements encore très importante à ce jour. Les communications entre les raccordements téléphoniques doivent être saisies comme des liens indirects entre les raccordements eux-mêmes, soit d'un niveau supérieur.

*Relation Moyen de transport – Personne*

Relation Véhicule (privé) – Personne

La possession ou l'utilisation d'un moyen de transport privé.

Relation Transport particulier – Personne

L'utilisation d'un moyen de transport particulier peut être également dans certaines situations un facteur important, même s'il peut paraître inutile dans une mémoire à long terme.

*Relation Biens (choses) – Personne*

Relation Objets (divers) – Personne

Il s'agit ici de mentionner le lien entre une personne et une chose identifiable, soit sa possession ou son utilisation.

### Relation Papiers d'identité – Personne

La relation entre une personne et des papiers d'identité peuvent être de plusieurs ordres. Dans le cas normal, les documents d'identités sont utilisés pour attester de son identité. Or, dans le contexte criminel, il arrive souvent que ceux-ci soient falsifiés et utilisés pour attester d'une autre identité que son identité réelle. Ces deux types relations doivent pouvoir être mentionnées.

### *Relation Biens (argent) – Personne*

#### Relation Compte bancaire – Personne

Dans le monde de la finance, il existe plusieurs types de relations entre un compte bancaire et des personnes physiques ou morales. On peut rencontrer des bénéficiaires économiques, des porteurs de procurations, etc. Toutefois, ces différentes relations dénotent un certain droit sur ledit compte. Le bénéficiaire ou l'utilisateur d'un tel compte peut revêtir un caractère très intéressant dans les affaires de criminalité financière ou organisée, notamment lorsque des transferts bancaires font l'objet d'investigations.

#### Relation Chèque & papier valeur – Personne

La relation indirecte entre deux personnes par le biais de chèques, de bordereaux, ou de papiers valeur permet de démontrer un transfert d'argent. Dans ce cas de figure, le récepteur de ces biens doit pouvoir être enregistré (direction), si le montant n'est pas déposé sur un compte, mais qu'il est directement encaissé.

### *Relation Evènement – Personne*

#### Relation Evènement & rencontre – Personne

Mention de la participation d'une personne à un événement particulier.

#### Relation Infraction – Personne

Il s'agit de répertorier des infractions qui concernent une personne en particulier et pour lesquelles elle a joué un rôle quelconque, soit comme auteur, co-auteur, complice, etc. .

#### Relation Arrestation – Personne

Lorsqu'une personne est arrêtée, il s'agit d'une information judiciaire importante.

#### Relation Condamnation – Personne

Idem, mais pour les condamnations.

### *Relation Forensique – Personne*

Il s'agit ici de mentionner les éléments forensiques récoltés sur une personne, lors d'une interpellation, comme les empreintes digitales, ou son profil génétique.

Nous n'avons traité jusqu'ici que des relations entre l'entité centrale, la *personne*, et les autres entités. Nous verrons plus tard en détail comment des liens entre les autres entités doivent être traités.

### 3.1.2.2 Représentation graphique des connexions

La représentation graphique des relations entre les différentes entités se fait selon les nouveaux standards de l'analyse criminelle à l'aide de connecteurs (traits) qui sont codés par couleur (chromographie) et qui dénotent également la qualité de la relation (trait continu, discontinu ou pointillé), ainsi que de son sens (flèche).

L'utilisation des codes de couleur permettent de spécifier graphiquement par un standard les différents types de relation énoncés ci-dessus. Le tableau de la page suivante propose une standardisation possible.

#### Chromographie





















Types	Eléments objectifs	Icônes	Relations Personne
Personne	Personne physique		_____ (bleu roi)
	Personne morale		_____ (vert pâle)
	Inconnu		_____ (bleu pâle)
Lieu	Résidence privée		_____ (vert olive)
	Résidence professionnelle		_____ (vert olive)
	Lieu particulier		_____ (noir)
Moyen de communication	Courrier postal		_____ (violet)
	Courrier électronique & Internet		_____ (turquoise)
	Téléphonie (fixe et mobile)		_____ (marron)
Moyen de transport	Véhicule privé		_____ (bleu foncé)
	Transport particulier		_____ (rose)
Biens (choses)	Objets divers		_____ (bleu foncé)
	Papiers d'identité		_____ (bleu foncé)
Biens (argent)	Compte bancaire		_____ (jaune)
	Chèque & papier valeur		_____ (jaune)
Evénement	Evénement & rencontre		_____ (rose)
	Infraction		_____ (rouge)
	Arrestation		_____ (rouge)
	Condamnation		_____ (rouge)
Forensique	Trace		_____ (gris)

fig. 93 : Exemple de chromographie actuelle<sup>297</sup>

<sup>297</sup> Les couleurs s'inspirent des standards suisses et du logiciel *Analyst's Notebook™* de *i2 inc.*

### Qualité de la relation

Comme nous l'avons vu aux chapitres précédents, la qualité des informations qui entrent en considération pour notre analyse peut être variable. C'est pourquoi nous devons reproduire dans le langage graphique des notions de qualité de l'information.

Pour évaluer l'information, nous avons vu le système 4x4 qui demande une évaluation de la source de l'information puis de leur relation. Les programmes de visualisation actuels tel que l'*Analyst's Notebook™* proposent par défaut de représenter trois degrés de qualité :

Qualité de la relation	Représentation
Confirmée	_____
Non – confirmée	-----
Possible	.....

Nous sommes d'avis que ces trois degrés de qualité sont suffisants pour éviter d'apporter trop d'importance à une relation incertaine dans son appréciation de la situation.

Lors des investigations, l'enquêteur va devoir s'efforcer de trouver d'autres sources d'informations pour tenter de confirmer ses hypothèses basées sur des informations capitales, mais qui ne sont pas confirmées.

L'utilisation de niveaux d'incertitude trop détaillés va sans doute amener à une mauvaise utilisation de ceux-ci, l'appréciation entre cinq ou seize (4x4) niveaux d'incertitude prêtant toujours à discussion.

### Sens de la relation

Dans une situation strictement centrée sur la personne, il n'est en général pas nécessaire d'inclure le sens de la relation. Dans ce cas de figure, on répertorie des personnes physiques, inconnues ou morales et leurs attributs propres, en espérant trouver des interconnexions entre ces différentes personnes.

Cependant, l'intérêt de la chose grandit, lorsque des relations indirectes sont présentes. C'est le cas, par exemple, lorsque l'on s'intéresse aux interactions téléphoniques, postales ou bancaires. Il est nécessaire d'inclure le sens de l'interaction, soit : qui appelle, qui envoie, qui envoie de l'argent et qui la reçoit.

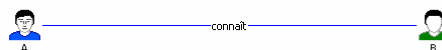
Dès lors, se pose le choix du degré de détail nécessaire à la recherche et à la gestion des liens, soit le nombre de niveaux de liens indirects entre des personnes. Cette problématique est justement abordée au point suivant.

### 3.1.3 Niveau de détail

Le niveau de détail est un facteur primordial et qui doit être une préoccupation constante des personnes intervenant dans les processus d'investigation et qui doit être défini *a priori*.

Prenons un exemple très simple : Une personne physique identifiée comme « A » appelle par téléphone une personne inconnue B. Différents niveaux de détail s'offrent à nous pour enregistrer et représenter cette information.

- « A » est en relation avec « Inconnu B » :



- « A » appelle par téléphone l'« Inconnu B » :



- « A » utilise son raccordement fixe « 021 A » pour appeler, le 30.09.2005 à 16h57, le raccordement prépayé « 079 B » utilisé par « Inconnu B » :

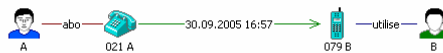


fig. 94 : Degré de détail – décomposition de l'information

On remarque immédiatement que la troisième solution est celle qui reflète le plus fidèlement la réalité et permet d'apprécier la situation avec le plus de précision.

Cependant, elle nécessite de pouvoir gérer des relations entre différentes entités qui ne sont pas que des personnes. Il s'agit de relations indirectes de niveau 2.

On pourrait encore compliquer la situation, mais, dans l'idéal, il ne devrait pas apparaître de relations de niveau supérieur à 2 :

- « A » utilise son raccordement fixe « 021 A » pour appeler le raccordement « 079 X » au nom de la « société X » et utilisé par un inconnu surnommé « Jules ». La « société X » est composée de deux personnes « J » (employé) et « B » (directrice) :

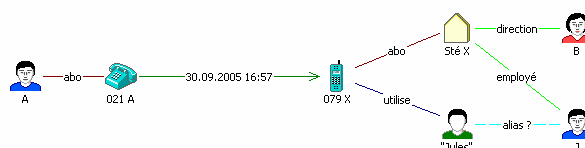


fig. 95 : Degré de détail – décomposition de niveau 2

Dans la situation ci-dessus, à part l'appel téléphonique, les entités sont en contact direct avec une personne (physique, morale ou inconnue). Il n'y a donc pas de relation de niveau supérieur à 2.

On pourrait imaginer des routings complexes par le biais de numéros téléphoniques déviés, qui entraîneraient des liens indirects de niveau supérieur. Mais il ne s'agit que d'artéfacts techniques qu'il n'est pas nécessaire d'énoncer systématiquement. On pourrait tout de même le représenter, mais uniquement à titre d'exemple pour illustrer la tentative délibérée de brouiller les pistes.

Une question se pose toutefois : pourquoi a-t-on besoin d'un degré de détail important dans le contexte de la lutte contre la criminalité organisée ?

Comme on peut s'y attendre, il arrive très fréquemment que les acteurs impliqués dans les affaires de criminalité organisée ne s'expliquent que très partiellement, ou pas du tout, sur leurs agissements et leurs relations. Il arrive aussi parfois qu'ils nient l'évidence, sans doute par principe, ou alors en connaissant les faiblesses du système judiciaire. L'enquêteur doit alors démontrer tout ce qu'il avance. Pour y parvenir, il est nécessaire d'être capable remonter l'enchaînement des inférences et de pouvoir les décomposer en éléments factuels vérifiables. Voilà pourquoi dans ce contexte particulier un grand niveau de détail est nécessaire.

### 3.1.3.1 Matrice relationnelle

Si le niveau de détail doit être important et qu'il peut être nécessaire de décomposer autant que possible les faits recueillis, quelles en sont les conséquences sur le modèle générique que nous essayons de construire ?

Afin de montrer la complexité que peut prendre la décomposition des faits, observons ce qui se passerait si nous voulions connecter chaque entité de notre lexique (volontairement réduit) de vingt mots avec chacun des autres.

Dans la matrice relationnelle présentée à la page suivante, on a considéré que les entités de départ ou d'arrivée sont équivalentes. Le sens de la relation n'est pas pris en compte, sinon, on devrait multiplier le nombre des relations possibles par trois (—, ←, →).

La formule pour calculer la combinaison arithmétique des entités est :  $\frac{n(n+1)}{2}$

Il est évident que plus on augmente son vocabulaire, le nombre d'éléments qui peuvent être associés deux à deux, le nombre de combinaisons augmente exponentiellement.

Donc, avec notre modèle, si  $n=20$  on a 210 combinaisons possibles.

Toutefois, la plupart des relations possibles n'ont aucune signification dans le monde réel, ou alors, elles peuvent être regroupées selon le type d'entité.

Nous avons centré notre modèle sur la personne et avons défini les relations directes ou indirectes. Les relations des personnes entre elles ou avec des entités différentes ont été déjà énoncées.

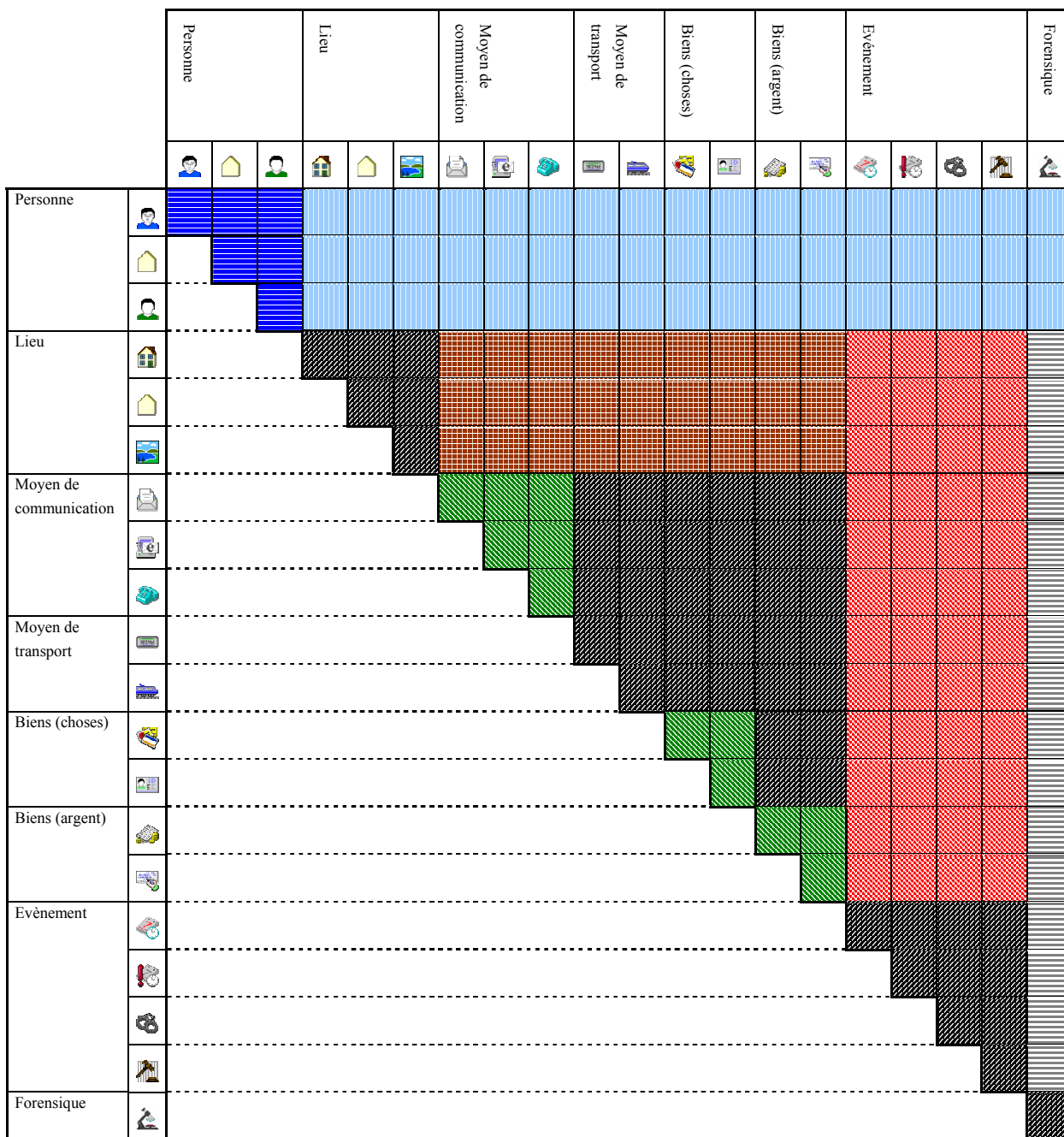
	Personne			Lieu			Moyen de communication			Moyen de transport		Biens (choses)		Biens (argent)		Evènement			Forensique		
Personne																					
Lieu																					
Moyen de communication																					
Moyen de transport																					
Biens (choses)																					
Biens (argent)																					
Evènement																					
Forensique																					

fig. 96 : Matrice relationnelle théorique du modèle générique

Les relations indirectes de niveau 2 qui peuvent être rencontrées concernent certaines entités de même type entre elles. Par exemple une communication téléphonique entre deux appareils téléphoniques ou une transaction financière. Par contre, il n'y a, par exemple, aucun sens de relier un téléphone avec un chèque.

La matrice relationnelle se réduit peu à peu en groupant les éléments à ce qui est schématisé ci-après :





**Légende** : en bleu : les relations « Personne » directes et indirectes ; en marron : les localisations; en rouge : les événements ; en vert : les transactions; en gris : les relations traces; et en noir : relations non-spécifiques (lien générique).

fig. 97 : Matrice relationnelle pratique du modèle générique

Les relations de lieux ont une importance particulière, puisqu'il s'agit d'une des dimensions de l'enquête. C'est pourquoi elles doivent constituer un groupe de relations indirectes à part entière, tout comme les liens possibles avec des événements, qui constituent la dimension du *temps*. Les relations traces doivent à nos yeux aussi constituer aussi un groupe de relations spécifiques, ceci principalement pour faciliter le travail de structuration de la preuve lors de la seconde étape de l'enquête, celles-ci y jouant habituellement un rôle prépondérant. Enfin, le reste des relations

possibles peut être regroupé en un lien générique, dont la spécificité n'est pas contrôlée par le système et qui préserve ainsi la souplesse nécessaire à une base d'analyse. On diminue de la sorte drastiquement le nombre de relations prédéfinies réellement utiles (ici sept).

Ce nombre ne devrait pas dépasser une dizaine, sous peine de rendre la saisie d'informations dans la base de connaissance trop laborieuse.

### 3.1.3.2 Adéquation du niveau de détail à la situation

Il est très important de définir à l'avance le niveau de détail en fonction des besoins des intervenants et surtout du but qui est recherché par la base de données d'analyse.

Nous avons vu dans la description du projet que les besoins des enquêteurs et ceux des analystes n'étaient pas les mêmes<sup>298</sup>, alors qu'ils cherchent tous deux à résoudre des affaires criminelles. Si un compromis doit être trouvé, il s'agit de déterminer, avant de mettre des moyens en œuvre, les questions auxquelles la base de données doit être capable de répondre. En voici quelques exemples :

- Situation 1 : Un enquêteur se trouve dans la situation de contrôler la présence ou l'absence d'une personne suspecte dans la base de données. Il va rechercher par son identité. Ici, le niveau de détail n'importe pas puisque l'entité « Personne » est l'élément central de la base de données.

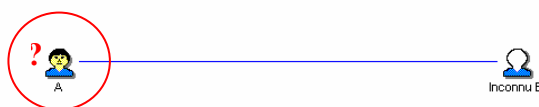


fig. 98 : Recherche d'une personne

- Situation 2 : Un analyste désirant établir le profil téléphonique<sup>299</sup> d'un suspect va vouloir comparer les correspondants téléphoniques de celui-ci avec la base de données contenant des raccords utilisés par des personnes délinquantes.

Si cette comparaison ne donne rien de positif, cela revient à dire que le suspect n'est pas en contact avec des délinquants connus. Le degré de détail apporté à la représentation prend plus d'importance, car on recherche désormais des entités créant des relations indirectes entre des personnes. Il faut donc qu'un degré de détail suffisant soit utilisé :

<sup>298</sup> Voir chapitre 2.5.1 – Besoins de chaque intervenant

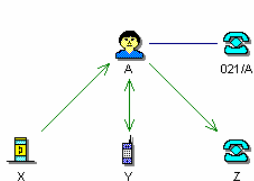
<sup>299</sup> Le logiciel CTAnalyser (voir chapitre 1.4.6.2) a été conçu justement pour réaliser rapidement et systématiquement ce type de profil.



fig. 99 : Analyse du profil téléphonique d'un suspect

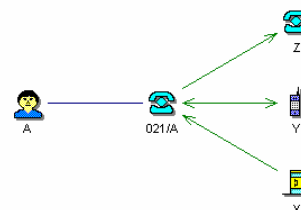
- Situation 3 : L'investigateur fait la même recherche que précédemment, mais trouve un résultat positif. Il lui sera ensuite nécessaire de pouvoir analyser plus finement ces relations, afin de pouvoir apprécier le degré d'implication de son suspect avec les différents délinquants de la base de données. Il lui faudra pouvoir répondre à un certain nombre de questions, soit : Quels sont les raccordements connus ? Qui sont les utilisateurs de ces raccordements et quels sont leurs antécédents ?

Pour que cette appréciation soit possible, il faut d'une part que les entités liant les personnes (les raccordements téléphoniques) soient présentes dans la base de données, et d'autre part, que l'organisation de cette dernière soit prédéfinie correctement, c'est-à-dire que les liens indirects soient formalisés et structurés dans ce but :



Tout est lié à la personne

Seul le type de connexions permet de différencier les propres raccordements de « A » (lien direct) par rapport aux raccordements avec lesquels il est en contact (lien indirect).

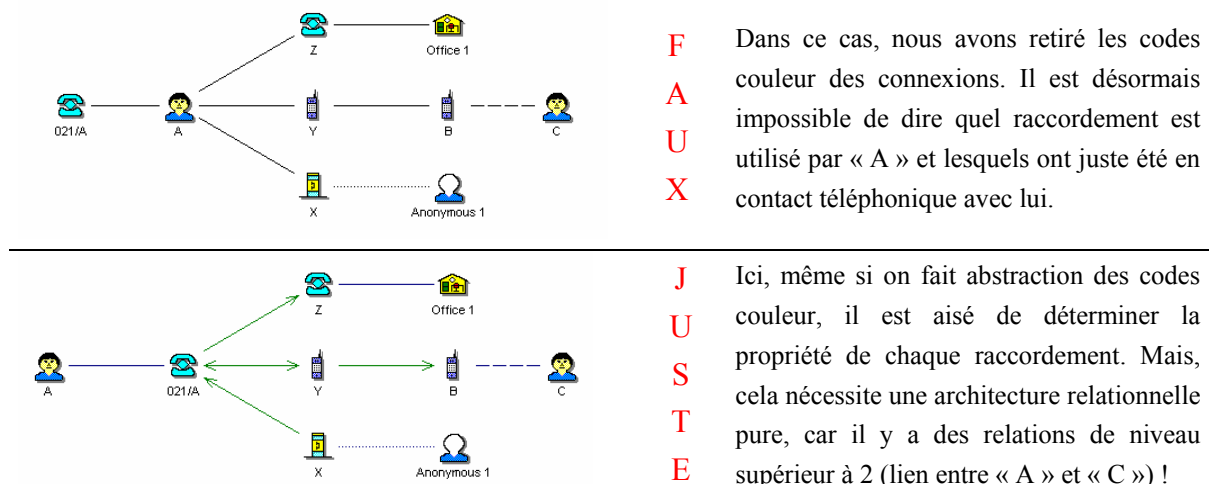


Les liens indirects sont formalisés

Les appels téléphoniques sont clairement représentés comme étant des connexions entre deux appareils téléphoniques (liens indirects de niveau 2)

fig. 100 : Décomposition incomplète des liens indirects

La décomposition des liens indirects nécessite une organisation des données prédéfinie *a priori* si l'on veut éviter les erreurs telles que représentées ci-après :



**F** Dans ce cas, nous avons retiré les codes couleur des connexions. Il est désormais impossible de dire quel raccordement est utilisé par « A » et lesquels ont juste été en contact téléphonique avec lui.

**J** Ici, même si on fait abstraction des codes couleur, il est aisé de déterminer la propriété de chaque raccordement. Mais, cela nécessite une architecture relationnelle pure, car il y a des relations de niveau supérieur à 2 (lien entre « A » et « C ») !

fig. 101 : Représentation correcte des relations indirectes

### 3.1.3.3 Possibilités de navigation (niveaux d'agrégation)

Malheureusement, les logiciels de représentation graphique ne permettent pas (encore ?) de naviguer dans des gradations de détail comme on le connaît aujourd'hui avec les cartes digitales de géographie. Cette lacune technologique nous oblige, tout comme le cartographe de l'époque (qui travaillait sur des croquis en papier), à déterminer à l'avance la bonne échelle en fonction des besoins opérationnels.

Dans le cadre des enquêtes criminelles, nous ne travaillons pas, de plus, avec des données aussi figées que les relevés topographiques. Le choix initial du niveau d'agrégation est aussi déterminé par cette évolutivité rapide des informations, les croquis devant pouvoir facilement s'adapter aux nouvelles informations. L'agrégation de données compliquant significativement la mise à jour.

Pour illustrer ce propos, voici une mise en parallèle du facteur de zoom (niveau d'agrégation) entre un diagramme relationnel sur une affaire fictive de recel avec une carte géographique du trajet de Lausanne à Morges :

Zoom minimum : (but : situer les éléments principaux)

N'apparaissent ici que les entités principales (localités – personnes) et la mention très grossière de leurs relations des unes par rapport aux autres (position relative).

On peut, par analogie, ne pas savoir sur la carte géographique quel type de route relie Lausanne à Morges, on a juste une vue des principales localités vaudoises.

Sur le diagramme relationnel, on remarque cinq personnages, dont une personne C qui semble intervenir dans cette affaire, mais les liens sont incertains. Cette représentation ne nous permet pas de comprendre ce qui s'est passé mais uniquement de connaître les personnes impliquées.

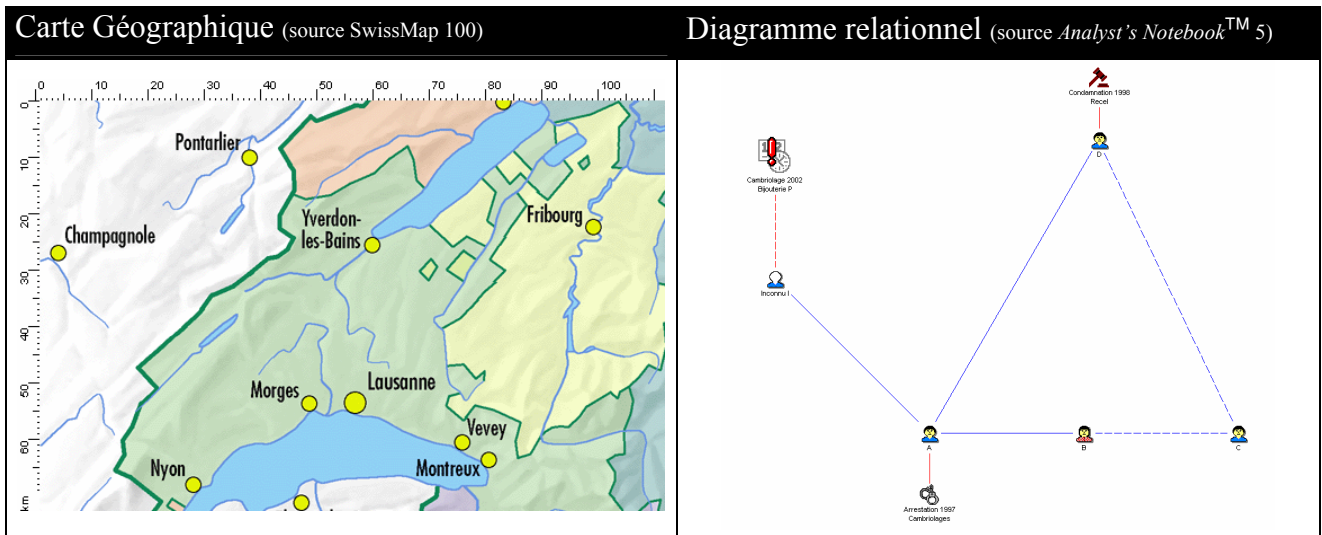


fig. 102 : Niveau de détail - Zoom minimum

Zoom moyen : (but : déterminer les connexions principales)

Avec ce niveau de détail, nous avons désormais schématisé les moyens de liaison entre les entités principales.

Sur la carte, il est désormais possible de remarquer des liaisons autoroutière et ferroviaire entre Lausanne et Morges.

Dans le diagramme relationnel, on note que la personne A (connue comme cambrioleur) a eu des contacts téléphoniques avec trois autres personnes, dont l'inconnu I qui est suspecté du cambriolage récent de la bijouterie P, une femme B chez qui A semble loger et une personne D condamnée pour recel. Enfin, C semble avoir été en contact avec D lors d'un déplacement en commun dans le véhicule de ce dernier.

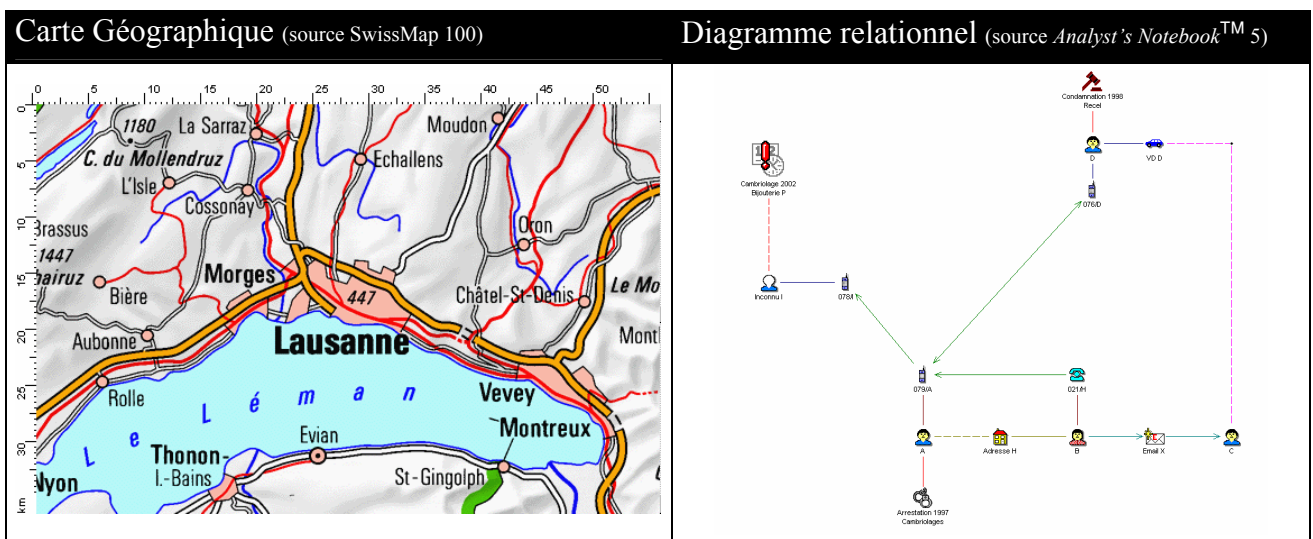


fig. 103 : Niveau de détail - Zoom moyen

Zoom maximum : (but apprécier la situation précise)

Ici, tous les éléments sont détaillés pour que l'on puisse apprécier la situation précisément.

Sur la carte, on distingue désormais aussi la possibilité de se rendre par une route secondaire qui chemine le long du lac. Cette solution peut être celle qui nous convient le mieux.

Sur le diagramme relationnel, des informations complémentaires apparaissent, notamment les transferts de biens (choses et argent). On voit maintenant qu'un échange a eu lieu entre l'inconnu I et la personne A, qui lui a remis de l'argent contre des bijoux. Cet argent provient peut-être de la femme B qui a reçu un virement bancaire équivalent et pour lequel elle a confirmé la réception à l'individu C. Enfin, la personne A devait avoir rendez-vous avec D pour lui remettre les bijoux.

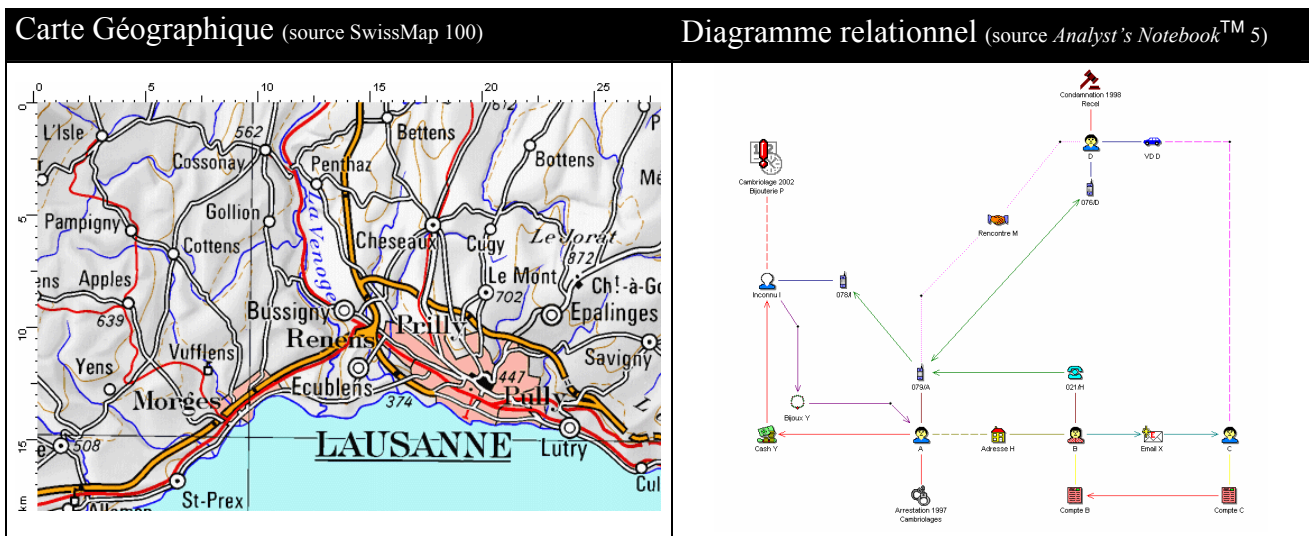


fig. 104 : Niveau de détail - Zoom maximum

Il est évident que la masse d'information présente sur ces visualisations dépend directement du degré de détail que l'on choisit. Mais il est plus intéressant de constater que, comme l'a montré l'exemple ci-dessus, l'échelle de la carte et le degré d'agrégation des données sur le schéma relationnel nous permettent bien de répondre à des questions se situant à des niveaux correspondants de généralité.

Un plan de ville très détaillé vous permettra de trouver une rue et, sans doute, même l'emplacement d'une adresse précise. Mais, si vous ne situez pas le quartier ou même la localité dans l'ensemble d'une région, vous ne pourrez pas vous rendre à cette adresse.

Il en est de même avec les données objectives de la criminalité, organisée dans un modèle. Imaginez que l'on utilise le plus grand niveau de détail, cela nous permet de déterminer sans trop de peine les liens et les fonctionnements d'une organisation criminelle. Mais, si nous ne pouvons pas changer de facteur de grossissement pour, par exemple, situer cette organisation par rapport à d'autres groupements criminels du même type, nous n'arriverons plus du tout à apprécier cette situation de manière globale. Nous serons alors toujours submergés par trop d'informations de détail.

Il s'agira alors de rétablir une nouvelle représentation adéquate à cette nouvelle question qui fait référence non plus à des connexions intra- mais inter-organisationnelles, en adaptant le niveau d'agrégation des données brutes disponibles.

Le besoin de représenter les informations à différents niveaux d'agrégation est donc évident. La définition de ces niveaux est toutefois beaucoup plus difficile. Il s'agit d'une question de modélisation, plus que de réalisation, qui peut s'appuyer sur des règles générales (représenter des relations entre des personnes en faisant apparaître progressivement des objets à chaque niveau), mais qui dépend aussi du problème spécifique à traiter (représenter un lot de montres comme le butin d'un vol ou représenter chaque montre individuellement).

### 3.1.4 Synthèse

Le modèle décrit ici est directement inspiré des expériences pratiques acquises en situation réelle ou en situation d'exercice<sup>300</sup>. Ce modèle s'inspire d'une part des techniques de représentation graphique et des standardisations qui ont vu le jour grâce à l'utilisation de certains logiciels et d'autre part des besoins des investigateurs dans la reconstruction de l'image de la situation en se basant sur les faits récoltés durant l'enquête.

Dès 2001, ce modèle pragmatique a été utilisé pour la création et l'utilisation d'une base de données d'analyse *générique*. Ce travail a servi non seulement de base à l'élaboration du prototype  $\beta$  qui sera présenté plus loin, mais il a surtout été utilisé pour illustrer les besoins de l'analyste criminel lors des séances du groupe de travail de JANUS PV 2.0. De nombreuses idées ont été reprises et intégrées à la nouvelle version de JANUS PV.

---

<sup>300</sup> Notamment dans le cadre de plusieurs exercices à l'échelle 1:1 du service de sécurité de la police militaire (SSPM) de 1999 à 2006.

### **3.2 *JANUS PV 2.0 (base de données d'enquête centralisée)***

Le système JANUS PV datait d'une quinzaine d'années, puisque seule sa dénomination avait évolué en fonction des diverses réorganisations de l'Office Fédéral de la Police. Le système lui-même n'avait subi que des retouches mineures. Ce n'est qu'en 2002 que le premier sous-système était véritablement mis à jour. Il s'agissait de JANUS JO, qui devint JANUS+ JO. La mise en service de ce nouveau sous-système posa quelques sérieux problèmes, notamment parce que les utilisateurs du système (les policiers) n'avaient pas été consultés lors de l'élaboration de la nouvelle version.

Fondamentalement, le résultat de la migration de JANUS JO en 2002 n'était pas mauvais, malgré quelques erreurs de conception. Mais, la migration avait été trop importante, puisqu'on était passé d'un système hiérarchique, dans sa structure et sa navigation, à un système strictement relationnel. Les avantages de l'ancien système hiérarchique, soit la simplicité de recherche et de saisie (malgré une navigation peu conviviale), avaient été remplacés par une saisie plus compliquée (rigueur, exhaustivité), accentuée par une navigation déroutante. Cette nouvelle base présentait néanmoins tous les avantages des bases relationnelles, soit une grande structuration des données, ce qui aurait dû réjouir les analystes. Mais, les avantages d'un système strictement relationnel étaient insuffisamment exploités. Les possibilités de visualisation et d'analyse des données, bien que présentes, étaient restreintes et elles n'étaient accessibles qu'à des utilisateurs expérimentés ou des analystes spécialisés. Le sentiment général des utilisateurs était donc plus que mitigé.

Cette migration difficile a eu pour effet la création d'un groupe de travail, composé d'utilisateurs de référence, dont l'auteur de cette recherche a fait partie. Il avait pour mission de définir le cahier de charges du nouveau JANUS PV et d'assurer le suivi de sa mise en production.

Ce groupe de travail a été constitué en 2002. Il était composé des membres du service informatique du Département fédéral de Justice et Police (CSI-DFJP), les spécialistes des systèmes de police au sein de l'OFP (PJF-Polsys), ainsi que des utilisateurs des cantons ayant manifesté un intérêt (AG, BE, BS, GE, LU, SG, TG, TI, VD et ZH). Le rôle de l'auteur était de rendre les développeurs attentifs aux besoins des analystes et que le système mis à jour puisse être compatible avec l'analyse criminelle.

Ce groupe de travail s'est réuni à intervalles réguliers, soit entre 6 à 10 fois par an, de 2002 à 2005. Un certain nombre de retards se sont accumulés durant le développement du projet, notamment à cause de restrictions budgétaires, ainsi que des remplacements successifs, pour diverses raisons, des deux premiers chefs de projet du CSI-DFJP.

Néanmoins, le nouveau « sous-système » JANUS PV 2.0 est entré en fonction dans le courant du mois d'août 2005. Les chapitres suivants décrivent cette nouvelle version du système de base de données d'enquête commun aux polices judiciaires suisses.



Depuis l'été 2007 et la mise à niveau du « sous-système » JANUS+ JO, les deux « sous-systèmes » sont à nouveau réunis en une seule application, baptisée JANUS 3.0.

### 3.2.1 Introduction

Les premières réunions du groupe de travail ont défini un certain nombre de recommandations clés qui devaient régir l'ensemble du projet. Le nouveau JANUS PV, en plus de respecter le cadre légal décrit dans l'ordonnance idoine<sup>301</sup>, devait répondre aux exigences suivantes :

- Etre centralisé et sécurisé au même titre que son prédécesseur.
- Pouvoir récupérer au mieux les données contenues dans l'ancien système.
- Etre axé sur les besoins des utilisateurs et rester aussi simple que possible lors de la saisie et de la recherche d'informations avec un temps de réponse inférieur à 3 secondes.
- Permettre de rechercher automatiquement des liens par lots (*comparaisons*).
- Permettre l'importation de données depuis des systèmes externes (cantonaux ou techniques) et l'exportation de données pour l'analyse.

Des recherches ont été faites, principalement par les membres du groupe Polsys de la PJF, afin de rechercher un produit commercial qui satisfasse aux exigences énoncées ci-dessus et qui soit financièrement acceptable.

Il est assez rapidement apparu que ce qui posait le plus de problème était la sécurisation des données. En effet, le système fédéraliste suisse provoque une multiplication des critères de sécurité qui sont définis selon les règles de procédures cantonales, les données étant, de plus, classées et sécurisées selon des domaines de criminalité décrits dans l'ordonnance JANUS. Le système devait donc être capable de gérer la sécurité non seulement selon le profil de l'utilisateur (administrateur, membre du groupe de contrôle [LPD], super-utilisateur, utilisateur ou encore analyste), mais également selon le rattachement juridique (PJF, polices cantonales ou municipales, etc.) et selon le domaine de criminalité (crime organisé, stupéfiants, traite des êtres humains, terrorisme, etc.).

Il s'agissait donc de définir une sorte de matrice en trois dimensions en accordant des niveaux de sécurité selon les règles de procédures cantonales et fédérales. Aucun système commercial ne disposait à la base d'une telle fonctionnalité.

Il a donc été nécessaire de développer le nouveau système en interne, avec les ressources disponibles au sein du CSI-DFJP.

Pratiquement, le CSI-DFJP devait mettre à disposition les ressources et les technologies nécessaires, soit des systèmes de gestion de bases de données adéquats (type Oracle), à prétention relationnelle, ainsi que des outils d'accès aux données via une interface client de type JAVA aussi légère que possible et indépendante de l'environnement de l'utilisateur distant.

---

<sup>301</sup> RS 360.2 – Ordonnance sur le système informatisé de la Police judiciaire fédérale du 30 novembre 2001

Il était primordial que l'utilisateur se sente à l'aise lors de la consultation des données. C'est pourquoi le masque de recherche de base a été particulièrement travaillé par le groupe de travail, et adapté aux besoins les plus courants, la grande majorité des recherches portant sur les mêmes critères (nom, prénom, date de naissance, numéro de téléphone).

La figure suivante reproduit ce masque de recherche de base :

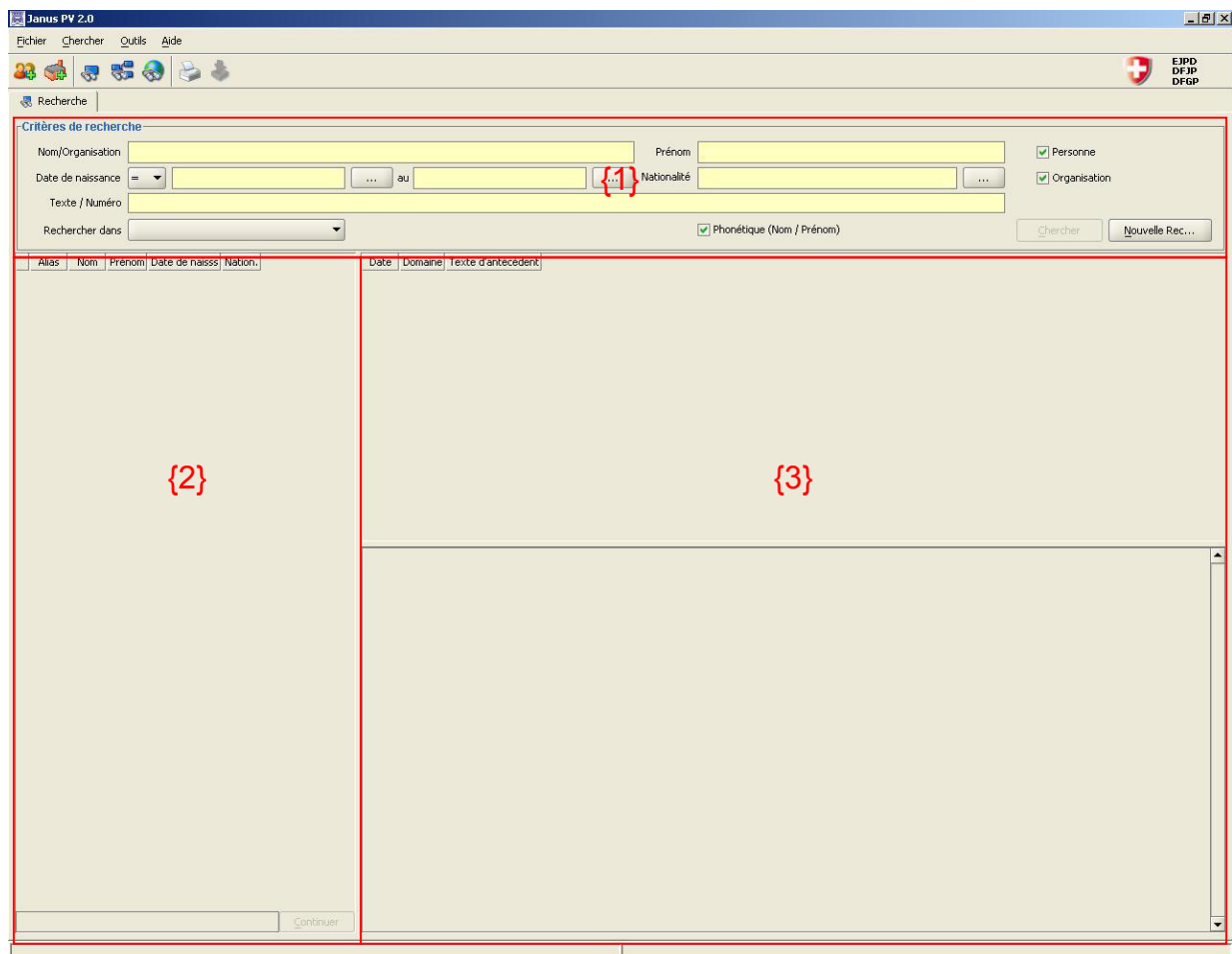


fig. 105 : Masque de recherche de base de JANUS PV 2.0

Le masque de recherche de JANUS PV2.0 est divisé en trois parties principales. La première, en haut {1}, contient les critères de recherche ; la deuxième en bas à gauche {2}, la liste des identités répondant aux critères de la recherche ; et finalement la troisième, en bas à droite {3}, le détail des antécédents des identités sélectionnées sur la gauche.

De la sorte, il est possible de consulter sur un seul et même masque les résultats d'une recherche de base. Si l'utilisateur désire approfondir la consultation d'une personne, il lui suffit de « double-cliquer » sur celle-ci, ce qui a pour effet d'ouvrir le masque de consultation des personnes (voir plus loin).

D'autres aspects furent encore abordés durant les trois ans de la réalisation du projet, comme, par exemple la simplification des accès aux nombreuses bases de données nécessaires au travail de police et mises à disposition par la Confédération.

C'est ainsi qu'un portail unique donnant accès à un maximum d'applications a été développé, puis mis en service simultanément à JANUS PV 2.0. Ce portail baptisé *SSO-Portal DFJP* était dans un premier temps accessible à l'aide d'un simple challenge *nom d'utilisateur – mot de passe*, mais il a été remplacé en 2006 par des clés chiffrées déposées sur des cartes à puces personnelles. Ce système baptisé *PKI-admin*, permet également de chiffrer les communications de manière forte<sup>302</sup>.

### 3.2.2 Structure et organisation

Comme nous l'avons mentionné ci-dessus, un des critères principaux du nouveau système était de pouvoir récupérer les données en répondant aux exigences légales. Il ne s'agissait donc pas ici de tout remettre en question. La structure du système devait rester sensiblement la même, sachant qu'elle donnait satisfaction jusqu'ici.

JANUS PV 2.0 devait donc rester un système de gestion de *personnes* suspectes et de leurs *antécédents*.

Une autre prérogative du nouveau système était de conserver les possibilités de recherche automatique de liens (*comparaisons*). Il était donc nécessaire de conserver un système de gestion des entités liantes.

Cependant, comme on l'a vu au chapitre 2.3.4 (faisabilité du projet), des problèmes structurels subsistaient au niveau de certaines entités, qui étaient uniquement enregistrées sous forme de texte marqués par les « sous-champs » dans l'ancien système.

On rappellera ici que ces problèmes étaient liés à une mauvaise définition des identifiants, à une décomposition incomplète des entités et à une confusion de niveaux entre les liens indirects.

C'est pour cette dernière raison qu'une distinction fondamentale a été faite dans ce nouveau JANUS PV entre certaines entités permettant de faire des liens indirects de niveau 1 (son propre téléphone, son propre compte bancaire, sa propre voiture) et les mêmes entités pouvant se retrouver à des niveaux supérieurs (numéro de téléphone d'un ami, etc.). Les éléments en lien direct avec la personne ont été appelés des « attributs » et les liens indirects en relation avec un antécédent restent des « sous-champs », bien qu'ils fassent tous deux partie d'une même base d'« objets ». Les « attributs » figurent désormais sur le masque de la personne.

---

<sup>302</sup> Le système d'écoute centralisé du service concerné (SCPT) au sein du CSI-DFJP (*LIS – Lawful Interception System*) dispose également d'un tel niveau de sécurité dans les communications avec le serveur, mais le moyen utilisé est encore différent (*SecureID*).

La figure suivante représente le masque de saisie/consultations d'une PERSONNE :

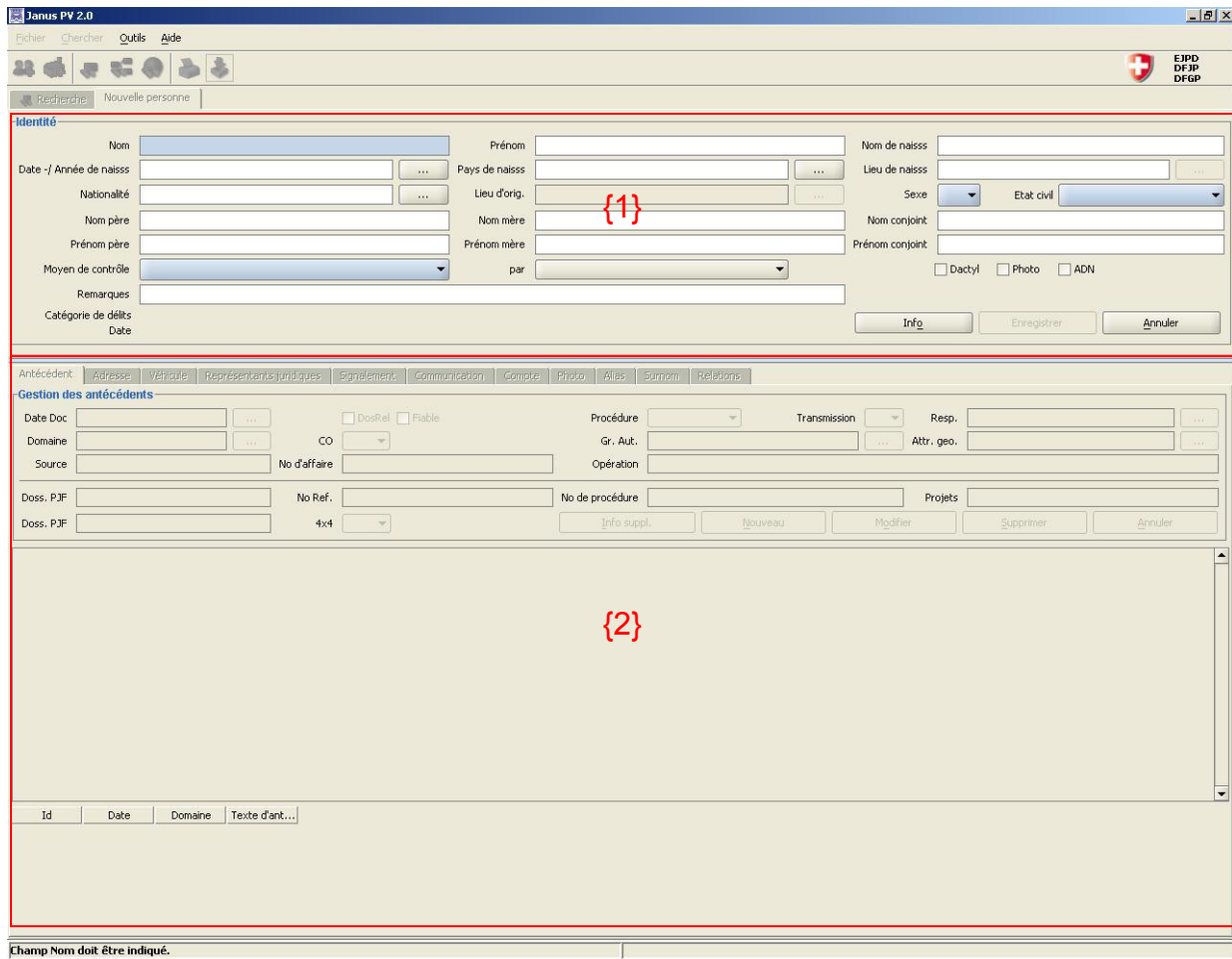


fig. 106 : Masque PERSONNE-ANTÉCÉDENT(S) de JANUS PV 2.0

Le masque PERSONNE est divisé en deux parties principales : la première, en haut {1}, contient les éléments de l'identité de la personne, alors que la seconde, en bas {2}, contient les antécédents et les « attributs » de la personne, consultables à l'aide d'onglets.

On remarque par rapport à l'ancien JANUS PV, que l'identité de la personne<sup>303</sup> s'est étoffée de champs plus structurés permettant de préciser l'identité complète d'une personne. Par exemple, l'ancien champ filiation a été décomposé en « nom du père », « prénom du père », « nom de la mère » et « prénom de la mère ». Il s'agit d'une demande des enquêteurs, pour qui le nombre et la structuration des champs de l'ancienne mouture étaient insuffisants dans ce cas.

<sup>303</sup> Nous reviendrons plus en détail sur la problématique de l'identité et de l'individualisation de ce type d'entité. Cependant, on peut préciser que les noms étrangers sont ici traités en appliquant des règles de phonétiques.

Au niveau de l'antécédent, il y a, à nouveau, peu de changements. Ils se cantonnent à des champs supplémentaires afin de pouvoir préciser le numéro de la procédure pénale pour les cantons, ainsi qu'une série de champs spécifique aux besoins internes de la PJF.

### 3.2.3 Entités : « sous-champs » et « attributs »

Les entités liantes ont donc été subdivisées en deux catégories, qu'elles soient directement liées à la personne (« attributs ») ou indirectement (« sous-champs »). Cette différenciation devait permettre à l'enquêteur de pouvoir interpréter plus rapidement les résultats des *comparaisons* automatiques et devait également permettre de générer des représentations graphiques qui différencient au moins ces deux niveaux, comme le montre la figure ci-dessous.

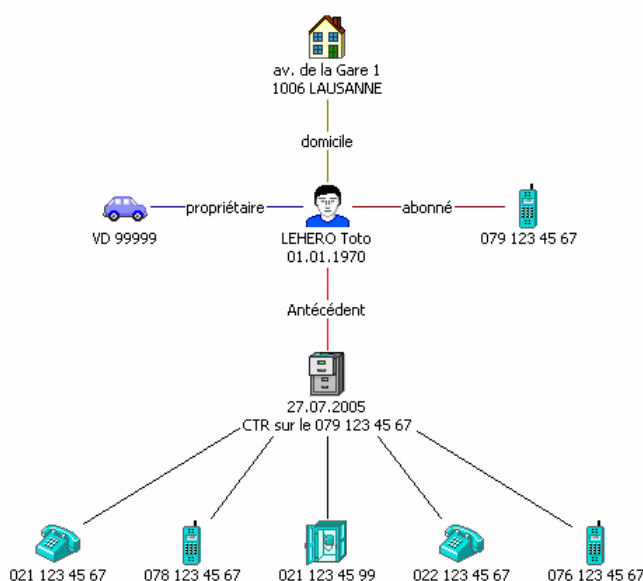


fig. 107 : Séparation des niveaux (« sous-champs » et « attributs »)

Alors que les « attributs » sont directement disponibles pour la saisie et la consultation dans les onglets du masque PERSONNE-ANTÉCÉDENT(S), les « sous-champs » se trouvent toujours dans le corps du texte de l'antécédent, comme dans l'ancien JANUS PV.

En sus des relations interpersonnelles directes récapitulées dans des onglets spécifiques (« Alias » et « Relations »), les « attributs » retenus par le groupe de travail sont au nombre de quatre :

- Onglet *Adresse* (lieu)
- Onglet *Véhicule* (moyen de transport)
- Onglet *Communication* (moyen de communication)
- Onglet *Compte* (biens [argent])

Il s'agit de tous les types définis dans le modèle d'analyse générique<sup>304</sup> à l'exception des événements (qui sont en fait des antécédents) et des traces (de type forensique). JANUS PV 2.0 suit donc assez fidèlement ce modèle.

D'autres onglets sont présents, mais il ne s'agit pas d'entités permettant une inférence, mais d'informations supplémentaires sur la personne :

- Onglet *Représentant juridique* (pour une personne morale)
- Onglet *Signalement* (pour une personne physique)
- Onglet *Photo* (idem)
- Onglet *Surnom* (idem)

Toutefois, afin d'être comparables, les entités (les « attributs » et les « sous-champs ») doivent figurer dans les mêmes tables de la base de données. C'est pourquoi au sens strict, ils sont tous définis comme des « objets » de JANUS PV 2.0, et sont informatiquement parlant stockés en format XML.

### 3.2.3.1 Objets de JANUS PV 2.0

L'étude des « sous-champs » de JANUS PV avait montré que cette ancienne version souffrait de deux problèmes. Le premier était la structure défaillante des « sous-champs » qui ne permettait pas de disposer d'un identifiant clairement défini, et le second était l'enchâssement de liens de différents niveaux dans un seul et même « sous-champ ».

Le problème du manque de structure des « sous-champs » de l'ancien JANUS PV devait être résolu avec cette nouvelle version. En effet, leur syntaxe n'est désormais plus simplement suggérée, mais il s'agit de remplir des rubriques structurées et prévues pour recevoir un type d'information déterminé, le formatage dans le texte étant ensuite automatisé.

Cette structuration des « sous-champs » allait bien évidemment poser un problème de récupération des anciennes données. Mais, comme la capacité de liaison de nombreux « sous-champs » n'était pas satisfaisante, certains d'entre eux étaient donc en fait très rarement utilisés. Les « sous-champs » réellement présents étaient les relations (REL> & SOC>), les numéros de téléphone (TEL> & ABO>), ainsi que les événements (VER>). Il a été prévu par le chef du projet au sein de la PJF-Polsys que des équipes soient mises sur pied au sein du service de contrôle, afin de restructurer certains « sous-champs » dans les meilleurs délais<sup>305</sup>.

---

<sup>304</sup> Voir chapitre 3.1.1 – Eléments objectifs

<sup>305</sup> En réalité, peu d'antécédents ont été corrigés, la validité opérationnelle moyenne de ces informations n'étant que d'une vingtaine de mois.

Pour saisir un « sous-champ », l'utilisateur doit donc maintenant activer une fenêtre de dialogue. Une fois les informations introduites, les données apparaissent automatiquement dans le texte de l'antécédent comme c'était ce cas dans l'ancienne version.

Le tableau suivant décrit les objets (« sous-champs » et « attributs ») de cette nouvelle version.

Description	« Sous-champ »	« Attribut »
Adresse	ADR	Adresse
Numéro d'immatriculation	AUT	Véhicule
Confiscation, caution, rencontre	BST	
Compte bancaire ou postal	CPT	Compte
Transaction	FTA	
Hôtel	HOT	
Communication (numéro, IMEI, SIM)	KOM	Communication
Objet	OBJ	
Organisation criminelle	ORG	
Passeport, pièce identité	PAS	
Profil stupéfiants	PRO	
Relation (personne)	REL	(Relation)
Routing	RTG	
Société	SOC	
Mesure de contrainte	VER	

fig. 108 : Objets (« sous-champs » et « attributs ») de JANUS PV 2.0

#### « Sous-champ » ADR et « attribut » Adresse

Voici donc la première description d'un « objet » liant pour lequel les relations indirectes de différents niveaux (« attribut » et « sous-champ ») peuvent désormais être distinguées.

Les « sous-champs » *ADR* – *Adresse* et l'« attribut » *Adresse* sont quasiment identiques. Le problème avec les entités de type *Lieu* est la qualité et la standardisation de la saisie, afin que l'identifiant, composé généralement de presque toutes les rubriques présentes, ait encore une certaine validité.

fig. 109 : PV2 – « Sous-champ » ADR

Avec JANUS PV 2.0, le groupe de travail a décidé d'inclure la norme ISO pour les pays, et, en ce qui concerne les numéros postaux et les localités, la table de conversion officielle de *La Poste* a été utilisée. Ce système plus contraignant (les pays apparaissent sous forme de codes) a connu quelques

défauts de jeunesse (erreurs dans la table de conversion), mais il devait effectivement montrer des améliorations dans la qualité de la saisie à plus long terme.



fig. 110 : PV2 – « Attribut » Adresse

« Sous-champ » AUT et « attribut » Véhicule

On retrouve exactement la même configuration des liens indirects pour le « sous-champ » *AUT – Numéro d’immatriculation*.

En plus du numéro d’immatriculation qui est l’identifiant, on trouve des informations descriptives du véhicule, soit le type, la marque et le modèle.



fig. 111 : PV2 – « Sous-champ » AUT

En ce qui concerne l’« attribut » *Véhicule*, des informations plus précises peuvent encore être saisies, comme le numéro de châssis et le numéro matricule. Ces informations figurent de manière standard dans les fichiers de véhicules et comme il n’est possible de saisir un véhicule en « attribut » qu’après avoir fait ces contrôles d’usage, il a été jugé utile par le groupe de travail d’ajouter ces deux rubriques informatives.



fig. 112 : PV2 – « Attribut » Véhicule

« Sous-champs » VER & BST

Le « sous-champ » *VER – Mesure de contrainte* a été repris de l’ancien JANUS PV. Il lui a été adjoint un nouveau « sous-champ » du même type qu’est le *BST – Confiscation, caution, rencontre*.



Ces deux « sous-champs » mentionnent des événements judiciaires particuliers relatifs à une personne. Ils ont un caractère plus informatif que réellement liant.

fig. 113 : PV2 – « Sous-champ » VER

Ce « sous-champ » contient, en plus des informations temporelles, des données spatiales. La réunion de données spatio-temporelles (deux-types différents) dans ce « sous-champ » est légitime, puisque c'est effectivement l'information qui permet de caractériser un événement. Si on voulait faire des inférences avec ces deux types de données, il faudrait soit pouvoir les décomposer et récupérer les données temporelles d'une part et les données spatiales d'autre part et les comparer avec les données de chaque type, soit tenir compte des deux simultanément à l'aide d'algorithmes spécifiques.

fig. 114 : PV2 – « Sous-champ » BST

### « Sous-champ » CPT et « attribut » Compte

Les données propres au compte bancaire ou postal se limitent à deux rubriques, le numéro et la banque de dépôt. Il est regrettable que l'IBAN<sup>306</sup> n'ait pas été explicitement mentionné, puisqu'il regroupe en un seul identifiant les notions de numéro de compte et de banque de dépôt.

Ces données sont complétées par le lien qui relie la personne en identité et le compte en ce qui concerne l'« attribut » (Rôle).

fig. 115 : PV2 – « Attribut » Compte

<sup>306</sup> IBAN (International Bank Account Number), voir chapitre 2.3.2.7

Par contre, en ce qui concerne le « sous-champ », comme il s'agit d'un lien indirect, le bénéficiaire du compte doit être indiqué, ainsi que son adresse. A nouveau, on trouve des informations de trois types différents enchâssées dans un même « sous-champ ». Le lien indirect de niveau 1, soit le numéro de compte, est une information de type *Bien (Argent)*, la seconde information (lien de niveau 2) est de type *Personne* et enfin la dernière information (lien de niveau 3) est de type *Lieu*. Il est très vraisemblable que les informations de niveau 2 et 3 ne possèdent pas de capacité de liaison lors des *comparaisons* automatiques. Cependant, elles sont facilement accessibles, puisque structurées, et vraisemblablement décomposables lors des exportations, réimportations vers des systèmes d'analyse.

fig. 116 : PV2 – « Sous-champ » CPT

### « Sous-champ » FTA

Le « sous-champ » *FTA – Transaction* était également présent dans l'ancienne version. Il était prévu pour pouvoir indiquer des transactions financières. Je ne suis pas persuadé de son utilité dans ce système<sup>307</sup>, mais il a été conservé à la demande des autorités fédérales. JANUS n'est effectivement, à mon avis, pas le système dans lequel on peut analyser des transactions financières. La mention des comptes bancaires à l'aide du « sous-champ » *CPT – compte bancaire ou postal* et de l'« attribut » correspondant suffisent à générer les liens, comme c'est le cas avec les *moyens de communication*.

fig. 117 : PV2 – « Sous-champ » FTA

### « Sous-champ » HOT

Le « sous-champ » *HOT - Hôtel* était aussi présent dans l'ancien JANUS PV et il a été repris. Il s'agit d'une information de type *Lieu* et d'un genre particulier, puisqu'il s'agit principalement d'un

<sup>307</sup> Tout comme l'analyse du détail des communications, l'analyse des transactions bancaires nécessite des outils spécialisés. Il peut être par exemple intéressant de pouvoir établir des profils d'utilisation de différents comptes bancaires en se basant sur un certain nombre d'indicateurs comme le solde moyen, la somme des mouvements mensuels, les types de mouvements et leur fréquence, etc. JANUS PV n'est pas le système approprié à ce type d'analyse.

lieu de résidence temporaire. Le groupe de travail a décidé de le conserver, car pour les criminels itinérants, les lieux de séjours peuvent être habituels et ils sont parfois utiles pour permettre leur interpellation.

fig. 118 : PV2 – « Sous-champ » HOT

### « Sous-champ » KOM et « attribut » Communication

Le « sous-champ » KOM est nouveau. Il regroupe en un seul objet les anciens « sous-champs » TEL> et ABO>. Comme pour les comptes bancaires et les véhicules, on retrouve dans ce « sous-champ » des liens enchâssés de trois niveaux et de trois types différents.

fig. 119 : PV2 – « Sous-champ » KOM

Ce « sous-champ », comme l'« attribut » d'ailleurs, contient toutefois une nouvelle complication. Seules trois rubriques (!) peuvent contenir un identifiant susceptible de créer des liens : « Moyen de communication » (au choix, un numéro de téléphone, un e-mail ou une adresse IP/URL), « IMEI » et « SIM ». J'aurais préféré plus de simplicité, soit une seule rubrique « Moyen de communication » avec une liste de choix incluant les numéros IMEI de SIM. Mais le groupe de travail en a décidé autrement. En effet, avec cette configuration, il est désormais possible, dans JANUS PV, de savoir quelle carte SIM a été utilisée avec quel appareil et sur quelle période (d'où la présence des champs « Valide du ... » « au ... »). C'est un plus, pour autant que les enquêteurs saisissent correctement cette information technique, qui est loin d'être triviale. A mon avis, cette information est d'un niveau de détail trop important pour une base de données qui sert de mémoire à long terme et qui aurait réellement sa place dans un système spécifique d'analyse des télécommunications.

fig. 120 : PV2 – « Attribut » Communication

L'« attribut » *Communication* suit exactement le modèle du « sous-champ » *KOM*. Il est composé des mêmes rubriques concernant les moyens de communications.

### « Sous-champ » OBJ

Ce « sous-champ », comme son nom l'indique, est de type *Biens (Choses)*. Il contient des informations sur la chose elle-même et un lien indirect de niveau 2 de type *Personne*. Malheureusement, il a été compliqué puisque désormais pas moins de cinq rubriques peuvent contenir l'identifiant de l'objet. Ceci risque bien de rendre ce « sous-champ » inutilisable en pratique pour des *comparaisons*.

fig. 121 : PV2 – « Sous-champ » OBJ

### « Sous-champ » ORG

Les liens avec des organisations criminelles doivent également être rapidement identifiables et recherchables. C'est pourquoi ce « sous-champ » particulier *ORG – Organisation criminelle* a été conservé en tant que tel, bien qu'il s'agisse strictement d'une information de type *Personne*.

fig. 122 : PV2 – « Sous-champ » ORG

### « Sous-champ » PAS

Le « sous-champ » *PAS – Passeport, pièce d'identité* se trouvait déjà dans l'ancien JANUS PV.

fig. 123 : PV2 – « Sous-champ » PAS

Le groupe de travail a décidé de le conserver, puisqu'il s'agit d'une information particulièrement importante sur le plan policier. Mais cette information aurait dû figurer en « attribut » plutôt qu'en « sous-champ », étant donné que les papiers d'identité saisis sont bien souvent en lien direct avec les personnes cibles.

Ce « sous-champ » contient désormais toutes les rubriques nécessaires à l'enregistrement d'un document d'identité, mais également une entité enchâssée (de type *Personne*).

### « Sous-champ » PRO

Le nouveau « sous-champ » *PRO – Profil stupéfiant* permet de générer des liens grâce aux profils chimiques des saisies de produits stupéfiants. La Confédération ne disposant pas de base de données spécifique comme c'est le cas pour les empreintes digitales ou les profils ADN, le groupe de travail a décidé d'utiliser JANUS PV 2.0 pour gérer ces liens.

fig. 124 : PV2 – « Sous-champ » PRO

Il est composé d'un code qui est fourni par le laboratoire faisant l'analyse<sup>308</sup>, ainsi que de quelques données basiques permettant son interprétation (lot mineur de revente au détail ou lot d'importance venant d'un grossiste).

### « Sous-champ » REL et « attribut » Relations

L'« attribut » *Relations* est d'un type particulier, puisqu'il ne permet pas de saisie directe. Cet onglet permet de regrouper dans une seule vue toutes les relations définies par les « sous-champs » *REL – Relation (personne)* qui se trouvent dans les antécédents d'une identité.

fig. 125 : PV2 – « Attribut » Relations

Le « sous-champ » REL est évidemment de type *Personne*. Une astuce technique permet de ne pas devoir ressaisir les informations d'une personne si elle est déjà connue du système. Le lien ainsi

<sup>308</sup> Depuis 2007, les laboratoires de l'IPS à l'Université de Lausanne ainsi que du Wissenschaftlicher Dienst (WD) de la police de la ville de Zürich sont en mesure de réaliser ce type de profilage de manière standardisée et de fournir ainsi des codes de profils à la police dans leurs rapports. Ces liens par profilage ont déjà montré par le passé qu'un stock de stupéfiants était réapparu après qu'un trafiquant eut purgé sa peine de prison et eut été libéré.

créé se répercutera automatiquement dans l'onglet *Relations* de la personne sélectionnée, ce qui évite de devoir saisir des relations croisées.

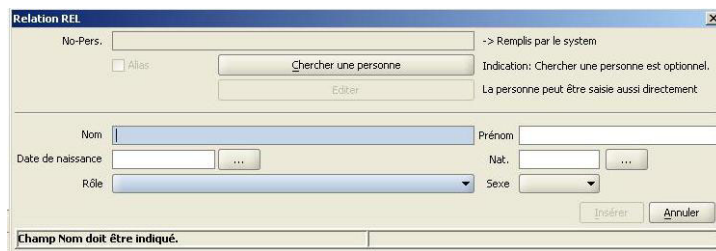


fig. 126 : PV2 – « Sous-champ » REL

### « Sous-champ » RTG

Le « sous-champ » *RTG – Routing* est un « sous-champ » à caractère purement informatif, qui n'a pas été présenté jusqu'ici, et qui a perduré de l'ancienne version. Ce « sous-champ » est utilisé pour décrire les routes empruntées principalement lors de livraisons de stupéfiants.



fig. 127 : PV2 – « Sous-champ » RTG

### « Sous-champ » SOC

Le « sous-champ » *SOC – Société* a aussi été conservé de l'ancien JANUS PV et bien qu'il contienne également des données de type *Personne*, le groupe de travail a décidé de le conserver, afin de bien différencier les relations de l'identité avec des personnes morales des relations avec des personnes physiques.

Ce « sous-champ » contient donc une rubrique unique pour le nom de la société et des informations de type *Lieu*, soit son adresse.

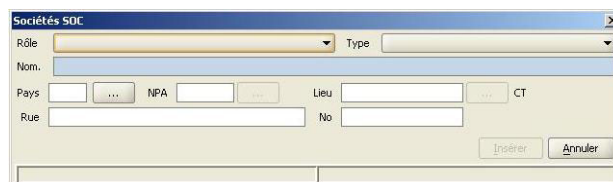


fig. 128 : PV2 – « Sous-champ » SOC

### 3.2.4 Système d'interconnexion : importation et exportation

L'ancien système JANUS PV ne disposait d'aucun moyen spécifique d'importation ou d'exportation de données, notamment en vue de leur analyse<sup>309</sup>.

#### 3.2.4.1 Importation des « sous-champs »

Dans l'ancien JANUS PV, la saisie des données par lots, telles que des listes de numéros de téléphones, était malgré tout aisée, puisque les « sous-champs » n'étaient que des chaînes de caractères pré-formatés dans le corps du texte de l'antécédent. Il suffisait que la syntaxe soit correctement préparée, par exemple dans un fichier transitoire de type MS Excel<sup>310</sup>, et la liste complète était saisie en une seule opération par un simple « copier – coller ».

Pour le groupe de travail, il était primordial que la saisie de lots d'information soit toujours possible et qu'elle reste simple. Cependant, la structuration des « sous-champs » rendait le « copier – coller » impossible. Il devenait nécessaire d'implémenter des interfaces d'importation pour les « sous-champs ».

Une interface a été réalisée et il est donc possible d'importer des données<sup>311</sup> contenues dans des fichiers d'échanges au format \*.csv (texte simple séparé par des points-virgules).

#### 3.2.4.2 Importation et exportation des données souches

Le groupe de travail ne s'est pas arrêté là. Il a également décidé qu'il devait être également possible d'importer et d'exporter les fiches personnes, leurs antécédents et les objets de JANUS PV 2.0 en tant que tels.

Cette décision a été prise en espérant, d'une part, pouvoir coupler JANUS PV 2.0 aux bases de données des polices cantonales via des interfaces particulières, et d'autre part, pouvoir importer et exporter facilement des données en vue de leur traitement dans des systèmes d'analyse externes.

A cet effet, le CSI-DFJP a choisi le format d'échange XML (*eXtensible Markup Language*). Le format XML, qui est de plus en plus répandu, est un métalangage, puisqu'il contient les données elles-mêmes, mais également la structure de ces données.

Ainsi, le CSI-DFJP a édité des schémas XML qui seront utilisés de manière standard pour le stockage de certaines données dans les différents systèmes et pour l'importation et l'exportation des

---

<sup>309</sup> Tout au plus, était-il possible d'extraire des données en les imprimant dans un fichier de type texte, de le récupérer et de le retravailler ensuite.

<sup>310</sup> De 2002 à 2005, un fichier MS Excel de pré-formatage des données appelé *Communiqué JANUS PV* était utilisé au sein de la police de sûreté vaudoise.

<sup>311</sup> A fin 2008, seules les données téléphoniques (« sous-champ » KOM) peuvent être importées.

données. Cette phase de liaison avec d'autres systèmes devait être opérationnelle dans le courant de 2006, soit environ un an après la mise en service de la nouvelle version de JANUS PV.

L'exemple suivant reproduit le modèle XML du fichier d'échange de données de type *Moyen de communication*.

```

<meansOfCommunication>
<telephone keepUnderSurveillance="1" usage="1" subscriber="1" preferred="1" type="1">
  <phoneNumberInternational>+41211234567</phoneNumberInternational>
</telephone>
<mobile keepUnderSurveillance="1" usage="1" subscriber="1" smsEnabled="1" preferred="1" type="1">
  <phoneNumberSwiss>0791234567</phoneNumberSwiss>
  <simNumber>123456789012345678</simNumber>
  <imeiNumber>123456789012345</imeiNumber>
</mobile>
<eMail keepUnderSurveillance="1" usage="1" subscriber="1" preferred="1" type="2">
  <eMailAddress>toto.lehero@abc.ch</eMailAddress>
</eMail>
<uri keepUnderSurveillance="1" usage="1" subscriber="1" preferred="1" type="1">
  <uri>www.abc.ch</uri>
</uri>
</meansOfCommunication>

```

fig. 129 : PV2 – Exemple de fichier d'échange XML

### 3.2.5 Synthèse

Depuis sa mise en service en août 2005, le nouveau sous-système JANUS PV 2.0 a obtenu l'approbation des utilisateurs qui ont subi la mise à jour sans heurts. L'ergonomie du système est donc bonne et l'esprit de l'ancienne version a pu être conservé, malgré une mue visuelle très importante. L'utilisateur retrouve très rapidement ses marques. Une demi-journée de formation est désormais suffisante pour atteindre un niveau de connaissance du système qui permette de faire des recherches et des saisies simples, alors qu'avec l'ancien système, deux journées complètes étaient nécessaires. On peut donc en conclure que la nouvelle version est beaucoup plus ergonomique et conviviale que la précédente.

Les problèmes principaux de structure et d'organisation des données qui empêchaient toutes velléités d'analyse ont pu être corrigés en grande partie. Le modèle adopté pour le « sous-système » JANUS PV correspond désormais d'assez près au modèle générique et universel qui a été défini au chapitre 3.1. Seul subsiste l'enchâssement d'entités de types différents à l'intérieur d'un même « sous-champ ». Il sera nécessaire d'évaluer la possibilité de restructurer ces données depuis les fichiers d'échanges lors de l'importation dans le composant d'analyse, qui va être décrit au chapitre 3.3.



### 3.3 Prototype $\beta$ (base de données d'analyse)

Le prototype qui est présenté dans ce chapitre est directement issu du modèle décrit dans l'étude méthodologique préliminaire et de JANUS PV 2.0 présenté aux chapitres précédents.

Une base de données d'analyse se doit de faire état d'une structuration précise des données, tout en laissant la liberté à l'analyste de représenter des situations toujours différentes. Il s'agit de faire preuve de rigueur dans la créativité, en restant compatible avec les principales sources de données.

#### 3.3.1 Introduction

Ce prototype  $\beta$  doit servir de base de données d'analyse durant l'enquête. Il s'agit d'un composant de mémoire à court terme<sup>312</sup>, qui ne vise pas les mêmes buts que JANUS PV 2.0, qui est la mémoire à long terme<sup>313</sup>.

Le composant d'analyse doit partir de zéro dans chaque enquête. Il sera alors alimenté d'informations issues de JANUS PV, mais aussi des autres sources d'informations à disposition de l'enquêteur<sup>314</sup>. Au cours des investigations, certaines informations contenues dans cette base d'analyse devront être injectées à leur tour dans des composants de mémoire à long terme. Il en sera de même en fin de processus. Au terme de l'enquête policière, cette base d'analyse sera effacée ou jointe au dossier pénal, suivant les procédures en vigueur, et elle ne devra en aucun cas servir d'archive d'informations pénales.

En Suisse, depuis la fin des années 1990, de telles bases de données d'analyse ont évidemment déjà été utilisées dans le cadre d'affaires pénales. Plusieurs entités ont contribué à standardiser leurs méthodes de travail et à proposer des standards pour l'utilisation de bases de données d'analyse. On peut mentionner, outre le fabricant du logiciel (*i2 Ltd*), qui propose un certain nombre de modèles en exemple, le groupe d'analyse criminelle de la PJF, ainsi que de la police de sûreté vaudoise. Ces deux dernières entités ont par ailleurs profité de leur collaboration dans le cadre de la sécurité militaire pour aboutir à un standard commun en 2004. Ce standard commun (appelé *generic 2004*) a subi depuis lors, tant à la PJF qu'à la sûreté vaudoise, des ajustements en fonction de besoins particuliers. Des affaires complexes ont été traitées dans ces deux entités à l'aide de ce modèle de base.

Cependant, une version entièrement compatible et standardisée ne peut être adoptée par l'ensemble des partenaires que si elle présente un avantage déterminant sur les solutions déjà présentes. Le prototype  $\beta$  décrit ci-après se veut une évolution de la base *generic 2004*, afin de la rendre

---

<sup>312</sup> Par court terme, on entend que les informations détaillées ne serviront que pour la durée d'une enquête ou d'une analyse « ponctuelle » en fonction d'une situation particulière.

<sup>313</sup> Voir chapitre 2.5 – Le projet

<sup>314</sup> Voir chapitre 1.2 – L'enquête

compatible avec le nouveau JANUS PV 2.0. Ainsi, cette nouvelle fonctionnalité devait lui permettre de devenir le nouveau standard au niveau suisse.

Comme nous l'avons mentionné dans la description du projet, les logiciels utilisés font partie de l'arsenal standard des unités d'analyse criminelle en Suisse et ailleurs, soit *iBase*<sup>TM</sup> pour la gestion des données et l'*Analyst's Notebook*<sup>TM</sup> pour leur visualisation. Le prototype  $\beta$  a été réalisé à l'aide de la version de *iBase*<sup>TM</sup> 4.0.11 SR2 de *i2 Ltd*.

### 3.3.2 Structure et organisation

Pour la base de données d'analyse, la structure est définie par un certain nombre d'entités reprenant les entités principales. Son organisation sera déterminée par des liens structurés en fonction des entités présentes.

#### 3.3.2.1 Structure

Par rapport aux éléments de l'étude méthodologique et de la base générique, une nouvelle entité fait son apparition, dans le souci de rendre compatibles les composants de mémoire à long et à court terme. Il s'agit de l'entité « Antécédent ». Ainsi, la base d'analyse prototype  $\beta$  comporte 9 entités :



fig. 130 : Entités du prototype  $\beta$

#### Entité Antécédent

Cette nouvelle entité *Antécédent* reprend donc l'ensemble des informations contenues dans JANUS PV 2.0. Il s'agit d'une vingtaine d'informations administratives comme la date de l'antécédent, sa source, sa qualification, ses diverses références cantonales et/ou fédérales, et puis spécifiquement son contenu sous forme de texte<sup>315</sup>.

L'élément identifiant est le code de l'antécédent (Id JANUS) repris de JANUS PV 2.0.

<sup>315</sup> Voir fig. 106 – Masque personne-antécédent(s) de JANUS PV 2.0

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Antécédent	Icon							Icone de l'antécédent
Id JANUS	Text	20	Yes	Yes	Yes		Upper Case	Record id de JANUS PV 2.0
Date Doc	Date			Yes			Long Date	Date de l'antécédent
Dossier	Yes/No							Dossier de police
Fiable	Yes/No							Antécédent fiable?
Domaine	Suggested from Code List			Yes				Domaine de criminalité
Lien CO	Yes/No							Lien avec le crime organisé?
Procédure	Suggested from Code List							Type de procédure
Transmission	Yes/No							Transmission de l'antécédent autorisée?
Resp. de l'enquête	Suggested from Code List							Responsable de l'enquête
Groupe d'auteurs	Suggested from Code List							Provenance des groupes d'auteurs
Attribution géographique	Suggested from Code List							Attribution géographique de l'activité délictueuse
Source PV	Text	50						Source de l'antécédent PV
N° d'affaire	Text	50						Référence de l'affaire
Opération	Text	50						Nom de l'opération
PJF_dossier_1	Text	50						Référence PJF 1
PJF_dossier_2	Text	50						Référence PJF 2
PJF_N°_Réf	Text	50						Référence PJF numéro
PJF_N°_procédure	Text	50						Référence PJF numéro procédure
PJF_Projet	Text	50						Référence PJF Projet
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Texte	Multi-Line Text							Texte de l'antécédent

fig. 131 : Détail de l'entité Antécédent du prototype  $\beta$ 

Toutes les entités comportent deux champs particuliers qui sont la *Source* [obligatoire] et la *Qualification (4x4)* [facultative] de l'information. Ces deux champs sont nécessaires à l'activité d'analyse (indexation et évaluation des informations).

### Entité Argent (biens)

L'entité *Argent (biens)* est beaucoup plus simple. Il s'agit d'une entité liante. Le *numéro de référence* est le champ obligatoire (*Mandatory*) qui sert d'identifiant (*Discriminator*).

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Argent (biens)	Icon			Yes				
Rôle	Suggested from Code List							Rôle de l'argent (biens)
Numéro de référence	Text	20	Yes	Yes	Yes		Upper Case	Identifiant du bien pécuniaire
Nom de la banque	Multi-Line Text							Adresse de l'organe émetteur
Renseignements divers	Multi-Line Text (Append Only)							Renseignements ne pouvant figurer ailleurs dans la base de données
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 132 : Détail de l'entité Argent (biens) du prototype  $\beta$ 

L'information est complétée par un champ décrivant l'organe bancaire ou financier émetteur et enfin un champ pour les renseignements divers.

### Entité Choses (biens)

Par analogie avec l'entité décrite ci-avant, l'entité *Choses (biens)* est relativement simple. Afin d'être compatible avec les objets de JANUS PV 2.0, des champs *Gravure*, *Marque/quoi* et *Description* permettent de décrire la chose dans le détail.

Le *numéro de référence* qui sera l'identifiant est, à nouveau, obligatoire. Ces entités ont pour but de créer des liens. Elles ne doivent pas être uniquement utilisées pour décrire une situation trop en détail, utilisant l'iconographie de manière purement cosmétique.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Choses (biens)	Icon			Yes				Liste des icônes pour représenter graphiquement un Bien (chose)
Type	Suggested from Code List							Types d'objets
Numéro de référence	Text	30	Yes	Yes	Yes		Upper Case	Identifiant du bien mobilier
Gravure	Text	50						Gravure
Marque / quoi	Text	30		Yes				Description sommaire de la chose
Description	Multi-Line Text							Description détaillée de la chose
Renseignements divers	Multi-Line Text							Renseignements ne pouvant pas figurer ailleurs dans la base de données
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 133 : Détail de l'entité Choses (biens) du prototype  $\beta$ 

## Entité Communication

Cette entité est sans conteste la plus compliquée et la moins bien définie. La faute en revient à la structure de l'objet *Moyen de communication*<sup>316</sup> dans JANUS PV 2.0. Afin de ne pas perdre d'informations, il a été nécessaire de reprendre sa structure, bien qu'elle contienne plusieurs éléments liants dans différentes rubriques (numéro d'appel ou adresse, numéro IMEI et numéro SIM).

Cette structure impose qu'un seul de ces trois éléments soit l'identifiant de l'entité. Le plus important et le plus courant est sans conteste le *Numéro /Adresse*, qui servira donc d'identifiant. Les deux autres serviront d'informations complémentaires. Ils ne pourront en aucun cas être directement utilisés pour faire des représentations du type SIM – IMEI<sup>317</sup>, permettant une analyse fine de l'utilisation des moyens de communication mobiles. Ce type d'analyse technique devra rester en dehors du processus global d'analyse d'enquête que ce prototype permet. Il restera l'apanage d'outils spécifiques, tel le *CTAnalyser*<sup>318</sup>.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Communication	Icon			Yes				Liste des icônes pour représenter graphiquement un Moyen de communication
Moyen de communication	Suggested from Code List			Yes				Description du moyen de communication
Numéro / Adresse	Text	30	Yes	Yes	Yes		Upper Case	Numéro d'appel ou adresse électronique
Fournisseur	Suggested from Code List							Prestataire de service
Sur écoute	Yes/No							Raccordement sous écoute ?
Type	Selected from Code List			Yes				Type de moyen de communication
IMEI	Text	25					Upper Case	Code IMEI
SIM	Text	25					Upper Case	Code IMSI
Rôle	Suggested from Code List							Rôle pour les moyens de communications
valable du	Date						Medium Date	Date de validité du moyen de communication (début)
au	Date						Medium Date	Date de validité du moyen de communication (fin)
Renseignements divers	Multi-Line Text (Append Only)							Renseignements ne pouvant pas figurer ailleurs dans la base de données
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 134 : Détail de l'entité Communication du prototype  $\beta$ 

Le niveau de détail pour cette entité est très important. Il va de soi qu'il n'est pas nécessaire de chercher à remplir toutes les rubriques. Seuls trois champs spécifiques sont obligatoires : la description du moyen de communication (numéro de téléphone, adresse mail, ou adresse IP/URL), le numéro ou l'adresse en question, et le type (analogique, mobile, ISDN, ...).

<sup>316</sup> Voir fig. 119 : PV2 – Sous-champ KOM et fig. 120 : PV2 – Attribut Communication

<sup>317</sup> Voir fig. 52 : Exemple réel d'échange de cartes SIM dans les téléphones GSM

<sup>318</sup> Voir chapitre 1.4.6.2 – Les analyses de contrôles techniques

## Entité Événement

L'entité *Événement* n'est pas directement liée à un objet de JANUS PV 2.0. Ce type d'entité se retrouve dans le système de la Confédération, sous la forme des antécédents qui constituent une entité à part entière, ou sous la forme des « sous-champs » VER et BST<sup>319</sup>, qui sont des mesures de contrainte.

Or, dans la résolution d'enquêtes judiciaires, de très nombreux événements utiles ne doivent pas figurer dans un système de mémoire à long terme, bien qu'ils doivent être analysés durant les investigations. Il s'agit principalement de rencontres, de rendez-vous, d'infractions résolues ou non, etc.

L'identification d'un événement se base sur la date, le type et le lieu.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Événement	Icon			Yes				Liste des icônes pour représenter graphiquement un Événement
Date	Date		Yes	Yes	Yes		Short Date	Date de l'événement
Heure	Time						Short Time	Heure de l'événement
Type	Suggested from Code List		Yes	Yes	Yes			Type d'événement
Lieu	Text	50	Yes		Yes			Description sommaire du Lieu de l'événement
Motif	Text	50						Motif de la mesure de contrainte
Détail	Multi-Line Text							Détail de l'événement, pour autant que ça ne puisse figurer ailleurs dans la base
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 135 : Détail de l'entité Événement du prototype β

## Entité Forensique (traces)

Comme l'entité *Événement*, l'entité *Forensique* ne découle pas directement de JANUS 2.0, bien que l'on retrouve un élément de ce type (le « sous-champ » PRO<sup>320</sup>). Pour ce dernier, une codification particulière a été mise en place afin de répondre aux besoins de JANUS. Ce code servira d'identifiant à l'élément de preuve matérielle. D'autres traces, comme par exemple le profil génétique ou les empreintes digitales, peuvent aussi entrer en ligne de compte dans la base d'analyse. Il faudra alors reprendre les codes des bases AFIS et ADN comme élément identifiant.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Forensic	Icon			Yes				Liste des icônes pour représenter graphiquement une trace
Type de trace	Suggested from Code List			Yes				Identifiant de la preuve (code ADN ou ED, ...)
Code	Text	20	Yes	Yes	Yes		Upper Case	Code de la trace selon JANUS, AFIS ou ADN
Description	Multi-Line Text							Description de la trace
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 136 : Détail de l'entité Forensique du prototype β

## Entité Lieu

Cette entité est devenue très détaillée avec JANUS PV 2.0. Il a encore fallu s'adapter au niveau de détail présent dans la base de la Confédération.

<sup>319</sup> Voir fig. 113 : PV2 – Sous-champ VER et fig. 114 : PV2 – Sous-champ BST

<sup>320</sup> Voir fig. 124 : PV2 – sous-champ PRO

La composante géographique dans la création et la gestion de liens est, comme nous l'avons déjà dit, une problématique particulière. C'est pourquoi, dans un premier temps, aucun élément liant ne sera prédéfini. Les données de lieu seront uniquement informatives. Le niveau d'inférence pourra être défini de cas en cas, ou alors selon une analyse interne (recherche ciblée automatique ou manuelle) ou externe par l'intermédiaire de systèmes d'information géographiques (SIG), comme *MapInfo™*, *ArcView™* ou encore *MapPoint™*.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Lieu	Icon			Yes				Liste des icônes pour représenter graphiquement un lieu
Type d'adresse	Suggested from Code List							Type d'adresse
Valable du	Date						Short Date	Date de validité de l'adresse (début)
au	Date						Short Date	Date de validité de l'adresse (fin)
Code pays	Suggested from Code List							Code des pays (norme ISO)
Pays	Suggested from Code List							Pays de résidence
NPA	Text	20						Numéro postal
Lieu	Text	30		Yes			Upper Case	Localité de résidence
Canton	Suggested from Code List							Canton de résidence
Rue	Text	50						Rue ou description de lieu
Numéro	Text	10						Numéro de la rue
c/o	Text	50						Chez
Renseignements divers	Multi-Line Text (Append Only)							Renseignements ne pouvant figurer ailleurs dans la base de données
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 137 : Détail de l'entité Lieu du prototype β

### Entité Personne / Société

L'entité *Personne / Société* doit de reprendre les informations disponibles dans JANUS PV 2.0 qui en fait son élément principal.

La nouvelle version de JANUS a vu l'apparition d'un nombre important de nouveaux champs, détaillant notamment les origines géographiques et biologiques de la personne.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Personne / Société	Icon			Yes				Liste des icônes utilisés pour représenter graphiquement une personne
Id JANUS	Text	20	Yes		Yes		Upper Case	Record id de JANUS PV 2.0
NOM	Text	50	Yes	Yes	Yes		Upper Case	Nom de la personne physique ou morale. Pour les inconnus, on mentionnera "INCONNU"
Prénom	Text	50	Yes	Yes	Yes		Upper First	Prénom de la pers. physique ou l'activité pour les pers. morales. Pour les inconnus: le surnom
Nom de naissance	Text	50	Yes				Upper Case	Nom de naissance de la pers. physique. Pour les pers. morales, on ne mentionnera rien
Date de naissance	Date		Yes		Yes		Short Date	Date de naissance de la personne physique
Pays de naissance	Suggested from Code List							Pays de naissance de la personne physique
Lieu de naissance	Text	50					Upper First	Lieu de naissance de la personne physique
Nationalité	Suggested from Code List							Nationalité de la personne physique
Lieu d'origine	Text	50					Upper First	Lieu d'origine de la personne physique
Sexe	Selected from Code List							Sexe de la pers. physique. Pour les pers. morales: "vide" et "I" pour les inconnus
Etat civil	Suggested from Code List							Etat civil des personnes physiques
NOM du père	Text	50					Upper Case	NOM du père de la personne physique
Prénom du père	Text	50					Upper First	Prénom du père de la personne physique
NOM de la mère	Text	50					Upper Case	NOM de la mère de la personne physique
Prénom de la mère	Text	50					Upper First	Prénom de la mère de la personne physique
NOM du conjoint	Text	50	Yes				Upper Case	NOM du conjoint de la personne physique
Prénom du conjoint	Text	50					Upper First	Prénom du conjoint de la personne physique
Moyen de contrôle	Suggested from Code List							Moyens de contrôle des données personnelles
Source du contrôle	Suggested from Code List							Source du contrôle des données personnelles
Dactyloscopié	Yes/No							Est-ce-que la personne physique a été dactyloscopiée?
Photo disponible	Yes/No							Est-ce-qu'une photo est disponible?
ADN	Yes/No							Est-ce-que le profil ADN de la personne a été pris?
Remarques	Multi-Line Text (Append Only)							Renseignements divers sur la personne ne pouvant figurer ailleurs dans la base de données
Surnom	Multi-Line Text (Append Only)						Upper First	Surnom(s) de la personne
Photo	Picture							Photo
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 138 : Détail de l'entité Personne / Société du prototype β

Afin de rendre l'identification des personnes aussi sûre et précise que possible, les identifiants de cette entité centrale sont au nombre de quatre. Outre les traditionnels NOM(s), prénom(s) et date de



naissance, un champ supplémentaire a été ajouté. Il s'agit du code de l'identité JANUS PV 2.0. L'ajout de ce champ dans l'identifiant a un avantage supplémentaire. Il permet de détecter immédiatement si la personne est enregistrée dans la base de données JANUS. Par contre, ce champ ne doit pas être obligatoire. En effet, dans la mémoire à court terme de l'enquête, de nombreuses personnes vont apparaître, bien qu'elles ne remplissant pas les critères légaux pour figurer dans JANUS.

Il sera également possible d'inclure une photo de la personne dans la base d'analyse. Cette photo sera immédiatement affichée dans les différents schémas de visualisation, qu'ils soient relationnels ou chronologiques.

La plupart des champs de cette entité correspondent aux attributs des personnes physiques. L'intitulé des rubriques correspond aux données qui doivent y être saisies. En ce qui concerne les personnes morales, on peut se restreindre aux seuls *NOM* et *Prénom*. Par convention, on utilisera le champ *NOM* pour inscrire le nom de la société ou de l'organisation et le champ *Prénom* pour le domaine d'activité de la dite société. Pour les inconnus, on pratiquera également de manière standardisée en indiquant la mention « INCONNU » dans le champ *NOM* et dans le champ *Prénom*, son surnom s'il existe, ou en dernier lieu, un nom d'enquête.

### Entité Transport

Enfin, l'entité *Transport* constitue la dernière entité de la base d'analyse prototype. Il s'agit toujours de veiller à la compatibilité avec la base fédérale.

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Icone Transport	Icon			Yes				Liste des icônes pour représenter graphiquement un moyen de transport
Genre vhc	Suggested from Code List							Type de moyen de transport
Pays	Suggested from Code List							Pays de l'immatriculation
Canton	Suggested from Code List							Canton de l'immatriculation
N° de plaque	Text	20	Yes	Yes	Yes		Upper Case	Numéro d'immatriculation du moyen de transport
Marque / fabricant	Suggested from Code List		Yes					Marque du véhicule ou fabricant du moyen de transport
Modèle	Text	20						Modèle du moyen de transport
Couleur	Suggested from Code List							
VIN	Text	50					Upper Case	Numéro de châssis du véhicule
N° matricule	Text	20					Upper Case	Numéro de matricule du véhicule
Renseignements divers	Multi-Line Text							Renseignements ne pouvant figurer ailleurs dans la base de données
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 139 : Détail de l'entité Transport du prototype  $\beta$

L'élément identifiant pour cette entité est le *numéro de plaque*, le reste des champs permettant de décrire en détail le moyen de transport.

### Iconographie

Pour chacune des neuf entités présentées ci-dessus, un champ particulier n'a pas encore été abordé. Il s'agit du champ appelé « Icône ... », qui est représenté en tête de liste (grisé) aux figures 128 à 136. Ce champ permet de choisir l'icône de chaque entité. L'iconographie actuelle est tellement

détaillée, plusieurs centaines d'icônes étant à disposition toutes catégories confondues, que la description exhaustive se trouve en annexe<sup>321</sup>.

Voici néanmoins un exemple des quelques 18 icônes disponibles pour l'entité *Communication*.

















Cellphone		CD-ROM	
Envelope		E-mail	
Fax Machine		Fax	
Pager		Letter	
Payphone		Parcel	
PDA		PC	
Phone Box		SIM Card	
Telephone		WWW	

fig. 140 : Icônes de l'entité *Communication* (exemple)

En regard des images, on trouve leur dénomination anglaise qu'il est nécessaire d'utiliser dans *iBase*<sup>TM</sup> pour que le dessin correct s'affiche<sup>322</sup>.

### 3.3.2.2 Organisation

L'organisation des données contenues dans le prototype  $\beta$  est d'une importance particulière. Si le choix des entités semble relativement simple et paraît être à la portée de tout un chacun se fiant à son bon sens, leur organisation en fonction de moyens d'inférence prédéfinis l'est beaucoup moins. En effet, pour pouvoir pratiquer des analyses de qualité de manière automatique ou guidée, il est nécessaire d'avoir au préalable organisé les données afin qu'elles permettent de répondre aux questions qu'il est légitime de se poser dans la situation que nous cherchons à apprécier.

Un des facteurs déterminants est une organisation aussi stricte que possible, sans toutefois être totalement rigide. Une rigueur totale doit être tenue dans la saisie des connexions de même type, sous peine d'obtenir des résultats d'analyse totalement erronés.

<sup>321</sup> Cf. Annexe II : Liste des icônes du prototype  $\beta$

<sup>322</sup> Il aurait été possible d'utiliser des noms en français, une table de conversion permettant de paramétrer les éléments utilisés lors de la saisie des données. Cependant, toute francisation nécessite une traduction en allemand et/ou en italien, si une distribution au niveau suisse du prototype est envisagée par la suite. Cette option n'a donc pas été retenue.



C'est ainsi que 18 liens ont été prédéfinis dans le prototype  $\beta$ , dont 17 sont des inférences analysables et dont la dernière amène la souplesse nécessaire à certaines situations, mais dont l'analyse n'est, par contre, plus possible (*Lien générique*).

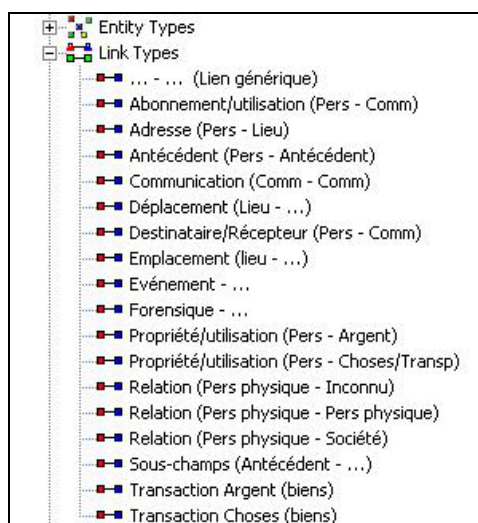


fig. 141 : Liens du prototype  $\beta$

Les liens peuvent être regroupés en différentes catégories. Par exemple, trois types de relations directes entre les personnes ont été définis. On trouve les liens entre deux personnes physiques, les relations entre une personne physique et une personne morale ou encore les relations entre une personne physique et une personne inconnue.

Les relations en rapport avec les biens, de type *Argent* ou *Choses* sont différenciées : d'une part la propriété ou l'utilisation, et d'autre part les transactions.

Il en est de même avec les moyens de communication. Un lien d'abonnement ou d'utilisation, et un lien de destination, sont définis entre les personnes et les moyens de communication. Puis, plus spécifiquement, la communication, qui est un lien entre deux moyens de communication est réservée à un usage encore plus précis.

Les liens concernant les lieux sont au nombre de trois : les adresses (lieux liés à des personnes), les emplacements et les déplacements.

Les événements et les traces forensiques peuvent être liés à tout autre type d'entité.

Restent les liens spécifiques à la structure de JANUS PV 2.0, soit le lien d'antécédent entre une personne et son antécédent et le lien de « sous-champ » réservé aux objets apparaissant dans l'antécédent (lien indirect de niveau  $> 1$ ).

Voici le détail des liens définis dans le prototype  $\beta$ . Outre la qualification par le système 4x4, la source de l'inférence et la légende du lien, on trouve parfois des informations temporelles ou contextuelles utiles à la compréhension d'une représentation.

... - ... (Lien générique)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Text	20		Yes				Légende du lien
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Abonnement/utilisation (Pers - Comm)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Suggested from Code List			Yes				Légende du lien
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Adresse (Pers - Lieu)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Suggested from Code List			Yes				Type d'adresse
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Antécédent (Pers - Antécédent)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Domaine	Suggested from Code List							Domaine de l'antécédent
Date	Date						Short Date	Date de l'antécédent
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Communication (Comm - Comm)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Selected from Code List			Yes				Type de la communication
Date	Date						Short Date	Date de la communication
Heure	Time						Short Time	Heure de la communication
Contenu	Multi-Line Text							Contenu de la communication
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Déplacement (Lieu - ...)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Suggested from Code List			Yes				Type de déplacement
Date départ	Date						Short Date	Date de départ
Date de retour	Date						Short Date	date du retour
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Destinataire/Récepteur (Pers - Comm)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Date d'envoi/réception	Date			Yes			Short Date	Date de l'envoi ou de la réception
Heure d'envoi/réception	Time						Short Time	Heure de l'envoi ou de la réception
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Emplacement (lieu - ...)								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Suggested from Code List			Yes				Type de localisation
Date	Date						Short Date	Date de la localisation
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations
Événement - ...								
Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
Légende	Suggested from Code List			Yes				Type de lien événement
Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
Source	Suggested from Code List			Yes				Source des informations

fig. 142 : Détail des liens du prototype  $\beta$  (part. 1)

L'utilisation de la chromographie standardisée permet un échange plus aisé des représentations graphiques. C'est pourquoi les couleurs standards du guide d'analyse criminelle suisse<sup>323</sup> ont été reprises.

<sup>323</sup> HOSTETTLER P. *et al.*, Brochure d'analyse opérationnelle, 2000

Field Name	Field Type	Field Size	Indexed	Mandatory	Discriminator	Attribute	Format	Description
<b>Forensique - ...</b>								
1144 Légende	Text	20		Yes				Légende du lien
1145 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
1146 Source	Suggested from Code List			Yes				Source des informations
<b>Propriété/utilisation (Pers - Argent)</b>								
1144 Légende	Suggested from Code List			Yes				Type de propriété / utilisation d'argent
1145 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
1146 Source	Suggested from Code List			Yes				Source des informations
<b>Propriété/utilisation (Pers - Choses/Transp)</b>								
1144 Légende	Suggested from Code List			Yes				Type de propriété/utilisation de choses
1145 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
1146 Source	Suggested from Code List			Yes				Source des informations
<b>Relation (Pers physique - Inconnu)</b>								
1144 Légende	Suggested from Code List			Yes				Type de lien entre une personne et un inconnu
1145 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
1146 Source	Suggested from Code List			Yes				Source des informations
<b>Relation (Pers physique - Pers physique)</b>								
1144 Légende	Suggested from Code List			Yes				Type de liens entre personnes physiques
1145 Source	Suggested from Code List			Yes				Source des informations
1146 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
<b>Relation (Pers physique - Société)</b>								
1144 Légende	Suggested from Code List			Yes				Type de liens entre des personnes physiques et morales
1145 Description	Text	50						Description de l'activité
1146 Source	Suggested from Code List			Yes				Source des informations
1147 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
<b>Sous-champs (Antécédent - ...)</b>								
1144 Légende	Suggested from Code List							Liste des codes de sous-champs
1145 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
1146 Source	Suggested from Code List			Yes				Source des informations
<b>Transaction Argent (biens)</b>								
1144 Légende	Suggested from Code List			Yes				Type de lien pour une transaction d'argent
1145 Montant	Real Number							Montant de la transaction
1146 Monnaie	Selected from Code List							Devises
1147 Date	Date					Short Date		Date de la transaction
1148 Heure	Time					Short Time		Heure de la transaction
1149 Source	Suggested from Code List			Yes				Source des informations
1150 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4
<b>Transaction Choses (biens)</b>								
1144 Légende	Suggested from Code List			Yes				Type de transaction de choses
1145 Date	Date					Short Date		Date de la transaction
1146 Heure	Time					Short Time		Heure de la transaction
1147 Source	Suggested from Code List			Yes				Source des informations
1148 Qualification (4x4)	Selected from Code List							Qualification de l'information suivant le système 4x4

fig. 143 : Détail des liens du prototype β (part. 2)

L'utilisation des liens prédéfinis est contrôlée par le logiciel *iBase*<sup>TM</sup>, qui vérifie que les entités liées soient du bon type. Comme le montre la figure suivante, lors de la conception de la base, il est possible de définir, par exemple, que le lien Pers – Antécédent ne peut être utilisé que pour relier ces types d'entités.

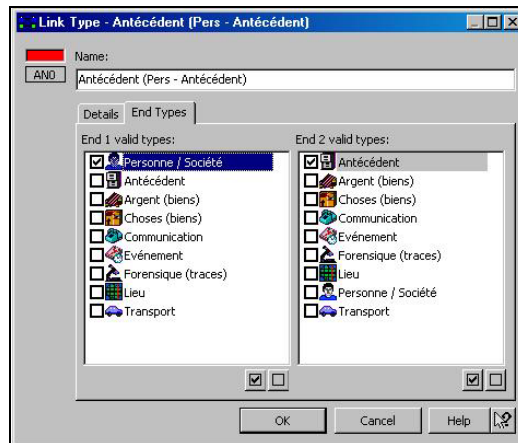


fig. 144 : Contrôle du type d'entité dans les liens dans iBase™

Ce contrôle est très utile, car il permet ensuite d'utiliser les inférences (liens) dans la création de recherches ciblées ou visuelles (*Query*) que permet le logiciel d'analyse, que ce soit dans la base de données ou dans les représentations graphiques.

Ainsi, il est possible de rechercher très simplement et de manière très conviviale une personne qui réside en France et qui a plus de trois antécédents JANUS PV à son actif :

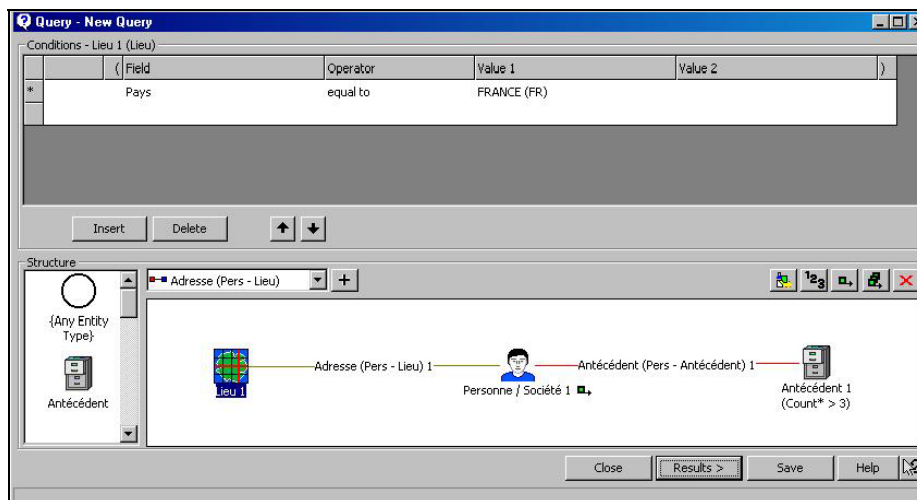


fig. 145 : Recherches visuelles dans iBase™ (*Query*)

Le résultat que nous retournera le système sera une liste des entités *Personne / Société* qui doit répondre à ces critères indépendants.

Il est possible de réaliser exactement le même type de recherches dans les schémas de visualisation relationnels ou chronologiques.

### 3.3.3 Valeurs standardisées : selon le standard ISO de JANUS PV 2.0

Outre la structure et l'organisation des données, un troisième paramètre influence grandement le potentiel d'analyse des données : la saisie. Ceci pour plusieurs raisons :

1. Les données doivent être présentes, donc saisies (influence du système global) ;
2. Les données doivent être saisies au bon endroit (influence de la structure) ;
3. Les données doivent être en relation avec les autres de manière correcte (influence de l'organisation) ;
4. Les données doivent être saisies avec rigueur (influence des données standardisées).

C'est justement pour influencer ce dernier point que des standards ont repris, autant que possible, des normes existantes lors de la création de JANUS PV 2.0.

Actuellement, un effort particulier est apporté en Suisse à la standardisation des données. Le projet de mise en commun des données cantonales et fédérales au sein de l'index suisse de police<sup>324</sup> a montré que le fédéralisme aggravait effroyablement la situation dans le domaine de la standardisation des données au sein des différents corps de police.

De plus, la mise à disposition par la Suisse de certaines données aux autres Etats de l'Union Européenne suite aux « *Bilatérales bis* » (Accords de Schengen/Dublin), a précipité la standardisation à un niveau supranational. C'est pourquoi pour les listes de codes, les normes ISO ont maintenant été choisies pour la réalisation des nouveaux systèmes d'information.

L'intégration des données standardisées se fait généralement par l'usage de liste de choix sous forme de menu déroulant lors de la saisie. Ces choix peuvent être suggérés (une autre donnée que celles présentes dans la liste pouvant être saisie) ou obligatoires (seul un élément de la liste peut être sélectionné).

Dans le prototype  $\beta$ , à de rares exceptions près, les choix sont suggérés. Alors que dans JANUS PV 2.0, ces choix sont habituellement obligatoires.

C'est ainsi que plus de 50 listes de saisie standardisées ont été adoptées dans JANUS PV 2.0. Et tout ceci en trois langues : allemand, français et italien.

La plupart de ces listes ont été intégrées au prototype  $\beta$ , afin d'assurer la compatibilité montante des informations (importation des données du prototype dans JANUS PV 2.0).

C'est ainsi qu'une quarantaine de listes de choix ont été définies, plus neuf pour les listes d'icônes à disposition.

---

<sup>324</sup> Voir chapitre 2.5.1.1

Pick Lists		
Pick List	No of Items	Description
↓ \$ _Lien Abonné	2	Type d'abonnement/utilisation de communications
↓ \$ _Lien Adresse	20	Type de lien entre une personne et un lieu (adresse privée ou prof)
↓ \$ _Lien Communication	5	Type de communication
↓ \$ _Lien Déplacement	3	Type de déplacement
↓ \$ _Lien Destinataire/Récepteur	4	Type de lien entre une personne et un moyen de communication
↓ \$ _Lien Emplacement	2	Type d'emplacement
↓ \$ _Lien Événement	11	Type d'événement
↓ \$ _Lien Personne - Inconnu	4	Types de lien Personne - Inconnu
↓ \$ _Lien Personne - Personne	8	Type de lien entre des personnes physiques
↓ \$ _Lien Personne - Société	7	Type de liens entre une personne physique et une personne morale
↓ \$ _Lien propriété/utilisation	14	Type de propriété ou d'utilisation
↓ \$ _Lien Sous-champs	15	Types de sous-champs
↓ \$ _Lien transaction (Argent)	7	Type de transaction de biens (Argent)
↓ \$ _Lien transaction (Choses)	6	Type de transaction de choses
↓ 4x4	16	Matrice 4x4
↓ Cantons	29	Liste des cantons suisses
↓ Code pays	240	Code pays ISO
↓ Couleurs	10	Liste des couleurs courantes de véhicules
↓ Domaine	13	Domaine de criminalité
↓ Etat civil	7	Etat civil des personnes physiques
↓ Événement	18	Type d'événement
↓ Géó_CH_International	269	Provenance des groupes d'auteurs
↓ Marque véhicules	84	Liste de marques courantes de véhicules
↓ Monnaie	162	Devises
↓ Moyen de communication	3	Descr. du moyen de communication
↓ Moyen de contrôle	11	Moyen de contrôle des données
↓ Pays	240	Liste des pays ISO
↓ Prestataires de service	29	Liste des principaux prestataires de service
↓ Procédure	3	Type de procédure
↓ Rôle Argent	4	Rôle de l'apersonne pour l'argent (biens)
↓ Rôle moyen comm	6	Rôle de la personne pour les moyens de communication
↓ Rôle vhc	4	Rôle de la personne pour un véhicule
↓ Sexe	3	Liste sexe
↓ Source	16	Source des informations
↓ Source contrôle	31	Source du contrôle
↓ Type Choses	11	Types d'objets
↓ Type d'adresse	17	Type d'adresse
↓ Type de moyen comm	5	Type de moyen de communication
↓ Type de traces	12	Type de traces rencontrés sur uenscène de crime
↓ Type vhc	22	Genre de véhicule

fig. 146 : Listes de choix du prototype β

Le détail de la conception du prototype β se trouve à l'annexe II. Le lecteur y retrouvera le détail des différentes listes ci-dessus. Une quinzaine de listes servent à saisir les légendes des liens qui apparaîtront lors des visualisations graphiques et permettront des analyses fines de la situation (au-dessus de la ligne grise de la figure ci-dessus).

Icon Lists		
Icon List	No of Items	Description
↓ Icone Antécédent	11	Liste des icônes pour représenter graphiquement un Antécédent
↓ Icone Argent (biens)	10	Liste des icônes pour représenter graphiquement un Bien (argent)
↓ Icone Choses (biens)	39	Liste des icônes pour représenter graphiquement un Bien (chose)
↓ Icone Communication	16	Liste des icônes pour représenter graphiquement un Moyen de communication
↓ Icone Événement	23	Liste des icônes pour représenter graphiquement un Événement
↓ Icone Forensique	19	Liste des icônes pour représenter graphiquement une trace
↓ Icone Lieu	162	Liste des icônes pour représenter graphiquement un Lieu
↓ Icone Personne	55	Liste des icônes pour représenter graphiquement une Personne
↓ Icone Transport	32	Liste des icônes pour représenter graphiquement un Moyen de transport

fig. 147 : Listes d'icônes du prototype β

Pour rappel, les listes d'icônes sont détaillées à l'annexe II, et illustrées à l'annexe I.

### 3.3.4 Système de visualisation : relationnel et chronologique

Comme nous l'avons abordé au chapitre portant sur l'analyse criminelle<sup>325</sup>, les principaux types de visualisations graphiques sont relationnels et chronologiques.

<sup>325</sup> Voir plus particulièrement le chapitre 1.4.6 – Techniques utilisées dans le cadre de la criminalité organisée

L'outil choisi pour élaborer le prototype  $\beta$  est particulièrement bien armé de ce côté-là. Il est en effet directement lié à l'*Analyst's Notebook*<sup>TM</sup>, logiciel qui est une référence mondiale en la matière.

C'est donc très simplement que les informations contenues dans les bases d'analyse peuvent être visualisées et même saisies. En effet, la saisie depuis le logiciel de visualisation est en général préférée par les analystes à la saisie dans le système de base de données. La saisie, ainsi rendue « visuelle », leur est très familière et ne se différencie du travail habituel de représentation que par le masque des données à saisir, qui est repris de la base de données *iBase*<sup>TM</sup>, et non plus de l'interface standard de l'*Analyst's Notebook*<sup>TM</sup>.

Le système JANUS PV 2.0 a tout de même prévu une possibilité de visualisation des données<sup>326</sup>, sans passer par le composant d'analyse, sujet de cette présente recherche. Afin de rendre une visualisation possible, un fichier d'échange doit être créé. Il est ensuite importé dans l'*Analyst's Notebook*<sup>TM</sup> à l'aide d'une interface prédéfinie.

En ce qui concerne le prototype  $\beta$ , toutes les entités sont immédiatement visualisables, selon des critères prédéfinis et qui peuvent être paramétrés selon des besoins génériques ou spécifiques. Ces critères sont donc aussi facilement évolutifs.

Des schémas d'utilisation récurrents allant des représentations relationnelles de tout type d'entités contenues dans la base de données à des représentations chronologiques spécifiques de connexions téléphoniques ou d'autres moyens de communication sont envisageables avec la structure de la base de données d'analyse du *prototype*  $\beta$ . Pour satisfaire à ces différents besoins dans les autres phases des investigations, certaines possibilités techniques s'offrent aux analystes au sein de la suite logicielle de *i2 inc.* Ces fonctions sont d'une réelle utilité et elles justifient pleinement le recours à de tels logiciels spécifiques comme support à l'analyse de données ou de situation.

#### **3.3.4.1 Représentations relationnelles**

Le logiciel *iBase*<sup>TM</sup> produit de manière standard des représentations relationnelles que ce soit dans l'*Analyst's Notebook*<sup>TM</sup> ou à l'aide d'un visualisateur interne nommé « *iBase Link Chart* ».

L'avantage de ce visualisateur est sa simplicité pour représenter de manière relationnelle les informations en relation avec une seule entité. La figure suivante en donne un exemple.

---

<sup>326</sup> Voir plus loin point 3.4.1.1 – Visualisation de JANUS PV 2.0



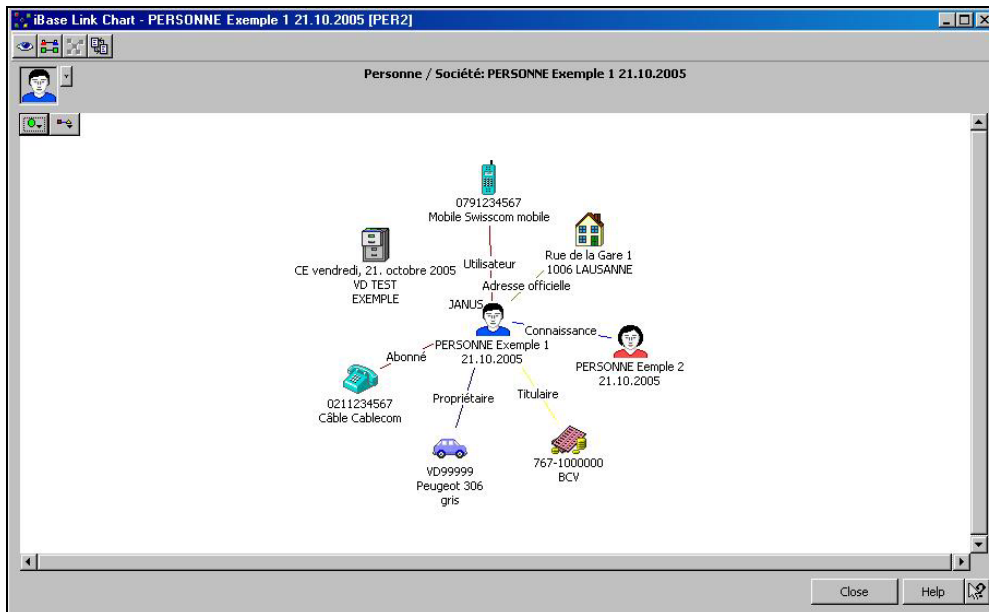


fig. 148 : Visualisateur interne de iBase™ (iBase Link Chart)

Ce visualisateur permet très simplement de limiter le champ des éléments à visualiser en utilisant un outil spécifique que ce soit par rapport aux entités à afficher, ou aux liens à prendre en compte. La figure suivante illustre un filtre appliqué sur certains liens présents.

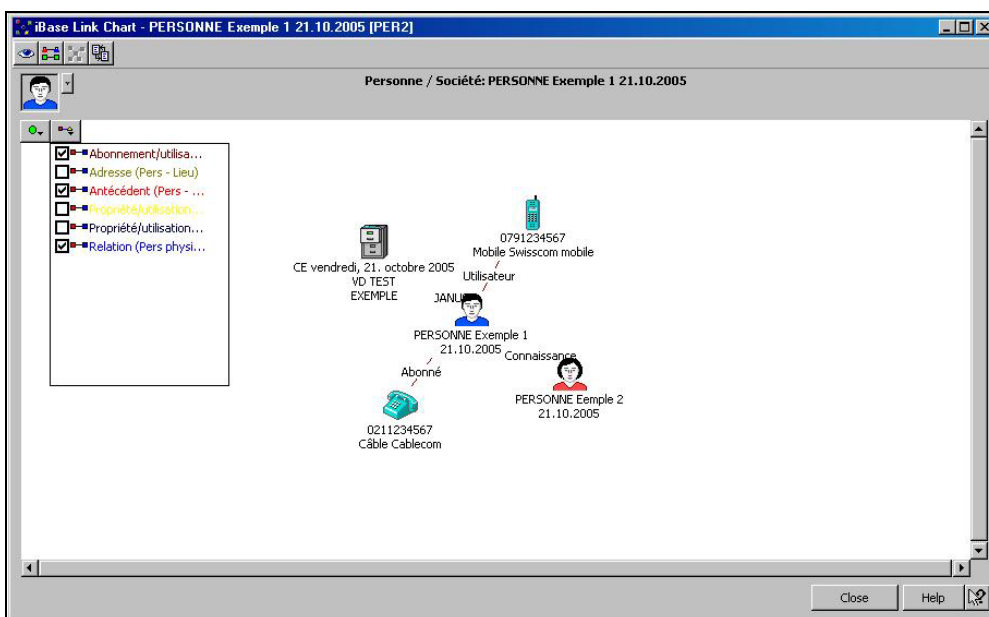


fig. 149 : Visualisateur interne de iBase™ (filtre sur les liens)

Le principal désavantage de ce visualisateur est qu'il n'est possible de représenter qu'une seule entité « centrale » avec ses liens directs. Pour des représentations plus complexes, il devient nécessaire de travailler avec l'*Analyst's Notebook™*.



La visualisation des données de *iBase*<sup>TM</sup> dans l'*Analyst's Notebook*<sup>TM</sup> est également très simple. Il suffit de donner l'ordre dans la base d'analyse de visualiser un élément dans un schéma pour que le programme de visualisation se lance, connecte la base de données à la visualisation et fasse apparaître l'entité en question sur le schéma.

La visualisation des liens de cette entité peut se faire de deux manières différentes. La première ressemble au visualisateur interne de *iBase*<sup>TM</sup> et elle s'active par la commande « *explore* ».

La figure ci-dessous reproduit l'exploration d'une entité du prototype  $\beta$  dans l'*Analyst's Notebook*<sup>TM</sup>.

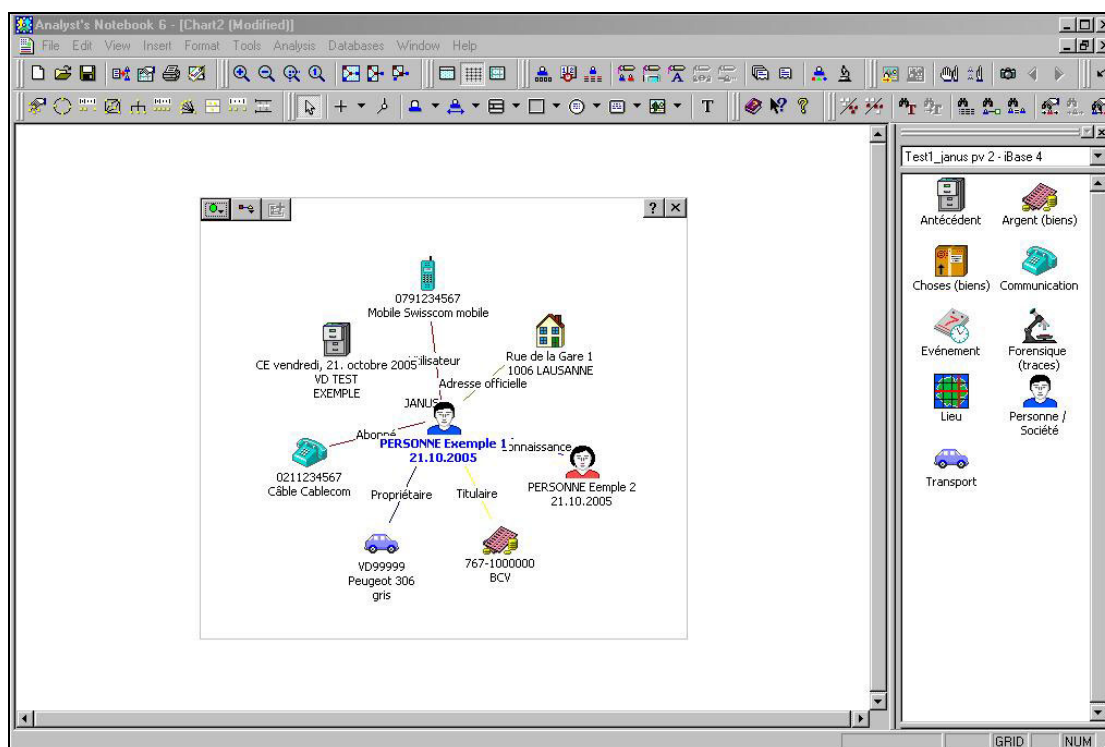


fig. 150 : Fonction « *explore* » dans l'*Analyst's Notebook*<sup>TM</sup>

Les mêmes possibilités de filtre des informations à afficher existent comme dans le *iBase Link Chart*. Une fois le filtre appliqué, l'analyste sélectionne les entités à ajouter et utilise le troisième bouton en haut à gauche de la fenêtre d'exploration pour valider son choix. Cette opération peut ensuite être répétée pour chaque entité présente sur le schéma qui va être construit automatiquement de proche en proche.

La seconde possibilité offerte à l'analyste est plus directe. Il s'agit de la fonction « *expand* ». Celle-ci est activable par un « clic-droit » de la souris.

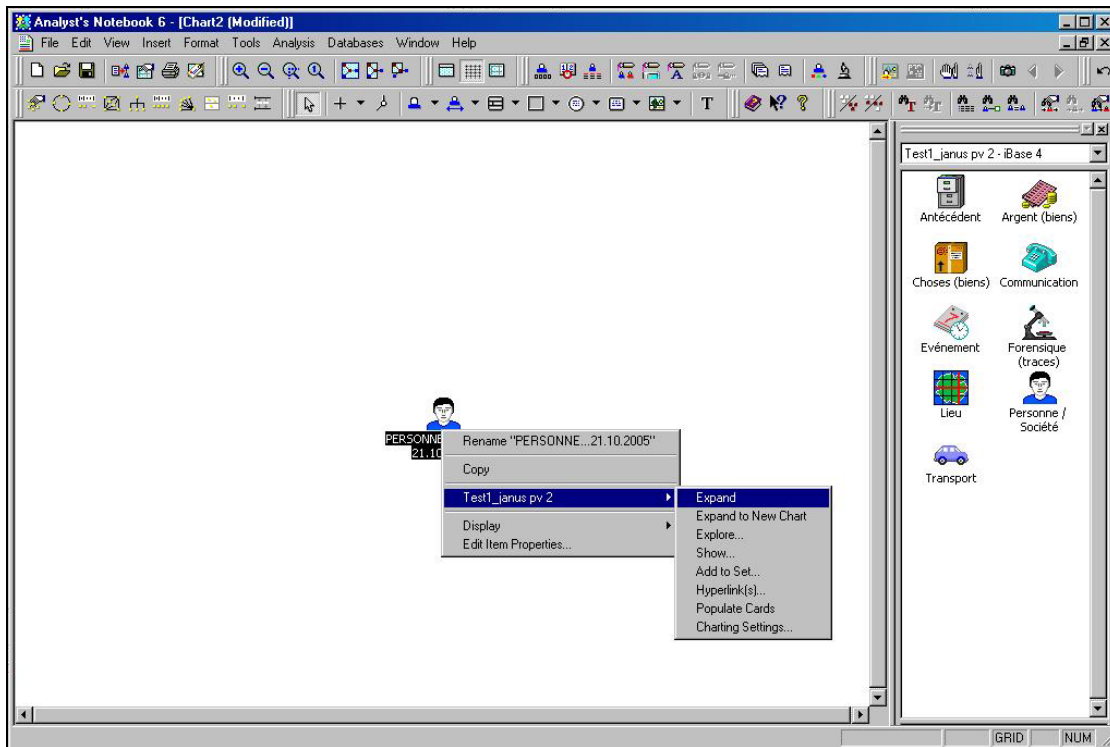


fig. 151 : Fonction « expand » dans l'Analyst's Notebook™

Une fois cette fonction activée, les entités liées vont automatiquement être ajoutées à la visualisation. Il est toutefois possible de paramétrer cette fonction « expand » par un menu appelé « charting settings ».

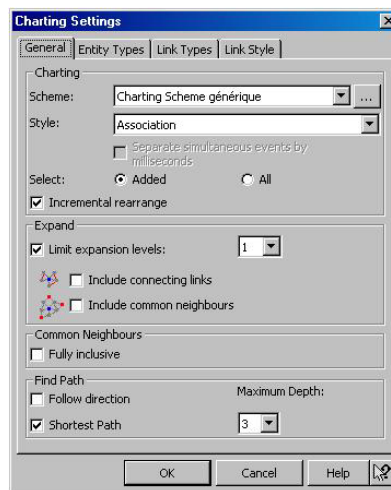


fig. 152 : Fonction « Charting settings » dans l'Analyst's Notebook™

De nombreuses fonctionnalités peuvent être paramétrées à l'aide de ce menu. Premièrement, il est possible de choisir le modèle d'affichage parmi ceux qui auront été prédéfinis, en fonction d'une représentation relationnelle, chronologique ou combinée.

Le nombre de niveaux de recherche de liens peut être ajusté de 1 à 5. En choisissant le niveau 2, on va faire apparaître automatiquement les éléments liés aux liens directs, et ainsi de suite.

Il est encore possible de faire apparaître automatiquement les liens internes aux entités présentes sur le schéma, les « *connecting links* » et les entités proches à plusieurs éléments déjà présents, les « *common neighbours* ».

Enfin, il est évidemment possible (par l'intermédiaire des autres onglets visibles à la figure précédente) de filtrer selon leur type les entités ou liens devant être affichés.

Comme on peut le constater, les possibilités offertes pour la construction assistée de représentations visuelles des données contenues dans la base d'analyse sont très importantes et permettent de produire des schémas particuliers ou généraux très rapidement, en quelques opérations.

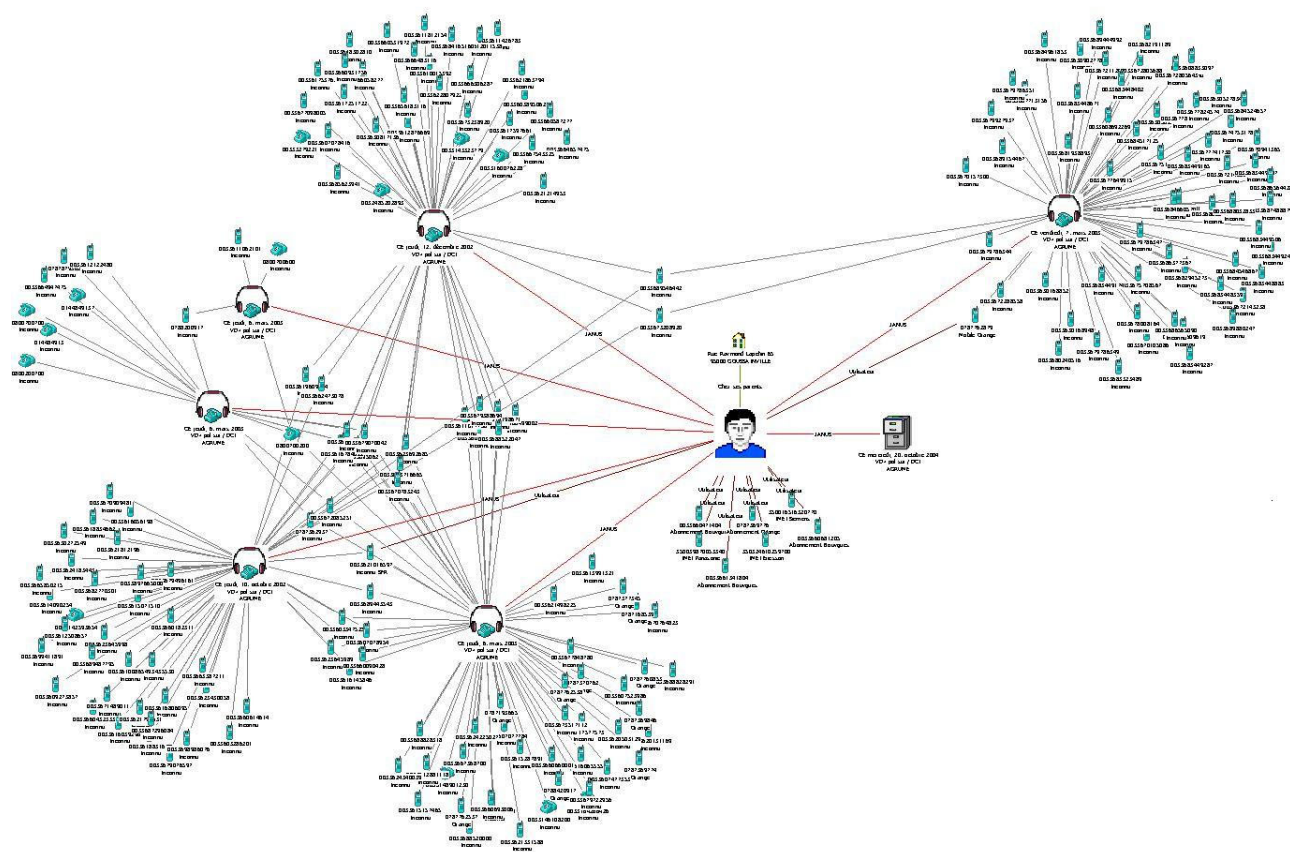


fig. 153 : Exemple de représentation relationnelle de données réelles contenues dans le prototype  $\beta$

L'exemple précédent est une représentation de données réelles concernant un suspect qui a fait l'objet de six contrôles techniques sur ses différents raccordements mobiles. La représentation de ces données contenues dans une base de test construite sur le modèle du prototype  $\beta$  est instantanée en choisissant la fonction « *expand* » avec les paramètres idoines.

### 3.3.4.2 Représentations chronologiques

Le principe est exactement le même pour la création de schémas temporels que pour les représentations relationnelles. Les données contenues dans la base d'analyse sont immédiatement prêtes à la visualisation. Il n'est toutefois pas possible de travailler uniquement avec *iBase™* et il faut avoir recours à l'*Analyst's Notebook™*.

Les paramètres de la visualisation sont déterminés dans les « *Charting settings* » (cf. figure 152). Il est ensuite possible de visualiser ses données par une simple fonction « *expand* ».

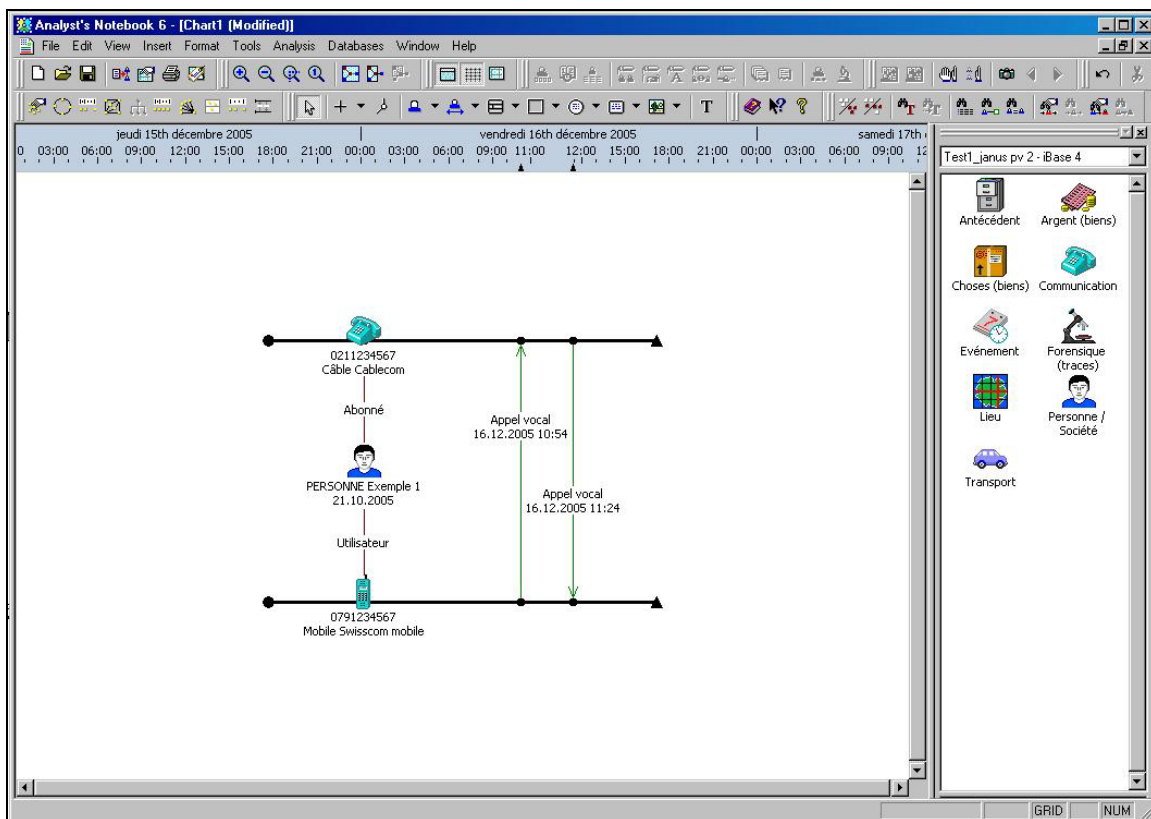


fig. 154 : Représentation chronologique de connexions (liens) contenues dans le prototype  $\beta$

Il s'agit ici en fait d'une représentation mixte, puisque la personne est représentée de manière relationnelle et que le flux des appels est visualisé.

Comme nous l'avons vu dans l'exemple précédent, certains liens comme les transactions et autres communications disposent d'une composante chronologique qui peut donc être utilisée pour une visualisation chronologique. Certaines entités comme les événements ou les antécédents possèdent aussi une information temporelle.

Il devient ainsi également possible de créer très rapidement et très simplement des schémas temporels des données présentant une composante chronologique et qui sont saisies dans les bases de données d'analyse.

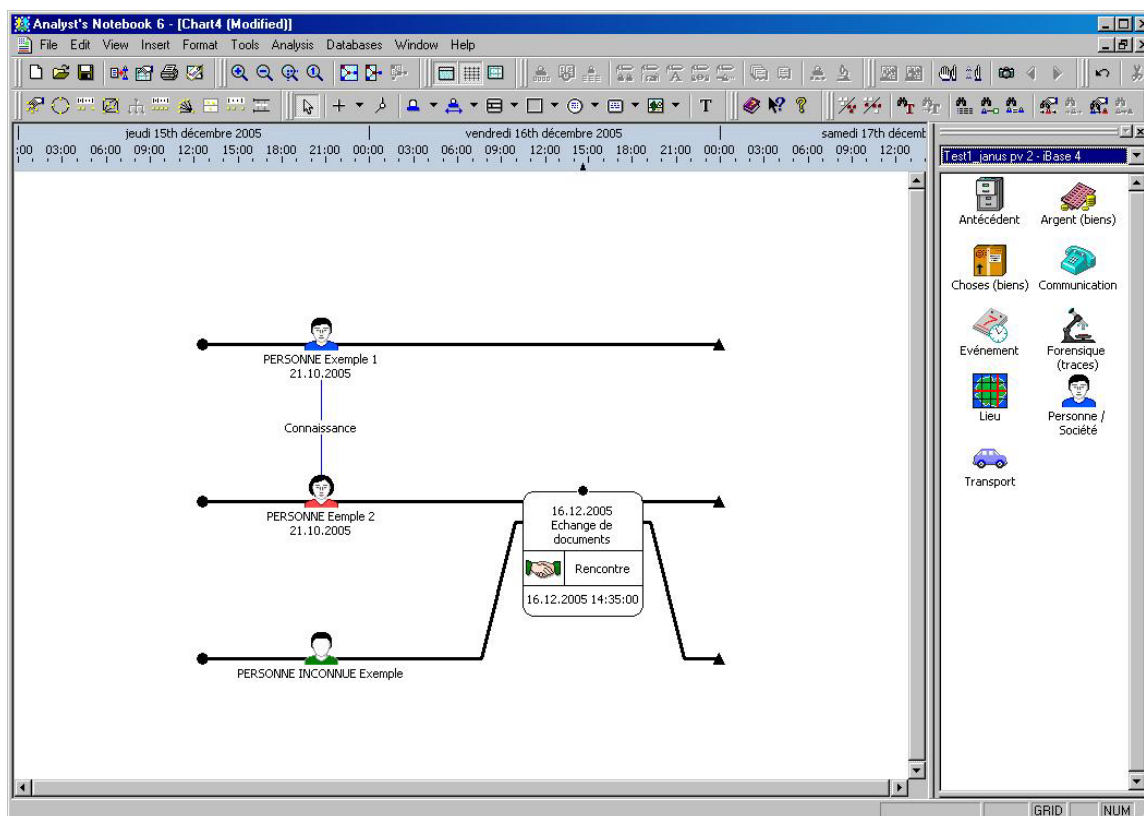


fig. 155 : Représentation chronologique d'événements (entités) contenus dans le prototype  $\beta$

Par exemple, pour en revenir à l'exemple réel illustré à la figure 153, on peut également représenter cette situation en ajoutant une composante temporelle, qui est la date des contrôles techniques issus de JANUS PV. Ainsi, on verra chronologiquement la succession des différents contrôles techniques, auxquels l'analyste a ajouté les raccordements téléphoniques communs.

Ce mécanisme permet de mettre aisément en évidence les différentes périodes d'activité des numéros communs. Et il devient ainsi aisé de sélectionner les raccordements communs aux différentes mesures de surveillance et qui perdurent dans le temps. Cette sélection de numéros communs et actifs sur de longues périodes est extrêmement utile, par exemple, pour la détection de structures persistantes au sein des groupements criminels organisés. Par exemple, certains soutiens logistiques sont contactés beaucoup moins fréquemment que les autres acteurs des trafics et doivent donc conserver leurs moyens de communication durant une plus longue période.

Le schéma de la page suivante illustre ce cas de figure où des contacts ont lieu de manière récurrente à plus d'une année d'intervalle, le reste des raccordements concernés étant très volatile.

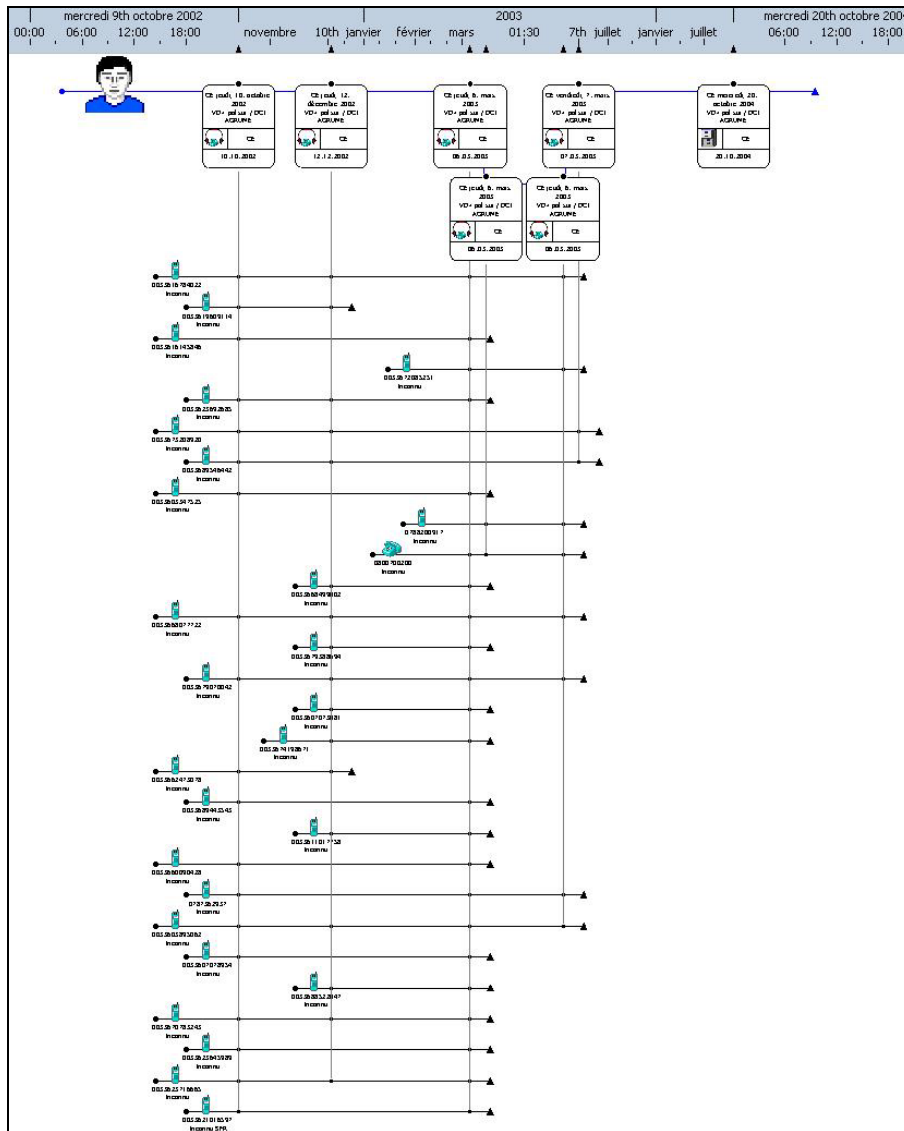


fig. 156 : Exemple de représentation chronologique de données réelles contenues dans le prototype  $\beta$

### 3.3.5 Autres fonctions d'analyse propres à *iBase*<sup>TM</sup> et utiles au prototype $\beta$

Le développement du prototype  $\beta$  à l'aide du logiciel *iBase*<sup>TM</sup> permet aussi de bénéficier des fonctionnalités d'analyse intégrées au logiciel, sans devoir les développer spécifiquement.

Nous allons ici passer rapidement en revue quelques-unes de ces fonctions supplémentaires et disponibles dans ce produit d'*i2 inc.*

#### 3.3.5.1 Recherches visuelles et pondérées

Nous avons vu précédemment que des recherches multicritères complexes (*Visual Search- Query*) pouvaient être créées et enregistrées dans *iBase*<sup>TM</sup><sup>327</sup>.

Les liens du prototype  $\beta$  devaient donc être prédéfinis de manière très précise pour que ce type de recherche complexe soit le plus efficace possible.

<sup>327</sup> Voir figure 139 - Recherches visuelles dans *iBase*



Une seconde fonctionnalité de recherche complexe peut être définie. Il s'agit d'introduire des pondérations pour certains critères (*Scored Matching*). L'exemple suivant permet de rechercher une voiture d'une certaine marque, modèle et couleur, de manière pondérée selon la validité d'un témoignage.

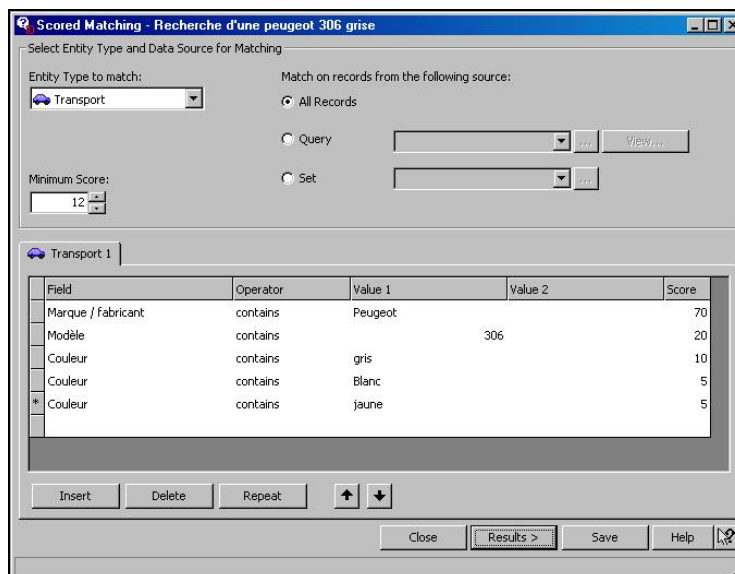


fig. 157 : Critères de la recherche pondérée d'iBase™

Les résultats apparaissent en fonction de leur score calculé selon la pondération définie.

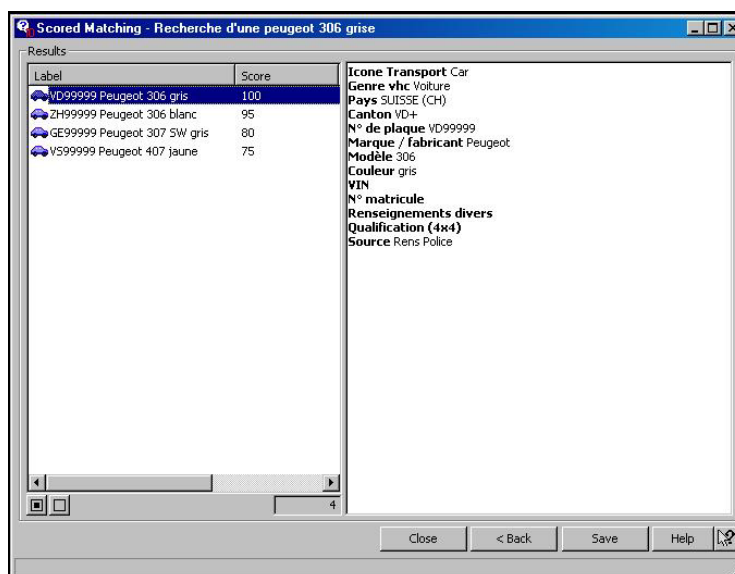


fig. 158 : Résultats de la recherche pondérée d'iBase™

Il est également possible de combiner une recherche visuelle prédéfinie et une recherche pondérée. Ceci permettant de rechercher une information incertaine dans une partie des données spécifiées par une recherche visuelle complexe.

### 3.3.5.2 Sélections (Sets)

En tout temps, il est possible d'enregistrer et de gérer des sélections (*Sets*) d'entités et/ou de liens. La création de sélections est très utile lorsque l'analyste voudra travailler sur une partie des données contenues dans sa base. S'il est possible d'enregistrer les critères des recherches visuelles ou pondérées, elles n'offrent pas la même stabilité que des sélections qui sont figées et qui ne réagissent plus aux éléments nouveaux.

Une fois ces sélections faites, il est possible d'analyser les informations qui y sont contenues de manière précise. L'exemple suivant présente des sélections issues de contrôles techniques réels traités avec le prototype  $\beta$ .

La figure suivante montre comment *iBase*<sup>TM</sup> permet simplement et rapidement de combiner deux sélections à l'aide d'intuitifs diagrammes de Venne.

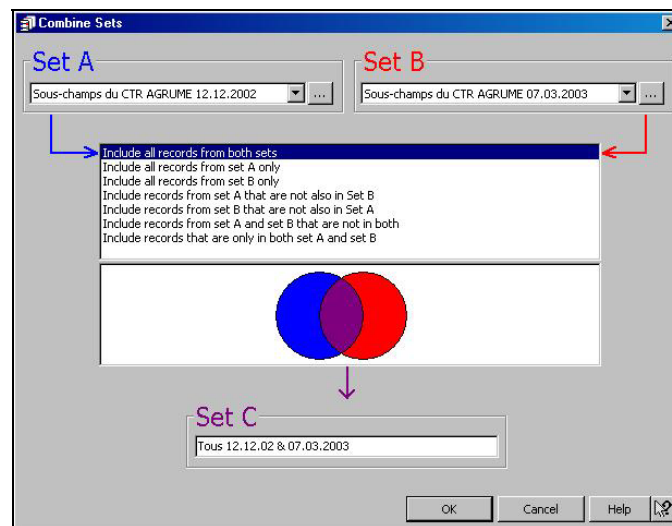


fig. 159 : Combinaison de sélections dans *iBase*<sup>TM</sup>

Il est possible avec cette fonction de fusionner deux sélections, ou d'en retirer la partie de son choix (intersection,  $A - [\text{tout } B]$ , etc.).

Mais il est également possible d'analyser plus que deux sélections entre elles. On fait alors appel à une autre fonction d'analyse. De cette manière on pourra rechercher soit tous les communs aux sélections choisies ou tout ce qui n'est pas commun à ces sélections. L'exemple suivant l'illustre :



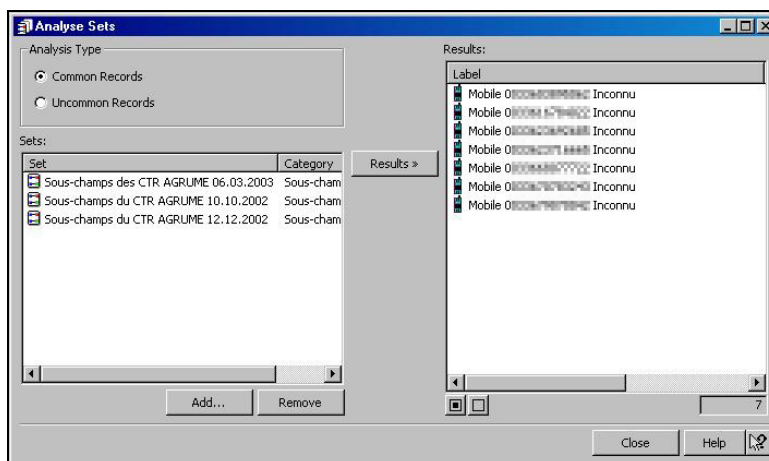


fig. 160 : Analyse de sélections dans iBase™

Toutefois, toutes ces fonctions de sélections et de combinaison ou d'analyse sont très simplement réalisables visuellement dans l'*Analyst's Notebook™*, comme le démontre la figure suivante :

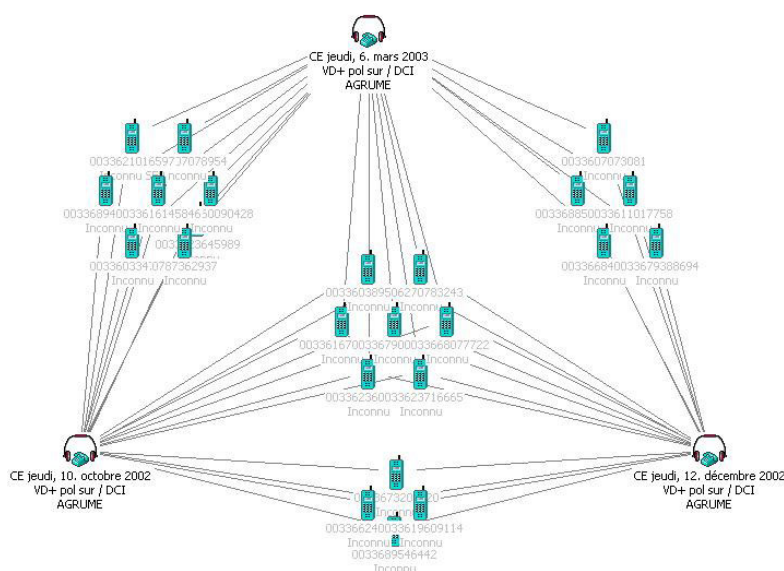


fig. 161 : Utilisation de l'*Analyst's Notebook™* pour la recherche d'éléments communs

### 3.3.5.3 Exploration et recherche « texte »

Enfin, pour compléter ces diverses fonctions de recherche complexe et de sélection, *iBase™* propose un explorateur permettant de lister les éléments.

L'explorateur permet également de sauvegarder une recherche qui peut être récurrente, afin de ne pas avoir à la re-paramétrer. L'exemple suivant montre le résultat d'une recherche faite sur tous les véhicules dont l'immatriculation se termine par « 99 », classés par canton.

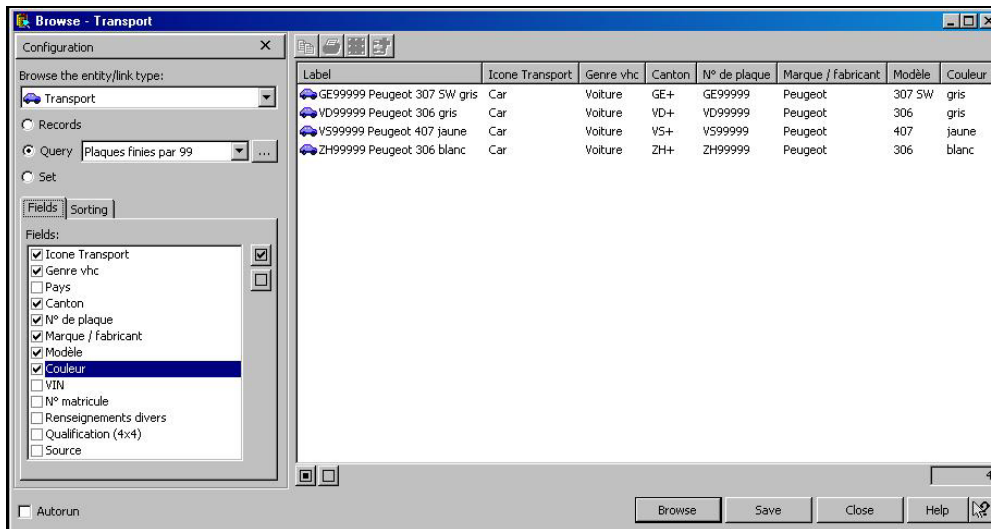


fig. 162 : Explorateur dans iBase™

Enfin, une fonction de recherche « texte » permet d’indexer tous les mots apparaissant dans la base de données d’analyse et de recherche par un critère indépendamment de toute autre considération. Il est encore possible de construire un dictionnaire des synonymes.

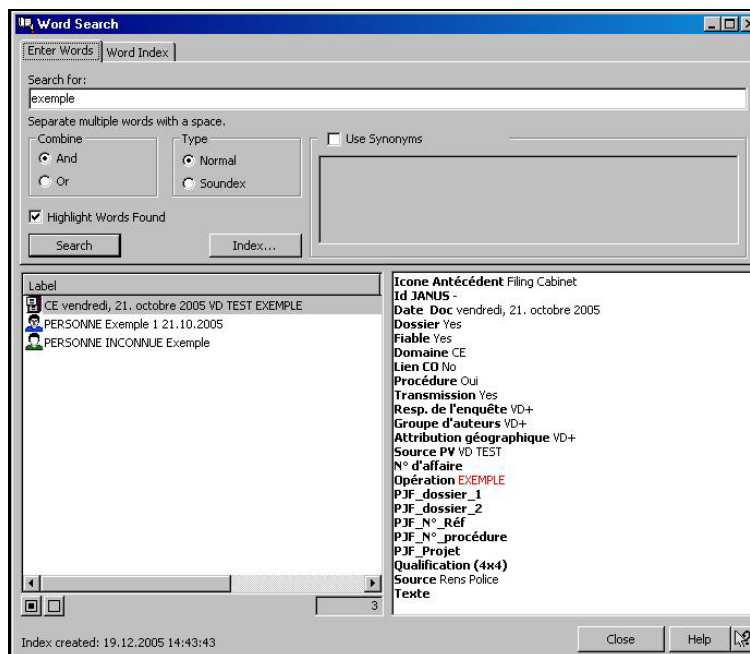


fig. 163 : Recherche « texte » dans iBase™

La figure ci-dessus illustre une recherche du mot « exemple ».

### 3.3.6 Synthèse

Le prototype  $\beta$  qui a été décrit ici a été développé afin de permettre l’importation des données contenues dans la base de données d’enquête fédérale JANUS PV 2.0. Un soin tout particulier a été apporté à la structure de cette base d’analyse, afin qu’elle puisse s’appliquer au plus grand nombre

possible de situations. D'autre part, l'organisation des données a été strictement définie afin de permettre à l'analyste d'utiliser tout le potentiel d'analyse qu'offrent les logiciels métier *iBase™* et *Analyst's Notebook™*.

Toutefois, avant de passer au chapitre de l'interconnexion des deux composants, soit les mémoires à long et court terme, comme définie dans la description du projet, il convient encore de préciser que la saisie manuelle des données par l'équipe d'enquête a été également simplifiée autant que possible par l'utilisation de masques de saisie spécifiques.

Par exemple, le masque de saisie de l'entité *Personne / Société* est le suivant :

fig. 164 : Masque de saisie Personne / Société du prototype  $\beta$

Cette figure devrait vous rappeler le masque de saisie de JANUS PV 2.0, puisque c'est de la base prototype que s'est inspiré le groupe de travail pour la création des masques de la base de données fédérale.

### 3.4 *Interconnexion des deux composants du système*

Lors de la réalisation de ce composant du système, il est rapidement apparu que les principales difficultés structurelles et techniques allaient se cristalliser ici.

En effet, alors que l'ancien système JANUS PV ne prévoyait aucune possibilité ou procédure d'exportation ou d'importation de données, le groupe de travail responsable de l'élaboration du nouveau JANUS PV 2.0 avait fait mention au cahier des charges que de telles possibilités devaient exister. Ceci étant posé, nous espérions que le projet de cette recherche pourrait être mené à son terme. Cependant, plus de trois ans après la mise en service du nouveau JANUS PV (devenu entre-temps JANUS 3.0), ces fonctionnalités n'ont toujours pas été implantées. Il serait toutefois souhaitable qu'elles le soient un jour et que les modalités techniques des importations/exportations (qui ont été décrites) soient enfin utilisées. Nous ne savons pas si ce besoin est finalement perçu comme superflu, ce qui ne justifierait pas les efforts et les coûts nécessaires à son développement ou si les retards pris dans la finalisation des autres fonctions des « sous-systèmes » PV et JO sont toujours prioritaires, puisqu'elles répondent aux besoins des enquêteurs<sup>328</sup>, traditionnellement mieux compris par la direction du projet.

Voici néanmoins les caractéristiques de cette hypothétique interconnexion entre les deux composants. Le langage prévu pour l'exportation des données était le XML (*eXtensible Markup Language*). Le XML<sup>329</sup> est, comme le dit GARDARIN : « plutôt un ensemble de règles de formatage pour composer un message valide »<sup>330</sup>.

Comme il le rappelle encore : « structurer les échanges en décrivant les messages et en adoptant un formalisme auto descriptif a beaucoup de conséquences ». L'exemple qui suit montre que l'autoréférence pose un problème de fond. Imaginons que nous demandions à plusieurs personnes de nous décrire une pomme. Il est vraisemblable que les éléments descriptifs donnés par chacun nous permettent d'identifier une pomme, mais ils seront sans doute très différents :

*« Il s'agit d'un fruit, qui est issu d'un arbre fruitier, qui se récolte en automne et qui est utilisé pour faire d'excellente tartes. »*

ou alors :

*« C'est rond, c'est un fruit qui peut être vert, jaune ou rouge et qui fait un excellent jus. ».*

---

<sup>328</sup> Voir chapitre 2.4.1 – Besoins de chaque intervenant

<sup>329</sup> XML est un modèle de représentation et d'échange de données standard et pérenne, indépendant de tout constructeur. Il s'agit d'un métalangage, puisque son vocabulaire spécifique est inclus au message sous la forme de balises ou tags. XML fournit les outils pour définir la structure et la grammaire des messages, celles-ci se retrouvant dans les schémas des documents.

<sup>330</sup> GARDARIN, XML – Des bases de données au service du Web, 2002

Si chacune des deux personnes devaient rédiger son message en XML, cela pourrait donner le résultat suivant :

Personne 1	Personne 2
Message : <i>Il s'agit d'un fruit, qui est issu d'un arbre fruitier, qui se récolte en automne et qui est utilisé pour faire d'excellentes tartes.</i>	Message : <i>C'est rond, c'est un fruit qui peut être vert, jaune ou rouge et qui fait un excellent jus.</i>
XML : <pre>&lt;message&gt;   &lt;type&gt;fruit&lt;/type&gt;   &lt;source&gt;arbre fruitier&lt;/source&gt;   &lt;recolte&gt;automne&lt;/recolte&gt;   &lt;production&gt;tartes&lt;/production&gt; &lt;/message&gt;</pre>	XML : <pre>&lt;message&gt;   &lt;forme&gt;rond&lt;/forme&gt;   &lt;type&gt;fruit&lt;/type&gt;   &lt;couleur&gt;vert, jaune ou rouge&lt;/couleur&gt;   &lt;production&gt;jus&lt;/production&gt; &lt;/message&gt;</pre>

Chacune des deux personnes a choisi les éléments nécessaires à la description de la pomme. Si certains sont récurrents comme le type et ce qu'on en fait (production), d'autres sont propres à chacune des personnes.

Lors de l'utilisation de documents (ou messages) XML pour la transmission de données, on se trouve exactement dans cette configuration. Des contenus similaires, mais pas immédiatement compatibles. La force du XML est son potentiel à les rendre compatibles, puisque le vocabulaire et la grammaire sont inclus au document. Il est donc possible de transformer les données de l'une pour les rendre compatibles avec l'autre. Mais, pour cela, il faut que la personne 1 conserve strictement la même manière de décrire les objets afin que la personne 2 puisse traiter ses messages de manière systématique et pérenne.

Afin que chacune des personnes conserve son « style » de communication, XML prévoit que des *schémas* soient définis, afin que les messages soient toujours formatés de la même manière. Dans notre exemple, cela donnerait :

Personne 1	Personne 2
XML : <pre>&lt;xsd :schema&gt;   &lt;xsd :element name="type" type="xsd :string"/&gt;   &lt;xsd :element name="source" type="xsd :string"/&gt;   &lt;xsd :element name="recolte" type="xsd :string"/&gt;   &lt;xsd :element name="production" type="xsd :string"/&gt; &lt;/xsd :schema&gt;</pre>	XML : <pre>&lt;xsd :schema&gt;   &lt;xsd :element name="forme" type="xsd :string"/&gt;   &lt;xsd :element name="type" type="xsd :string"/&gt;   &lt;xsd :element name="couleur" type="xsd :string"/&gt;   &lt;xsd :element name="production" type="xsd :string"/&gt; &lt;/xsd :schema&gt;</pre>

XML n'étant pas un langage de programmation, il a fallu prévoir un langage de transformation de documents XML. Ces transformations s'effectuent via XSL (*eXtensible Styling Language*). Elles sont décrites dans ce qu'on appelle des *feuilles de style*.

Pour en revenir à la problématique de cette recherche, d'une part JANUS PV 2.0 devait donc produire des documents XML contenant les informations exportées de la base de données (des schémas ont d'ailleurs été créés par les développeurs du système) et d'autre part, la base d'analyse *iBase™* a besoin de recevoir les informations selon un schéma qui, évidemment, lui est propre. Il est donc nécessaire de définir des feuilles de style afin de permettre à *iBase™* de comprendre les informations extraites de JANUS PV 2.0. Ces transformations et formatages sont des étapes courantes dans les processus d'échanges avec XML. GARDARIN le schématise de la manière suivante :

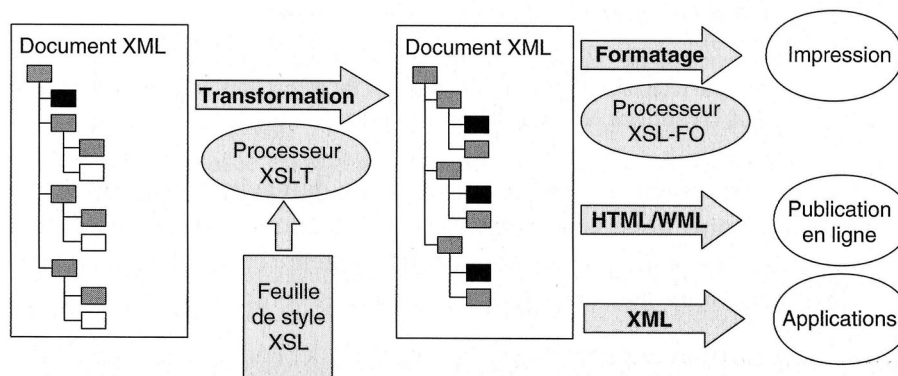


fig. 165 : Transformation et formatage de document XML<sup>331</sup>

Les traitements sont toutefois loin d'être simples et nous avons dû nous concentrer sur le flux descendant de données de JANUS PV 2.0 vers *iBase™*.

La suite de ce chapitre va donc naturellement être décomposée en trois parties, soit : la description de l'exportation de JANUS PV 2.0, l'importation et l'exportation XML avec *iBase™* et enfin les traitements nécessaires aux documents XML pour les transformer.

### 3.4.1 Exportation de JANUS PV 2.0

Bien que des standards XML aient été validés par tous les services informatiques de la Confédération, en particulier au sein du CSI-DFJP, l'exportation de données brutes de JANUS PV 2.0 n'est pas encore pratiquement à l'ordre du jour, bien que cette fonctionnalité ait été demandée par le groupe de travail et qu'elle soit déjà expressément prévue par l'ordonnance JANUS<sup>332</sup>. Nous ne désespérons pas que l'exportation de données soit réalisée avec la réunion des « sous-systèmes »

<sup>331</sup> Tiré de GARDARIN, *op. cit.*, 2002, p. 119

<sup>332</sup> Voir chapitre 1.3.4 – art. 19 de l'Ordonnance JANUS de 2002

dans JANUS 3.0 courant 2007, mais nos espoirs ont à nouveau été déçus, et nous allons devoir encore attendre d'éventuelles maintenances évolutives pour voir peut-être la réalisation de ces passerelles.

La conversion des éléments présents dans JANUS PV, soit les PERSONNES et leurs ANTECEDENTS, ainsi que leurs objets, soit les « attributs » et les « sous-champs » devrait pouvoir se faire quasiment intégralement. Seuls deux « sous-champs » que sont les transactions financières (FTA) et les *routings* (RTG) ne seraient pas repris. Le schéma ci-dessous illustre dans quel type d'entité ces éléments seraient repris.

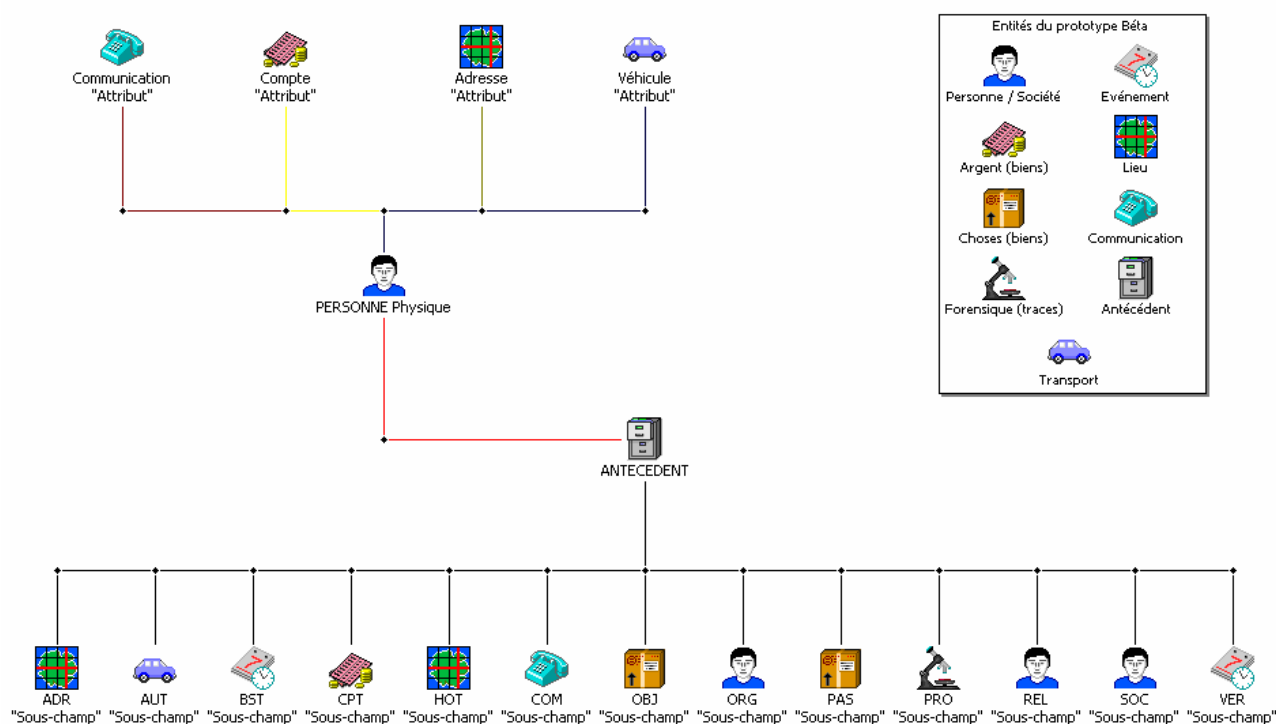


fig. 166 : Schéma de conversion entre JANUS et le prototype  $\beta$

Pour le retour des données dans JANUS, qui n'est pas encore à l'ordre du jour non-plus, un filtre humain d'éligibilité est nécessaire, étant donné que les informations contenues dans la base de données d'analyse n'ont pas toutes pu être vérifiées, ni ne répondent aux critères de l'ordonnance JANUS<sup>333</sup>.

En été 2006, soit une année après la mise en service de la nouvelle version de JANUS PV, la seule possibilité « d'exportation » des données se faisait par le biais d'une visualisation des « sous-

<sup>333</sup> Bien que la nouvelle loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP) permet désormais que : « Chaque canton peut, pour ses propres données, accorder un accès en ligne aux autorités cantonales et fédérales de police et de poursuite pénale qui, dans le cadre de leurs tâches, collaborent avec le canton concerné. » (Art. 13 al. 3)

champs » contenus dans les antécédents d'une personne, sous la forme d'un fichier texte décrivant les relations selon un modèle tabulaire. Malheureusement, cette visualisation était inutilisable, les programmeurs n'ayant pas tenu compte de la nouvelle plus-value de JANUS PV 2.0 qui permet de différencier des liens indirects de différents niveaux. Ainsi le résultat d'une telle visualisation ne reflétait pas la situation réelle et rendait toute analyse vaine. Une réunion de travail spécifique a donc eu lieu entre l'équipe de développement de JANUS, des analystes vaudois et d'autres travaillant au sein de la police judiciaire fédérale. Il a été décidé que le principe de visualisation devait répondre aux spécificités décrites ci-après.

### 3.4.1.1 Visualisation de JANUS PV 2.0

Pour la visualisation des données, il est primordial que les relations directes et indirectes puissent être mises en évidence. Pour cela, il faut reformater les données afin que les objets directement liés à la personne (les « attributs ») soient liés à celle-ci et que les « sous-champs » d'un antécédent lui soient liés, à lui, comme le montre le schéma suivant :

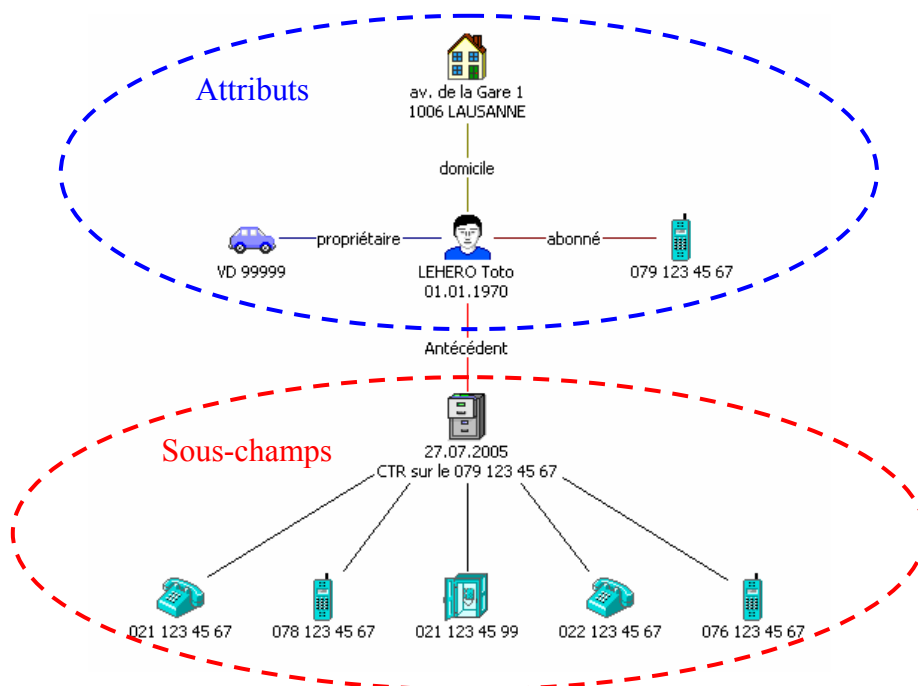


fig. 167 : Principe de représentation des liens de différents niveaux dans JANUS PV 2.0

Le niveau informatique moyen des personnes appelées à utiliser un tel système de visualisation nous amène à préférer un pré-formatage des données dans un fichier \*.txt, \*.csv ou \*.xls. Ces trois formats sont compatibles avec *l'Analyst's Notebook™* de *i2 inc.*, connus et généralement maîtrisés par les enquêteurs et analystes. Pour le XML, il faut bien constater qu'il est encore trop peu connu de cette communauté d'utilisateurs.



Il faut donc préparer le fichier tabulaire, chaque ligne correspondant à un lien entre deux entités. La table doit convenir à chaque type d'entité, si l'on veut pouvoir importer l'ensemble des informations en une seule opération !

Le choix s'est porté sur un compromis réaliste, soit 7 colonnes pour l'entité A, 3 colonnes pour le lien et 7 colonnes pour l'entité B, soit 17 colonnes au total :

Entité A							Lien			Entité B						
...																

### Détail des entités

Pour la visualisation, en plus des personnes (identité principale) et des antécédents, il faut tenir compte des objets principaux (personnes et organisations, adresses, véhicules, communication et comptes bancaires).

Pour tous ces éléments de JANUS PV 2.0, il est nécessaire de leur adjoindre leur numéro d'identification JANUS PV 2.0 pour permettre de les identifier formellement.

#### *Personnes*

Pour les personnes, que ce soit l'identité, un alias ou une relation (REL), pour pouvoir l'identifier, il faut mentionner : *NOM, Prénom, Date de naissance* et *Nationalité*.

L'icône standard pour la visualisation a été défini comme l'image « Male » pour les hommes et l'image « Female<sup>334</sup> » pour les femmes. Mais, il est aussi possible de définir l'icône « Alias », justement pour ce type d'identité. Et pour les organisations : l'image « Organisation ». Subsiste le problème des éventuels inconnus, réglé par l'image « Anonymous ».



Un exemple de personne est reproduit dans la table suivante :

N° JANUS	Label	NOM	Prénom	Date naiss.	Nationalité	Icône
86971	LEHERO Toto, 01.01.1973, CH	LEHERO	Toto	01.01.1973	CH	Male
...						

#### *Antécédents*

Pour les antécédents, peu importe le type, seuls les champs « techniques » important : *Domaine, Date, Source* et *Opération*.

<sup>334</sup> Les noms des fichiers image reproduits plus bas diffèrent. Les logiciels de *i2 inc.* contiennent les tables de conversion nécessaire. Voir par exemple l'Annexe I pour iBase™.

L'icône standard choisi est l'image « Cabinet », mais on peut aussi utiliser l'image « Telephone Tap »<sup>335</sup>.



Cabinet.bmp



Srvlanc1.bmp

Un exemple d'antécédent est reproduit dans la table suivante :

N° JANUS	Label	DOMAINE	Date	Source	Opération	Icône
117338	CE, 10.07.2006, VD pol. Sur - DAO, ZOOMOUT	CE	10.07.2006	VD pol sur - DAO	ZOOMOUT	Cabinet
...						

### Adresses

Pour les adresses, quatre colonnes sont malheureusement insuffisantes, il en faudrait cinq. Nous avons dû ignorer le code pays, comme nous sommes le plus souvent confrontés à des adresses suisses. Dans ce cas, nous avons donc conservé les informations suivantes : *NPA, Lieu, Rue* et *Numéro*.

Les images des icônes standards sont : « House », pour les adresses privées et « Building » pour les adresses professionnelles.



House.bmp



Building.bmp

Un exemple d'adresse est reproduit dans la table suivante :

N° JANUS	Label	NPA	Lieu	Rue	Numéro	Icône
123456	1014 LAUSANNE, Centre de la Blécherette 3	1014	LAUSANNE	Centre de la Blécherette	3	Building
...						

### Véhicules

Les véhicules ont, tout comme les moyens de communication et les comptes, des informations enchâssées (personne et adresse), lorsqu'ils sont mentionnés en tant que « sous-champs » ! Il s'agit dans la mesure du possible de détailler ces liens enchâssés.

Pour les véhicules, il faut mentionner : *No d'immatriculation, Marque, Modèle* et *Couleur*.

Les images des icônes standards sont « Car » pour les voitures, « Lorry » pour les camions, « Motorcycle » pour les motos et même « Cruiser » pour les bateaux. Afin de ne pas compliquer

<sup>335</sup> Cette image sera aussi utilisée pour la visualisation de JANUS JO 3.0

inutilement la visualisation, nous avons choisi d'utiliser l'image « Number Plate », pour ce qui est différent de ces 4 types.



Car.bmp



Lorry.bmp



Meycle.bmp



Cruiser.bmp



Nplate.bmp

Deux nouveaux liens doivent être introduits ensuite, selon les indications décrites précédemment, si une personne et une adresse sont mentionnées dans le « sous-champ ». Un exemple de véhicule avec les liens supplémentaires est reproduit dans la table suivante :

N° JANUS	Label	No d'immatr	Marque	Modèle	Couleur	Icône
654321	VD307107, Peugeot 107 jaune	VD307107	Peugeot	107	jaune	Car
	<i>LEHERO Toto</i>	<i>LEHERO</i>	<i>Toto</i>			<i>Male</i>
	<i>1014 LAUSANNE, CB 3</i>	<i>1014</i>	<i>LAUSANNE</i>	<i>CB</i>	<i>3</i>	<i>Building</i>
...						

### *Moyens de communication*

Pour les moyens de communication, ça se complique encore un peu, étant donné que les champs *IMEI* et *SIM* sont deux champs spécifiques et qui ne peuvent pas être utilisés comme identifiants. En conséquence ces informations ne sont que de simples indications.

Il s'agit donc de mentionner : *Numéro/adresse*, *Type*, *Prestataire* et *Moyen de communication*.

Le Champ *Moyen de communication* est utilisé pour déterminer l'icône qui sera utilisé. Pour les *Tel.Nr.*, il faut encore aller voir si le Type est *Mobile*. Les images des icones à utiliser sont donc : « Telephone », « Mobile Phone », « Email » et « Web Site ».



Phone.bmp



Cellphone.bmp



Email.bmp



WWW.bmp

Comme pour les véhicules, deux nouveaux liens doivent suivre, si une personne et une adresse sont mentionnées dans le « sous-champ ». Un exemple de moyen de communication est reproduit dans la table suivante :

N° JANUS	Label	Numéro/adresse	Type	Prestataire	Moy. comm.	Icône
321654	0790791702, Mobile Swisscom mobile	0790791702	Mobile	Swisscom mobile	Tel.Nr.	Cellphone
	<i>LEHERO Toto</i>	<i>LEHERO</i>	<i>Toto</i>			<i>Male</i>
	<i>1014 LAUSANNE, CB 3</i>	<i>1014</i>	<i>LAUSANNE</i>	<i>CB</i>	<i>3</i>	<i>Building</i>
...						

### Comptes

Pour les comptes, c'est très simple, puisque l'« attribut », comme le « sous-champ » n'ont que deux rubriques : *No compte* et *Nom de la banque*.

L'icône à prévoir est le suivant « Account », et si des cartes de crédit sont mentionnées ici (alors qu'elles devraient être des OBJ), on peut encore prévoir le suivant : « Credit Cards »



Account.bmp



Credit.bmp

Deux nouveaux liens devaient suivre, si une personne et une adresse étaient mentionnées, selon les indications décrites précédemment. Un exemple de compte est reproduit dans la table suivante :

N° JANUS	Label	Numéro/adresse	Nom de la banque	(...)	(...)	Icône
654123	267-1234567, BCV	267-1234567	BCV			Account
	<i>LEHERO Toto</i>	<i>LEHERO</i>	<i>Toto</i>			<i>Male</i>
	<i>1014 LAUSANNE, CB 3</i>	<i>1014</i>	<i>LAUSANNE</i>	<i>CB</i>	<i>3</i>	<i>Building</i>
...						

### Détail des liens

Pour les liens, la situation est bien plus simple. Les trois colonnes nécessaires dans la table doivent reprendre dans tous les cas la même structure : *Légende*, *Qualité*, *Couleur*.

La légende doit être reprise de rubriques des « attributs » ou des « sous-champs », si de telles informations sont prévues. La qualité permet de différencier les antécédents qui ne doivent pas être transmis (confidentiels). La couleur des liens est établie sur les bases d'un standard suisse issu du manuel d'analyse criminelle opérationnelle de l'OFP et des modèles échangés lors d'expériences communes.

Le tableau des données qui doivent être mentionnées dans les liens est le suivant :

<i>Entité A</i>	<b>Légende</b>	<b>Qualité</b>	<b>Couleur</b>	<i>Entité B</i>
<i>Personne / Org.</i>	JANUS PV	Confirmed	Red	<i>Antécédent (Pouvant être transmis)</i>
<i>Personne / Org.</i>	CONFIDENTIEL	Unconfirmed	Red	<i>Antécédent (Ne pouvant pas être transmis)</i>
<i>Personne / Org.</i>	REL	Confirmed	Blue	<i>Personne / Org.</i>
<i>Personne / Org.</i>	ALIAS	Confirmed	Aqua	<i>Personne (Alias)</i>
<i>Personne / Org.</i>	Type d'adresse	Confirmed	Olive	<i>Adresse (attribut)</i>
<i>Antécédent</i>	Rôle	Confirmed	Grey	<i>Adresse (s-champ)</i>

<b>Entité A (suite)</b>	<b>Légende</b>	<b>Qualité</b>	<b>Couleur</b>	<b>Entité B</b>
<i>Personne / Org.</i>	Rôle (attribut)	Confirmed	Navy	<i>Véhicule (attribut)</i>
<i>Antécédent</i>	Rôle (s-champ)	Confirmed	Grey	<i>Véhicule (s-champ)</i>
<i>Véhicule (s-champ)</i>	Rôle (s-champ)	Confirmed	Navy	<i>Personne / Org</i>
<i>Personne / Org.</i>	Rôle (attribut)	Confirmed	Maroon	<i>Moyen Com. (attribut)</i>
<i>Antécédent.</i>	Rôle (s-champ)	Confirmed	Grey	<i>Moyen Com. (s-champ)</i>
<i>Moyen Com. (s-champ)</i>	Rôle (s-champ)	Confirmed	Maroon	<i>Personne / Org</i>
<i>Personne / Org.</i>	Rôle (attribut)	Confirmed	Yellow	<i>Compte (attribut)</i>
<i>Antécédent</i>	Rôle (s-champ)	Confirmed	Grey	<i>Compte (s-champ)</i>
<i>Compte (s-champ)</i>	Rôle (s-champ)	Confirmed	Yellow	<i>Personne / Org</i>

### Synthèse

Ainsi en produisant un document tabulaire, pour chaque identité, en sélectionnant les antécédents qui nous intéressent, une visualisation relationnelle des éléments contenus dans JANUS PV devient possible en une seule étape d'importation-exportation. Ceci en tenant compte des liens directs et indirects par la différenciation des « objets » en « attributs » et « sous-champs ». Cette fonction de visualisation des informations introduites dans JANUS PV 2.0, doit tenir compte des liens indirects de différents niveaux et correspondre aux standards déjà établis au niveau suisse.

L'utilisation d'un fichier d'échange tabulaire plutôt que d'un fichier en XML est privilégiée, étant donné le niveau informatique moyen des analystes criminels et policiers formés à cette discipline.

De la sorte, la quasi-totalité des informations réellement utiles à une visualisation doit être disponible dans une table facilement récupérable pour une réimportation dans le système de visualisation graphique.

Le modèle de la représentation graphique telle que décrite en détail dans les pages précédentes est reproduit à la page suivante :

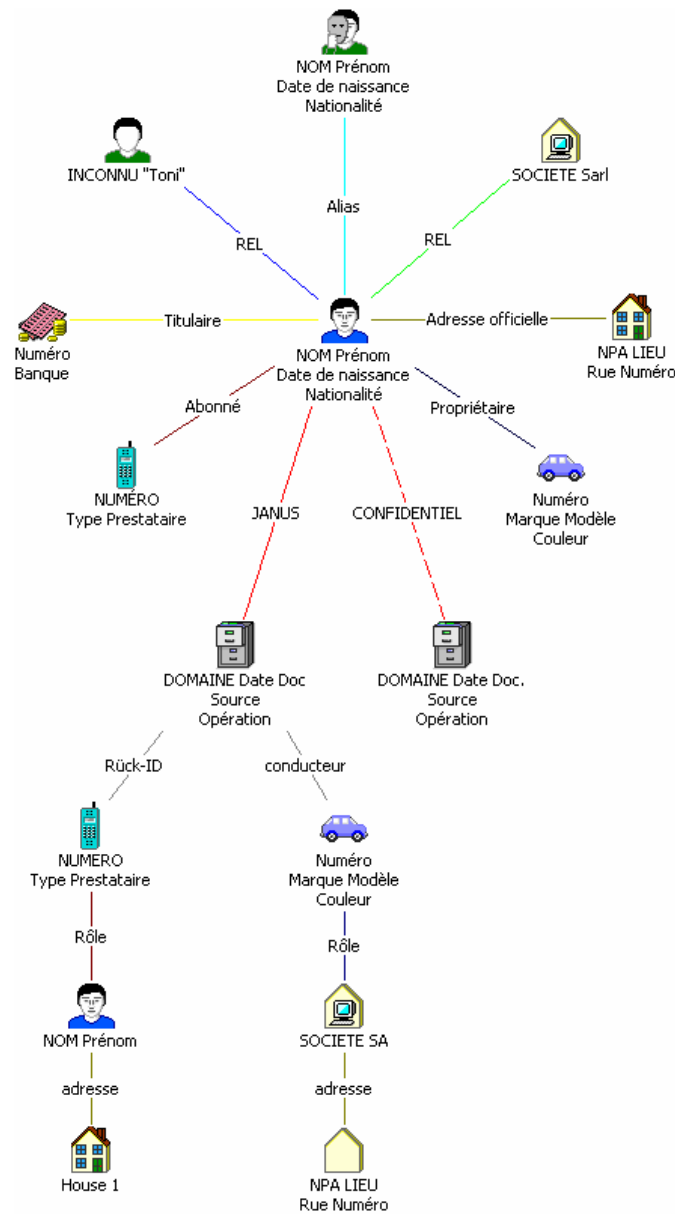


fig. 168 : Modèle de représentation des liens de différents niveaux dans JANUS PV 2.0

### 3.4.1.2 Relation avec d’autres systèmes d’information

Comme nous l’avons mentionné plus avant, les relations avec d’autres systèmes d’information, que ce soit des systèmes d’analyse ou des systèmes d’information de police exploités dans les cantons, ont été discutées en détail lors de l’élaboration du cahier des charges lors des séances du groupe de travail. Cependant, la réalisation de ces fonctionnalités a connu des retards suffisamment importants.

A fin 2008, il n’existait réellement aucune relation effective de JANUS PV 2.0 avec d’autres systèmes d’information, alors que le système était en fonction depuis plus de trois ans. L’effort de développement a été mis entre 2005 et 2007 sur le second « sous-système » de JANUS (JO), ce qui a amené en 2007 à la réunion des deux « sous-systèmes » et la version 3.0 de JANUS.

Des interfaces avec les systèmes POLIS (ZH) et ABI (autres cantons) ont enfin vu le jour en 2009, mais ce n'est que pour importer des données dans JANUS et pas le contraire.

### 3.4.2 Importation XML dans *iBase*<sup>TM</sup>

Cette possibilité existe, mais il faut bien avouer qu'elle est assez limitée. Ceci pour deux raisons.

La première est le type d'importation qu'*iBase*<sup>TM</sup> propose. En effet, *iBase*<sup>TM</sup> laisse le choix à l'utilisateur, à l'instar des importations classiques dans l'*Analyst's Notebook*<sup>TM</sup>, d'importer soit des entités, soit des liens avec les deux entités qui y sont jointes. Si dans l'*Analyst's Notebook*<sup>TM</sup>, l'importation de fichiers XML laissait entrevoir la possibilité d'importer en une seule phase des entités et des liens, quels que soit leurs types et leurs nombres, il n'en est pas de même avec *iBase*<sup>TM</sup>. Dans ce logiciel les importations globales ne sont simplement pas possibles. Il faut donc prévoir des importations multiples (en plusieurs phases), soit une par type de lien présent. *iBase*<sup>TM</sup> facilite toutefois ce laborieux travail en permettant de conserver les caractéristiques de ces importations récurrentes (*import batch specifications*).

La seconde limitation de l'importation de données XML dans *iBase*<sup>TM</sup> est le schéma des données issu d'une base d'analyse. Le schéma que crée la base de données se fonde sur le modèle de Microsoft appelé *XML Rowset Schema*. Ce schéma « réduit » est spécifique et il crée dans la première partie du document les types de données et les caractéristiques du schéma (telles que les valeurs par défaut, les clés primaires, etc.). Un processus similaire extrait ensuite les données à placer dans le document XML.

Les schémas sont donc non seulement spécifiques à la structure de la base de données, mais également selon une grammaire « simplifiée », issue du *XML Reduced Data Schema* de Microsoft.

Cette grammaire « simplifiée » implique par exemple que l'en-tête du document XML qui ne concerne que le lien PERSONNE – ANTECEDENT de notre prototype de base d'analyse représente 200 lignes de code dont nous vous faisons grâce de son intégralité.

```
- <xml xmlns:s="uuid:BDC6E3F0-6DA3-11d1-A2A3-00AA00C14882" xmlns:dt="uuid:C2F41010-65B3-11d1-A29F-00AA00C14882" xmlns:rs="urn:schemas-microsoft-com:rowset" xmlns:z="#RowsetSchema">
- <s:Schema id="RowsetSchema">
- <s:ElementType name="row" content="eltOnly">
- <s:AttributeType name="Domaine" rs:number="1" rs:nullable="true" rs:maydefer="true"
  rs:writeunknown="true">
  <s:datatype dt:type="string" dt:maxLength="255" />
  </s:AttributeType>
- <s:AttributeType name="Date" rs:number="2" rs:nullable="true" rs:maydefer="true" rs:writeunknown="true">
  <s:datatype dt:type="dateTime" rs:dbtype="variantdate" dt:maxLength="16" rs:fixedlength="true" />
  </s:AttributeType>
  ...
  <s:extends type="rs:rowbase" />
</s:ElementType>
</s:Schema>
</xml>
```

Le contenu d'une information étant ensuite beaucoup plus restreint, les balises correspondant aux champs de la base de données étant remplacées par des attributs XML [c1... cn]. Voici un exemple :

```
<xml xmlns:s='uuid:BDC6E3F0-6DA3-11d1-A2A3-00AA00C14882'
:dt='uuid:C2F41010-65B3-11d1-A29F-00AA00C14882'
:rs='urn:schemas-microsoft-com:rowset'
:z='#RowsetSchema'>
<rs:data>
<z:row Source='JANUS' Direction='0' Strength='0' c6='Male' c7='-' c8='NOM PERSONNE' c9='Prénom Personne'
c11='1980-03-03T00:00:00' c12='France' c14='France' c15='Algérie' c16='Masculin' c17='Concubin' c18='NOM DU
PERE' c19='Prénom du père' c20='NOM DE LA MERE' c21='Prénom de la mère' c24='Rapport F' c25='F' c26='True'
c27='True' c28='False' c32='JANUS' c33='Headphones' c34='-' c35='2002-10-10T00:00:00' c36='True' c37='True'
c38='CE' c39='True' c40='Enquête' c41='True' c42='VD+' c44='VD+ BE+ GE+' c45='VD+ pol sur / DCI' c46='PE02.
...' c47='AGRUME' c54='CT / CTR' c55='Texte de l'antécédent pouvant être relativement long et se trouver sur
plusieurs pages, évidemment.'/>
</rs:data>
</xml>
```

Un des désavantages principaux du langage XML est qu'il peut-être terriblement bavard, étant donné qu'il s'autoréférence. L'utilisation d'un modèle de données permet de ne pas l'inclure au document comme c'est le cas avec le *XML Rowset schema* de Microsoft. Ici, les 6 premiers éléments du modèle font référence au lien entre la PERSONNE et son ANTECEDENT, les 26 suivants à l'entité PERSONNE et les 23 derniers à l'entité ANTECEDENT.

Or, la description du schéma en début de document est absolument nécessaire à tout document qui veut être utilisé pour l'importation. Il est nécessaire à la transformation (mappage = descriptif de la structure) du document pour pouvoir l'importer dans la base de données relationnelle. Et comme on l'a vu, cet en-tête est relativement conséquent. L'assistant d'importation *iBase™* est capable de déterminer ensuite la position relative des informations, comme le montre la figure ci-dessous :

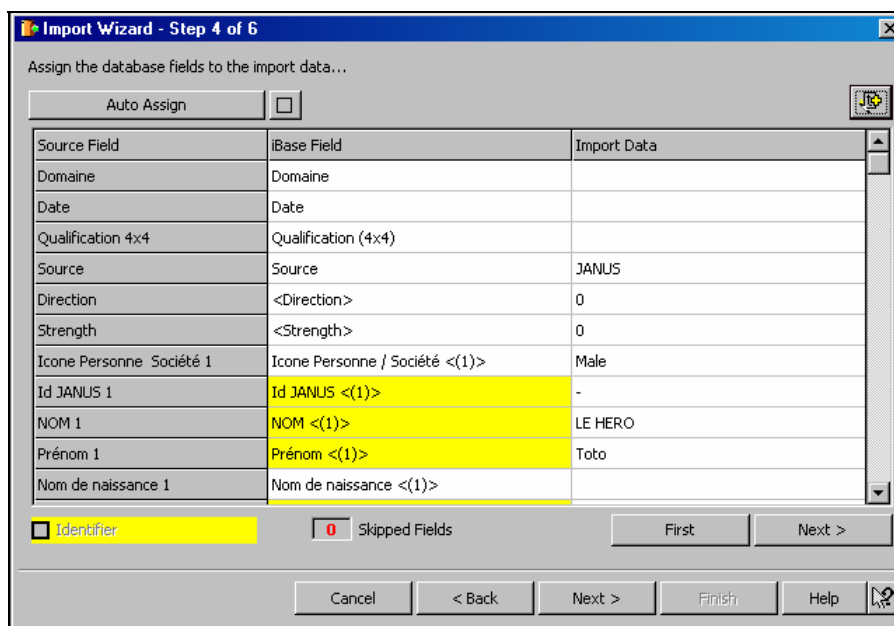


fig. 169 : Vue de l'assistant d'importation de *iBase™* 4, en-tête XML présent et compatible.



### 3.4.3 Traitements XML

Comme nous n'avons pas reçu de données provenant de la base de mémoire à long terme, il ne nous a pas été possible de détailler et de proposer un parseur XML (processeur de feuille de style), qui permette de traduire un document XML issu de JANUS PV 2.0 en un nouveau fichier compatible avec le *prototype  $\beta$* , notre composant d'analyse.

La phase de réalisation du projet s'arrête donc ici. Nous espérons toutefois pouvoir réaliser cette dernière étape dans les années futures.

### **3.5 Résultats de la mise en œuvre**

Cette dernière partie de la réalisation du projet présente succinctement quelques situations pratiques qui ont bénéficié de l'un ou l'autre des composants du projet, puis des deux, bien qu'ils n'aient pas pu être interconnectés de manière complète et satisfaisante. Les contraintes qui ont influencé la faisabilité du projet seront abordées dans la première partie de la discussion.

#### **3.5.1 Composant mémoire à long terme**

JANUS PV 2.0 a donné satisfaction aux enquêteurs dès les premiers mois d'exploitation. Dans un premier temps, la facilité de navigation et la convivialité du nouveau système ont immédiatement reçu la faveur des utilisateurs. Par la suite, ceux-ci se sont rendu compte que les autres fonctionnalités avaient également évolué dans un sens positif. La vitesse des *comparaisons* a notamment été appréciée.

Les premières expériences concrètes que nous avons pu faire au sein de la police de sûreté vaudoise n'ont pas été particulièrement différentes de ce que nous connaissions avec l'ancien JANUS PV. La méthode de travail était restée la même, les changements se faisaient tout en douceur.

##### **3.5.1.1 Enquête B&W**

Nous pouvons relater ici une des enquêtes qui s'est déroulée entre fin 2005 et début 2006. Le départ de cette investigation est justement dû à JANUS PV et les renseignements qu'il est possible d'en tirer en utilisant les liens générés par le système et en valorisant les éléments découverts, sans qu'ils soient l'objet des premières investigations. Nous appellerons cette enquête B&W, en référence au nom donné à l'opération par l'enquêteur principal.

L'origine de cette investigation est donc un constat qui a été fait par des enquêteurs grâce à JANUS PV, qui trouvaient très souvent un même numéro de téléphone dans les données téléphoniques récupérées lors des contrôles effectués sur des trafiquants de cocaïne. Cependant, lors des écoutes en direct, l'utilisateur de ce numéro n'apparaissait jamais en lien direct avec un quelconque trafic de stupéfiants.

L'une des hypothèses développées par ces enquêteurs était que l'utilisateur de ce raccordement mobile pouvait servir de soutien logistique aux trafiquants. Ce renseignement a alors été transmis et exploité par le groupe spécialisé de la brigade financière de la police de sûreté vaudoise (DCO<sup>336</sup>), qui a fait un rapport préliminaire à un juge d'instruction vaudois en vue de faire ouvrir une enquête et d'obtenir ensuite une surveillance rétroactive sur le numéro suspect, afin de vérifier les premiers soupçons.

Une enquête a donc été ouverte par le magistrat vaudois et les données téléphoniques rétroactives ont été obtenues auprès de l'opérateur de téléphonie mobile. Leur exploitation à l'aide des outils

---

<sup>336</sup> Division criminalité organisée (DCO)

d'analyse criminelle<sup>337</sup> ont rapidement permis de confirmer les soupçons, la comparaison JANUS PV étant particulièrement intéressante. A ce stade, un schéma relationnel a été établi manuellement à l'aide de l'*Analyst's Notebook*<sup>TM</sup>.

Un nouveau rapport intermédiaire était produit, afin de demander au magistrat instructeur une écoute en direct, celle-ci devant permettre d'identifier la personne suspecte<sup>338</sup>, d'établir l'étendue de ses activités délictueuses et de ses contacts, et finalement, de permettre son interpellation.

Cette nouvelle mesure coercitive était également ordonnée par le juge et les premières semaines d'écoutes permirent de confirmer la nature délictueuse des liens qui avaient été établis par les contacts détectés entre des trafiquants de stupéfiants et l'activité de blanchisseur du suspect. Son identité a pu être déterminée, bien qu'il habitât clandestinement dans un logement officiellement inscrit au nom d'un compatriote.

Enfin, les contours d'un réseau de rapatriement de fonds d'origine criminelle ont pu être dessinés et transmis au magistrat instructeur. A ce stade de l'enquête, un nouveau schéma était produit manuellement.

Dès lors, une question de compétence s'est posée au niveau de l'autorité d'instruction. La problématique énoncée au chapitre 1.1 et plus particulièrement au sens de l'art 340<sup>bis</sup> du code pénal<sup>339</sup>, soit les infractions relevant du blanchiment d'argent et de soutien et d'appartenance à une organisation criminelle. Le magistrat vaudois a donc demandé, comme il se doit, une détermination au Ministère Public de la Confédération (MPC). Celui-ci répondait que la compétence était bien fédérale, le dossier devait donc être transmis à un procureur fédéral qui déléguerait naturellement une partie du travail d'enquête à la police judiciaire fédérale (PJF).

Les faits se passant principalement en Suisse romande (Vaud et Genève) et en France, ce fut l'antenne de la PJF de Lausanne qui reprit l'affaire, et en fin de compte, dans un souci d'efficacité, une task-force fut créée avec les nouveaux éléments de la PJF et l'équipe de la DCO vaudoise déjà en charge de l'enquête.

Dans cette phase de reprise de l'enquête par une juridiction différente (cantonale - fédérale), l'utilisation de JANUS comme base de données d'enquête a joué un rôle prépondérant. En effet, toutes les données introduites par les Vaudois au début de l'enquête ont été directement disponibles aux enquêteurs fédéraux, une fois les droits d'accès à ces données mis à jour. Mieux, ce système étant utilisé quotidiennement par les deux organisations, la continuité était assurée, les enquêteurs utilisant les mêmes outils. Sans JANUS, la reprise de l'enquête aurait été extrêmement difficile. Les

---

<sup>337</sup> Voir chapitre 1.4.6.2 – Les analyses de contrôles techniques

<sup>338</sup> Il faut préciser ici que même si depuis 2002, les cartes téléphoniques prépayées doivent être enregistrées lors de l'achat, la revente entre particuliers n'est pas illégale. Parallèlement, les requérants d'asile n'ont plus été autorisés à utiliser leur permis de séjour comme justificatif. Naturellement, un important marché gris s'est donc rapidement développé, permettant ainsi, malgré tout, aux délinquants de disposer de cartes SIM sans aucun rapport avec leur identité réelle.

<sup>339</sup> Voir 1.1.4.2 – Survol de l'état de la lutte contre la criminalité organisée en Suisse – Au plan de la procédure

enquêteurs fédéraux auraient dû réintroduire toutes les données vaudoises dans leur propre système de gestion des informations, ce qui aurait été long, fastidieux, peu productif, et cela aurait largement compromis le succès de l'affaire, le temps nécessaire à la reprise des informations pénalisant directement le suivi des événements et la compréhension des développements quotidiens obtenus par l'écoute téléphonique en direct.

Après plusieurs mois d'enquête, la taille, l'organisation et le fonctionnement du réseau était connu. Le schéma établi précédemment par les enquêteurs vaudois était mis à jour par les membres de la task-force. Dans les grandes lignes, il s'agissait de deux structures de récolte d'argent sale localisées en Suisse romande, l'une à Lausanne et l'autre à Genève. Ces structures étaient composées de quelques personnes, seulement. Les fonds récupérés étaient rapatriés vers le pays d'origine des auteurs, des voyages de ressortissants de ce pays étaient organisés pour ramener les fonds récoltés en Suisse au pays. Ces fonds devaient d'abord transiter par les résidences officielles en France voisine, de certains membres du réseau qui résidaient clandestinement en Suisse. Les fonds étaient collectés jusqu'à ce qu'une somme justifiant un voyage soit amassée. Les transferts d'argent liquide étaient effectués principalement par des passeurs au départ des aéroports internationaux français. En cours d'enquête, l'interception de plusieurs « mules » lors de leur passage de la frontière a permis la saisie de plus d'un demi-million de francs suisses.

Finalement, les auteurs principaux à Lausanne et à Genève ont pu être arrêtés simultanément et des perquisitions ont été ordonnées jusqu'en France voisine.

Dans cette affaire, l'utilisation de JANUS a été une des clés du succès de la première phase de l'enquête, soit la recherche d'infractions, suivie de la recherche et de l'identification des suspects. Sans cette base de données commune, la transmission de l'affaire des enquêteurs vaudois aux autorités judiciaires fédérales aurait vraisemblablement compromis la réussite des investigations. De plus, la création d'un groupe d'enquête mixte regroupant des policiers cantonaux et fédéraux a été possible grâce à l'unité de doctrine de travail déjà présente due à une formation en analyse criminelle standardisée au plan suisse et à l'utilisation d'outils communs comme JANUS et l'*Analyst's Notebook*<sup>TM</sup>. A titre illustratif, le nombre d'éléments d'enquête saisis dans JANUS avant les interpellations des membres du réseau ont été les suivants : 6 relevés de facturation (CT rétroactif), représentant env. 40'000 connexions téléphoniques ; 4 écoutes en direct, représentant env. 8'000 communications intégralement traduites et retranscrites ; plus pléthore d'éléments d'enquête divers.

Il faut encore ajouter à cela deux écoutes en direct effectuées par voie de commission rogatoire en France et dont les contenus ne nous étaient pas intégralement transmis.

Dans cette affaire, le composant d'analyse (base de données *iBase*<sup>TM</sup>) n'a pas été utilisé. La raison était simplement l'impossibilité technique d'extraire les données de JANUS PV 2.0. De plus, l'ampleur du réseau était relativement restreint et son fonctionnement assez simple à cerner. Des

méthodes de visualisation manuelles classiques ont donc été suffisantes pour cette enquête, bien que beaucoup de ressaisie d'informations ait été nécessaire.

### 3.5.2 Composant analyse

Très rapidement, l'utilisation de composants de base de données d'analyse s'est avérée utile dans la pratique de l'analyse criminelle opérationnelle. Les situations qui nécessitaient l'utilisation d'un tel outil ne sont pas des plus fréquentes, mais dans ces cas-là, peu d'alternatives existent.

Une première base d'analyse a été développée dans le cadre d'exercices organisés au sein du service de sécurité de la police militaire (S Séc PM)<sup>340</sup>. L'intégration d'une base de données d'analyse comme base de renseignements de la centrale d'engagement (ou de l'état-major de conduite) d'un détachement a considérablement augmenté la qualité de l'appréciation de situations évoluant très rapidement et a certainement contribué aux succès répétés des exercices dans lesquels elle a été utilisée. La mise en place d'une telle base de données a bien sûr nécessité des aménagements dans le fonctionnement plus traditionnellement militaire d'un état-major de conduite. Ces aménagements ont toutefois été relativement peu contraignants et ont pu être mis en place avec succès dès le premier exercice, bien qu'une très grande attention doive être portée à la transmission interne de l'information.

Aujourd'hui, un système informatisé est à l'étude, ce qui devrait ouvrir de nouvelles perspectives, et améliorer la célérité du flux de l'information.

La figure de la page suivante décrit le circuit de l'information au sein de l'état-major de conduite.

Pour des raisons évidentes, nous ne nous étendrons pas ici sur le contenu des exercices et les bénéfices précis qui ont pu être retirés d'une telle intégration d'un composant d'analyse opérationnelle dans une telle structure de conduite. Mais il est toutefois possible de relever que lors de la réforme *Armée XXI*, la sécurité militaire a également subi une réforme de fond, qui a touché le SSPM<sup>341</sup>, devenant le S Séc PM. Si ses missions et la qualité de ses effectifs sont restées inchangés, les quatre détachements territoriaux actifs jusqu'alors ont été regroupés en une seule unité nationale. Durant cette réorganisation, c'est le modèle de fonctionnement décrit ci-dessous et qui avait été introduit dans le détachement romand qui a été choisi pour le S Séc PM.

---

<sup>340</sup> Le service de sécurité de la police militaire (S Séc PM), qui fait partie des services spéciaux de la police militaire, est une formation mixte, composée de militaires professionnels et de militaires de milice. Lorsque l'armée est mise sur pied pour un service d'appui ou un service actif, il apprécie la situation militaire en matière de sécurité et il prend des mesures préventives pour assurer la sécurité de l'armée contre l'espionnage, le sabotage et contre d'autres activités illicites. Il prend aussi des mesures préventives pour protéger les engagements suisses à l'étranger (cf. art 100 de la LAAM - RS 510.10).

<sup>341</sup> Avec *Armée 95* le S Séc PM était abrégé SSPM.

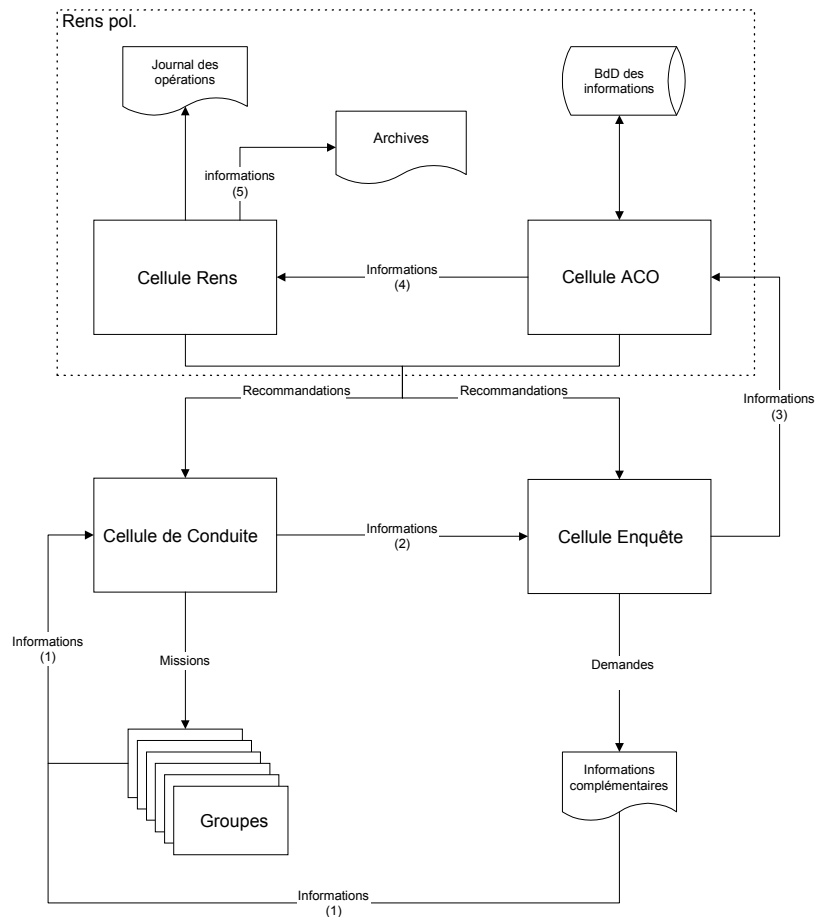


fig. 170 : Schéma du flux d'information au sein d'un EM de conduite incluant un composant d'analyse

Après une phase de création et de consolidation de la nouvelle structure nationale, les premiers exercices complets, incluant l'ensemble du détachement, y compris son état-major de conduite, ont eu lieu en 2006. La principale difficulté résidant désormais non pas dans le regroupement de plusieurs groupes linguistiques avec leurs méthodes et sensibilités différentes comme on aurait pu le penser, mais principalement dans la quantité d'informations à traiter par une centrale d'engagement encore largement sous-équipée en matériel et en ressources humaines.

Ces différentes expériences recueillies dans le cadre d'exercices depuis 2001 ont permis d'acquérir la certitude que ce type de base de données d'analyse pouvait avoir sa raison d'être dans le cadre de la lutte contre la criminalité organisée. Cependant, sa mise en place nécessite une logistique suffisamment importante pour être réfléchi *a priori*. C'est pourquoi elle n'a été mise en œuvre que dans le cadre de certaines opérations bien précises au sein de la police de sûreté vaudoise, alors qu'elle était déjà mise à disposition des enquêteurs à la police judiciaire fédérale au tournant du millénaire.

### 3.5.2.1 Opération DK

Un composant d'analyse très proche du modèle final du *prototype β*, tel qu'il vous a été présenté au chapitre 3.3, a été utilisé dans le cadre d'une opération qui débuté en 2004 et qui est toujours active, que l'on appellera DK.

Cette opération, à l'inverse de la situation de la sécurité militaire où de très nombreuses informations parvenaient dans un temps très court, consiste en la récolte systématique d'éléments issus de l'activité judiciaire ordinaire cantonale, dans le but de rechercher des indices permettant de vérifier si un secteur d'activités commerciales était en train d'être petit à petit infiltré par des personnes en lien étroit avec la criminalité organisée. Ces activités commerciales pouvaient ensuite être utiles pour le blanchiment d'argent, par l'investissement de fonds d'origine criminelle au sein de sociétés officiellement enregistrées. Différents signaux avant-coureurs étaient perceptibles et la décision de mener cette concentration d'information a été prise par l'état-major de la police de sûreté vaudoise.

Un groupe d'enquêteurs issus des différentes brigades spécialisées (stupéfiants, mœurs, financière) était réuni, sous la direction du chef de la division criminalité organisée, avec l'appui des membres de la division d'appui opérationnel de la BAAC<sup>342</sup>, dont font désormais partie les spécialistes en analyse criminelle.

Les répondants des brigades spécialisées avaient pour mission de recueillir, évaluer et étayer les informations issues de leurs propres domaines de compétence et de les transmettre en cas de nécessité.

Afin que ces renseignements soient accessibles à tous les membres de la police cantonale, une main courante était ouverte dans le sous-système JANUS JO. Toutes les informations y étaient introduites sous une forme textuelle. Les entités tels que des personnes, sociétés, lieux, numéros de téléphones et plaques numéralogiques étant accessibles rapidement par des recherches spécifiques.

Parallèlement, la division d'appui opérationnel avait pour mission d'alimenter une base d'analyse *iBase™* à l'aide des informations figurant dans les notes de main courante.

Après la première année de fonctionnement de cette petite structure transversale, le bilan était le suivant :

- Sur le plan opérationnel, deux groupes principaux distincts géographiquement et selon l'origine des ressortissants apparaissaient. Ils se trouvaient, sans surprise, au sein des plus grandes agglomérations du canton.
- Sur le plan organisationnel, le groupe DK disposait des effectifs suffisants pour la collecte des renseignements. Des contacts plus ténus étaient toutefois nécessaires avec la police judiciaire du

---

<sup>342</sup> BAAC : Brigade d'Appui, d'Analyse et de Coordination. Cette brigade, née en 2005 de la réunion des divisions d'appui opérationnel et de coordination judiciaire, est rattachée à la section commandement de la Police de sûreté.

chef-lieu, ainsi qu'avec les polices du commerce (cantonale et communale) qui disposent de nombreuses informations administratives utiles.

- Au niveau de la base d'analyse, 44 notes de main courante étaient à la source de l'introduction de 700 informations structurées, soit 300 personnes, 50 sociétés, 120 événements et 250 entités diverses (téléphones, véhicules, etc.).

Sur la base de ce constat, l'état-major prenait la décision de poursuivre l'opération en renforçant la publicité interne de l'opération, afin de recueillir un maximum d'informations et de mener lorsque cela était possible des actions ponctuelles et superficielles sur des membres actifs de ces réseaux afin de compléter les renseignements déjà en notre possession. Le but étant d'amener le réseau à se réorganiser et à commettre des erreurs permettant de mettre à jour le cœur de leurs activités criminelles.

L'intérêt de l'analyste à ce niveau se portait bien entendu aussi sur la méthodologie mise en place et sur le fonctionnement à moyen terme de ce type de groupe d'enquête ad hoc. A ce stade un certain nombre d'observations étaient intéressantes.

- La saisie des informations dans JANUS devait se faire de manière décentralisée, c'est à dire par les répondants. Ceux-ci avaient aussi la possibilité d'interroger directement la base d'analyse et s'ils le désiraient d'y saisir les informations de leur main courante. Or, dans les faits, il est rapidement apparu que la saisie de la main courante se reportait sur la division d'appui opérationnel et plus particulièrement sur son personnel administratif spécialement formé à ce type de travail. De plus, ce personnel devait assumer la saisie des informations dans la base de données d'analyse.
- Les informations recueillies au début de l'opération avaient donné une image de la situation après quelques mois qui n'évoluait guère par la suite. Les informations supplémentaires ne faisant que corroborer et renforcer l'image préliminaire. Cet état de fait nous amenait à nous poser la question de savoir si nous étions trop focalisés sur les mêmes personnes suspectes ou s'il s'agissait réellement de la réalité.

En ce qui concerne la saisie des informations, on remarque que pour des opérations à moyen ou long terme, il est indispensable de disposer de personnel dédié à l'intégration et à l'analyse des informations. De manière générale, les enquêteurs ne disposent pas des compétences, des ressources et du temps nécessaires à ces activités. Cette remarque était aussi valable dans le cadre des exercices effectués au sein de la police militaire.

En conclusion, l'utilisation du composant d'analyse permet, en tout temps, d'obtenir une image de la situation, qu'elle soit globale ou spécifique à un acteur ou à un groupe. Cette base de données d'analyse confinée à une unité d'enquête particulière est également parfaitement adaptée aux



besoins des différents intervenants, qu'il s'agisse d'enquêteurs, d'analystes ou d'opérateurs de saisie.

### 3.5.3 Système interconnecté

Bien que l'interconnexion n'ait pas pu être complètement réalisée pour des raisons plus techniques que méthodologiques, un test a été réalisé, en réintroduisant aussi fidèlement que possible les données qui étaient contenus dans JANUS PV et qui pouvaient être utiles à l'affaire traitée à l'aide de ces outils.

Le problème de l'interconnexion des deux composants n'est pas surprenant. Les projets d'envergure qui regroupent de nombreuses entités différentes, avec des buts différents recherchés par des groupes d'utilisateurs dissemblables<sup>343</sup>, n'aboutissent souvent jamais réellement. Le groupe le plus fortement représenté ou les fonctionnalités les plus urgentes l'emportent sur des besoins souvent novateurs, mais plus complexes à réaliser.

Les travaux entrepris au sein du groupe de travail, ainsi que la réalisation du composant d'analyse permettraient de travailler avec deux composants interconnectés, si cette dernière interface était fonctionnelle.

#### 3.5.3.1 Affaire VO

L'affaire qui a été traitée en simulant une interconnexion des deux systèmes découle naturellement de l'opération DK évoquée juste précédemment. En effet, lors de la recherche de renseignements de police dans ce domaine commercial précis, des indices de potentiel blanchiment d'argent ont été mis à jour. Nous ne reviendrons pas ici, à nouveau, sur les innombrables problèmes de détermination de compétence entre les autorités de poursuite pénales cantonales et fédérales, mais ce processus dans ce cas d'espèce a duré environ une année. Ce n'est qu'à l'été 2006 que cette affaire a réellement connu sa phase opérationnelle. Jusqu'ici, seuls des contacts avec des représentants d'autorités étrangères avaient été entrepris, afin de pouvoir qualifier la nature des fonds amenés par le principal suspect.

Ces éléments en provenance du pays d'origine du suspect ont permis de confirmer la nature plus que suspecte des fonds investis. Malheureusement, cet homme est retourné à ce moment dans son pays et il ne revenait plus que sporadiquement en Suisse. C'est lors de l'un de ses passages éclairés qu'il a été interpellé.

En conséquence, le développement que nous désirions donner à l'affaire n'a pas été possible et c'est dans une phase relativement statique que les opérations ont eu lieu. Il n'a donc pas été possible de juger dans ce cas précis des avantages du système complet (bien que fonctionnant en mode « manuel ») et de ses inconvénients. C'est le lot de tout enquêteur qui n'est pas maître des événements.

---

<sup>343</sup> Voir chapitre 3.2 – Les besoins de chaque intervenant (enquêteur – analyste)



## 4 Evaluation des résultats et discussion

Lors des précédents chapitres, nous avons abordé la problématique de la lutte contre la criminalité organisée en Suisse et les changements récents de la politique criminelle de ce pays, qui ont amené des modifications législatives dans les années 1990 par l'ajout dans le code pénal notamment de l'article punissant l'appartenance ou le soutien à une organisation criminelle (art 260<sup>ter</sup> CPS), puis au début des années 2000 de l'attribution des compétences d'enquête à une juridiction fédérale au sens de l'article 340<sup>bis</sup> CPS. Parallèlement, les structures des organisations répondant de la juridiction fédérale, soit le Ministère public de la Confédération (MPC) et l'Office fédéral de la Police (OFP) devaient s'adapter en conséquence et subissaient une mue importante, par la création de deux entités distinctes : le service d'analyse et de prévention (SAP) et la police judiciaire fédérale (PJF). Des crédits substantiels étaient votés par le Parlement et le projet d'efficacité devait permettre d'atteindre les objectifs fixés initialement, par des *mesures tendant à l'amélioration de l'efficacité et de la légalité dans la poursuite pénale*. Le plan de mise en œuvre (Rapport conceptuel de l'an 2000) partait du principe que toutes les procédures devaient pouvoir être traitées et que les effectifs du personnel devaient suivre l'accroissement de leur nombre. D'après ce rapport, les autorités de poursuite pénale de la Confédération auraient dû recevoir 804 postes au total d'ici à 2005.

Ces procédures étant nouvelles, leur mise en place a parfois créé des problèmes, par exemple au niveau de la définition de la compétence fédérale, de la double instruction (instruction préparatoire du MPC, avant la transmission à un Juge d'instruction fédéral) ou encore de la délimitation des responsabilités entre le MPC et la PJF lors de l'enquête préliminaire<sup>344</sup>. Le programme d'allègement budgétaire 03 a mis fin à ce développement. Ainsi, seuls 577 postes ont été créés, soit 227 de moins que prévu par le rapport conceptuel.

En filigrane de ces problèmes structurels, des difficultés méthodologiques étaient déjà mises en évidence dans le rapport de situation 2000 de l'OFP, qui relevait le manque d'intégration de l'analyse criminelle dans les enquêtes<sup>345</sup>. S'il était difficile d'appliquer ces méthodes, il pouvait y avoir plusieurs raisons.

Une première cause pouvait être la formation insuffisante du personnel. Or, les offices centraux, puis la PJF ont disposé dès le départ d'un certain nombre de collaborateurs formés en analyse criminelle. Ceux-ci faisaient même partie du groupe suisse de référence et étaient eux-mêmes des formateurs sur le plan suisse.

Une deuxième raison pouvait être que les outils à disposition ne permettaient que difficilement d'appliquer les méthodes d'analyse criminelle. Sur ce point précis, si des logiciels spécifiques d'analyse criminelle étaient à la disposition des analystes, les bases de données d'enquête devant

<sup>344</sup> Voir à ce sujet les rapports USTER et LUTHI, 2007, *op. cit.*

<sup>345</sup> Voir chapitre 1.1.4 – Survol de la lutte contre la criminalité organisée en Suisse

leur faciliter le travail ne permettaient d'appliquer les méthodes que très partiellement et au prix de trop nombreux efforts<sup>346</sup>.

Le but de cette présente recherche était donc de profiter des évolutions positives des cadres politiques, légaux, économiques et dans une moindre mesure organisationnels pour proposer une méthode de travail qui s'inspire et tienne compte intimement de l'analyse criminelle, et qui favorise son intégration dans les enquêtes relatives à la criminalité organisée. Le système bi-composant proposé pouvait ainsi autant profiter aux autorités de poursuite pénales de la juridiction fédérale luttant contre la criminalité organisée qu'aux cantons, de par la portée du système JANUS d'ores et déjà commun à ces différentes entités.

Ce chapitre va donc dans un premier temps discuter des hypothèses posées lors de la définition du projet de thèse.

La première hypothèse H1<sup>347</sup> traitant de la faisabilité du projet, des difficultés rencontrées et qui n'ont pas permis la finalisation du projet est reprise et discutée dans la première partie de ce chapitre.

La deuxième partie se concentre sur la discussion de la plus-value du système, soit de son utilité au sens de la seconde hypothèse H2<sup>348</sup>. Son efficacité est estimée en se basant sur des résultats empiriques et sur l'évolution de la situation au niveau de la lutte contre la criminalité organisée, selon la méthode d'évaluation pragmatique décrite au chapitre 2.6.1.

Enfin, la dernière partie est réservée à certaines perspectives dans la phase d'analyse qui produit la valeur ajoutée dans le cycle du renseignement<sup>349</sup>. En effet, si la réalisation technique de cette recherche se focalise sur les phases de collecte, d'intégration et de traitement, il ne faut pas omettre de discuter la phase d'analyse. Cette phase critique fait appel à de perpétuels allers-retours entre des raisonnements progressifs (synthétiques) ou régressifs (analytiques). Certains pièges cognitifs connus y sont décrits et des moyens d'encadrer formellement cette phase délicate où se mêlent les faits et la subjectivité de leur interprétation y sont proposés. Le recours à une *matrice d'analyse bayésienne d'hypothèses concurrentes* originale est ainsi présentée. Puis, pour terminer, les possibilités futures de l'automatisation de cette phase analytique sont discutées.

---

<sup>346</sup> Voir chapitre 2.5.4 – Synthèse (hypothèse 1)

<sup>347</sup> H1 : *Il est possible de coupler aux bases de données centralisées un composant d'analyse externe évolutif qui intègre des systèmes de représentation graphique, dans le but d'analyser les relations complexes de la criminalité organisée.*

<sup>348</sup> H2 : *L'utilisation des méthodes d'analyse criminelle, à l'aide d'un composant d'analyse externe couplé aux bases de données d'enquête centralisées et par conséquent compatible avec la structure des informations qui y sont contenues, est utile à l'investigation dans le cadre de la criminalité organisée.*

<sup>349</sup> Voir chapitre 1.4.5 – La méthode de travail

## 4.1 *Faisabilité du projet*

Le projet<sup>350</sup> décrit dans les termes présentés à la fin du chapitre 2 a été déposé en juin 2002 et défendu en mai 2003. La partie pratique voulait profiter de la possibilité offerte par la refonte du système JANUS PV, ce qui devait permettre de placer à l'endroit opportun un composant d'analyse qui faisait selon nous défaut en Suisse.

Le calendrier présenté à l'époque prévoyait un développement de projet rythmé par l'évolution du composant de mémoire à long terme (JANUS PV), sur lequel nous n'avions que peu d'influence. Sa mise en service était initialement prévue dans le courant du premier semestre 2004. Or, comme on l'a vu, le système a été mis en service dans le courant de l'été 2005, soit avec un retard d'un peu plus d'une année.

Toutefois, et c'est le plus gênant, certaines fonctionnalités ont été mises en service plus tard encore, et au compte-goutte. Leur réalisation a sans doute été dépendant de leur complexité et des ressources encore disponibles auprès de l'unité chargée du développement du système au sein de l'administration fédérale.

Une des raisons du retard d'une année dans la mise en service de JANUS PV 2.0 a été le changement répétitif du chef de projet informatique au sein du service informatique du département fédéral de justice et police (CSI-DFJP). Un tel retard n'est pas étonnant pour un projet d'envergure nationale qui regroupe la Confédération et les cantons, si on en juge les précédentes tentatives<sup>351</sup>. Cependant, la mise en service de JANUS PV 2.0 ne comportait initialement que les fonctions de base, comme la saisie et la recherche des informations présentes dans la base de données. Les anciennes données contenues dans des « sous-champs » n'étaient pas reformatées sous la nouvelle forme et n'étaient disponibles que par une recherche dans le corps du texte. De même, les *comparaisons* automatiques n'ont été fonctionnelles que quelques mois après l'introduction de la nouvelle version de la base de données. Ces comparaisons ne prenaient alors en compte que les nouvelles informations introduites selon la nouvelle structure des « sous-champs ». Ensuite, ce ne fut qu'au début de 2006 que les « attributs » en lien direct avec une personne présente en identité dans le système ont été inclus aux comparaisons. Enfin, la visualisation des données dans le programme de représentation graphique *Analyst's Notebook*<sup>TM</sup> n'a elle aussi été disponible qu'au début de 2006. Seulement, cette visualisation ne proposait alors qu'une représentation insatisfaisante, puisque les deux niveaux de liens (directs et indirects), introduits dans JANUS PV 2.0 en différenciant les « objets » en « attributs » et en « sous-champs », n'apparaissaient pas<sup>352</sup>.

---

<sup>350</sup> Sous la forme du mémoire de thèse.

<sup>351</sup> Voir chapitre 1.3.3 – Survol historique des bases de données de police en Suisse

<sup>352</sup> Voir chapitre 3.4.1.1 – Visualisation de JANUS PV 2.0

Tous les objets étaient directement liés à la personne, alors que la cosmétique était, elle, assurée : un téléphone portable étant graphiquement différent d'un téléphone fixe !

Des corrections ont été immédiatement demandées sur plusieurs points et de nouveaux délais ont encore été nécessaires pour la réalisation de ces modifications.

Toutefois, le point le plus pénalisant pour ce projet a été l'absence des fonctionnalités d'importation et d'exportation de données initialement prévues par le cahier des charges du groupe de travail.

Ces fonctionnalités n'ont pas été développées durant le projet JANUS PV 2.0. Elles ont été reportées sur le projet connexe suivant JANUS JO 3.0. Ce second projet avait pour but de relier à nouveau le sous-système JO à la nouvelle ossature logicielle de JANUS PV 2.0 qui semblait solide et donner satisfaction aux utilisateurs. Donc, fin octobre 2005, le groupe de travail PV 2.0 a été définitivement dissout pour se reformer immédiatement en groupe de travail JO 3.0. Dès lors, les efforts se sont naturellement portés sur le futur nouveau sous-système JO et, ce qui devait être terminé pour JANUS PV 2.0, dans cette enveloppe budgétaire et temporelle, n'était du coup plus du tout prioritaire.

Des solutions intermédiaires ont donc finalement été envisagées afin de permettre au moins l'exportation des données de JANUS PV 2.0, sous un format compatible avec *l'Analyst's Notebook*<sup>TM</sup> pour la visualisation correcte des données. Ces données, même partielles, pourraient, en dernier recours, aussi servir à alimenter la base de données *iBase*<sup>TM</sup> servant de composant d'analyse.

Dans le courant de l'été 2006, une séance de travail portant spécifiquement sur ces problèmes était organisée par le chef des projets JANUS PV 2.0 et JANUS JO 3.0. Elle débouchait sur l'acceptation des propositions faites pour l'exportation des données pour une visualisation correcte, mais avec des délais de réalisation de plusieurs mois, voire plusieurs années au vu du manque d'effectif au sein du CSI-DFJP. Ces fonctionnalités n'étaient désormais plus prioritaires par rapport aux autres demandes de correction. Le temps nécessaire aux corrections et modifications après la mise en service n'avait visiblement pas été planifié au début du projet. Ceci est une erreur de conception de projet qui laisse aux utilisateurs à chaque fois la désagréable impression de travailler avec des outils qui n'ont pas pu proprement aboutir.

En conséquence, comme les fonctionnalités d'importation et d'exportation de JANUS 3.0 n'ont pas encore pu être réalisées, l'auteur de cette recherche a décidé de s'en tenir aux expériences qui ont pu être accumulées lors de la phase exploratoire et de réalisation du prototype du composant de base de données d'analyse et de la mise en fonction de la nouvelle version de la mémoire à long terme, soit la base de données centralisée JANUS PV 2.0.

Nous espérons toujours que ces blocages techniques, organisationnels ou même budgétaires sauteront ces prochaines années, ce qui permettrait enfin à ce projet d'être entièrement mené à son terme.

Il faut toutefois relever que la visualisation graphique des données contenues dans JANUS PV, telle que décrite au chapitre 3.4.1.1 a été réalisée et mise en production en décembre 2009. Cette visualisation, qui permet enfin de distinguer les différents niveaux de liens entre les protagonistes, a été accompagnée de visualisations des journaux et des contrôles techniques contenus dans le sous-système JO. Nous espérons que ces fonctions permettront aux utilisateurs de mieux se rendre compte de la valeur des informations contenues dans cette base de données et de la plus-value qu'elles peuvent apporter lorsqu'elles sont intégrées à un système d'aide à l'enquête prédéfini et performant.

Nous pouvons toutefois nous interroger sur une autre raison de ce développement parfois chaotique. Il s'agit d'un aspect plus méthodologique. En effet, on peut ici mettre en cause la problématique générale des développements informatiques qui, en ce qui concerne le contexte policier, souffrent souvent d'un manque de stratégie et de gestion des processus métiers. Ainsi, voit-on naître des projets pharaoniques qui ne répondent qu'à une seule préoccupation (comme par exemple l'archivage des données, alors que cette étape n'est qu'une de celles que rencontre le praticien), sans se soucier suffisamment des autres éléments qui font partie du même processus fondamental d'investigation.

C'est ainsi que les enquêteurs se trouvent perpétuellement confrontés à des systèmes disparates et peu ou pas interconnectés ce qui leur rend la tâche toujours aussi difficile.

Rares sont les projets qui se préoccupent non-seulement de la disponibilité et de la pérennité des données, mais qui englobent de manière systémique l'ensemble de l'activité cognitive qui y est associée et qui fait partie intégrante du processus d'investigation. Seule une approche de ce type qui décrive *a priori* la méthode et les mécanismes du traitement des données dans l'ensemble du processus peut aboutir sur un outil intégré et parfaitement adapté au travail d'investigation.

Aujourd'hui, seuls existent quelques projets exploratoires ou qui ne disposent que de moyens dérisoires en regard de ce qui est investi ailleurs<sup>353</sup> et qui sont souvent développés sous la forme de prototypes.

De tels projets systémiques étant visiblement novateurs, il est difficile d'établir une quelconque responsabilité dans les lenteurs du développement de JANUS, mais il est certain que le processus

---

<sup>353</sup> Comme par exemple le projet PICAR (Plateforme Informatique du CICOP pour l'Analyse du Renseignement), qui consiste grossièrement à regrouper les différentes bases de données des différentes coordinations du CICOP (Concept Intercantonal de Coordination Opérationnelle et Préventive - organe intercantonal d'analyse du renseignement, qui coordonne l'information de police à l'échelle intercantonale), qui couvre en partie le territoire du concordat RBT (Romandie, Berne et Tessin).

d'investigation est si mal encore défini et si méconnu (même des investigateurs), que les développements informatiques ne peuvent que souffrir de carences méthodologiques.

Tout du moins peut-on espérer qu'à l'avenir ces processus soient mieux explicités, exprimés et restitués et qu'ils fassent partie intégrante des premières préoccupations stratégiques des équipes de projet, pour qu'ils soient conceptualisés en tenant compte d'une méthode qui soit celle de l'investigation criminelle. L'analyste criminel peut et doit y contribuer, mais son rôle est sans doute encore insuffisamment pris en compte.



## 4.2 *Utilité du projet*

Cette deuxième partie cherche tout de même à mesurer l'utilité de cette recherche sur un plan pratique. Selon la méthodologie décrite au chapitre 2.6.1, un certain nombre de tests ont été réalisés, si ce n'est quantitativement, ces sujets seront traités au moins qualitativement, les données nécessaires n'étant, loin s'en faut, pas toujours disponibles. Des réflexions seront faites aussi bien au niveau du composant de mémoire à long terme (JANUS PV 2.0) qu'à celui de la base de données d'analyse (*Prototype β*).

Enfin, les problèmes nouveaux ou récurrents seront identifiés et discutés, qu'il s'agisse de difficultés pratiques, méthodologiques ou structurelles.

### 4.2.1 **Gain d'information ?**

La question centrale ici est de savoir si, avec ce nouveau système on engrange plus de données, dans un premier temps, et, dans un second temps, si ces données constituent effectivement un gain d'information. Pour tenter d'y répondre objectivement, nous avons pu obtenir quelques chiffres au sujet des systèmes JANUS, car c'est surtout à ce niveau que se trouvent les enjeux de gain d'information. Le système d'aide à l'enquête complet peut bien-entendu influencer la démarche de l'investigateur durant l'enquête en mettant à jour des lacunes d'information ou des zones d'ombre nécessitant de nouvelles recherches.

#### 4.2.1.1 **Système plus facile d'accès → Plus d'adhérents ?**

Il ressort des chiffres qui ont pu être obtenus auprès de *fedpol*<sup>354</sup> que le nombre d'utilisateurs du système JANUS a passablement augmenté.

En effet, le nombre d'utilisateurs ayant accès au système est passé de 2169 au 31 août 2005, soit le mois de la migration de JANUS PV à JANUS PV 2.0 à 2659 au 30 juin 2006, ce qui constitue une augmentation de 23% en moins d'une année. Autrement dit, chaque mois depuis la mise en service de JANUS PV 2.0, une cinquantaine de nouveaux utilisateurs sont enregistrés auprès de *fedpol*.

Cette augmentation semble bien significative, JANUS ou ses prédécesseurs existant depuis une quinzaine d'années. Elle démontre que JANUS PV 2.0 a suscité l'intérêt du monde policier, qui l'a adopté, et que de nombreux nouveaux collaborateurs individuellement ou en groupe ont été intéressés à y avoir accès. Une telle augmentation ne semble pas pouvoir être attribuée à la seule évolution naturelle des nouvelles technologies, qui tend à une adhésion toujours plus forte des utilisateurs, mais bien à une perception générale de l'utilité du système.

---

<sup>354</sup> Ces données ont été aimablement produites à début juillet 2006 et transmises par Mme S. KALBERMATTER, PJF-Polsys, *fedpol*. Nous ne disposons toutefois pas de données qui permettraient une étude longitudinale, par exemple de pouvoir comparer le taux de progression à une autre période.

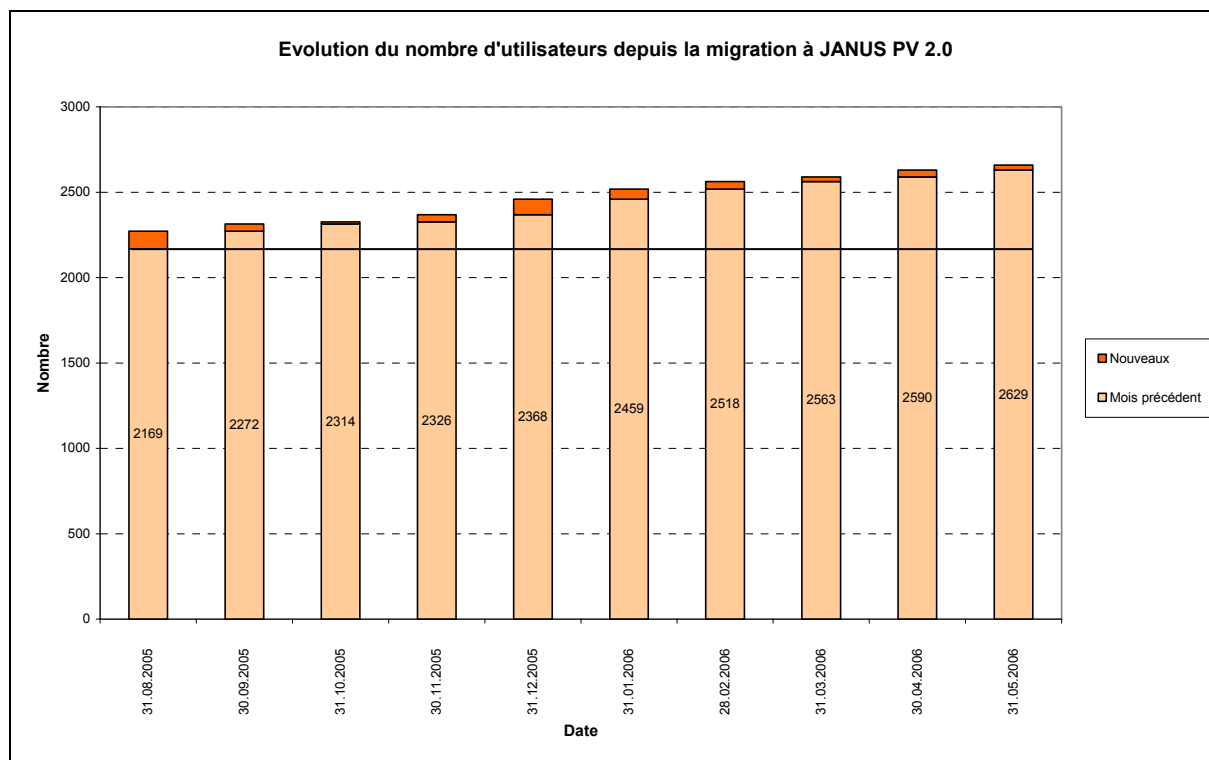


fig. 171 : Evolution du nombre d'utilisateurs depuis la migration à JANUS PV 2.0

Sur le plan vaudois, le nombre d'utilisateurs n'a globalement pas augmenté de manière significative, l'ensemble des collaborateurs de la police de sûreté étant déjà normalement enregistrés auprès de *fedpol* avant 2005. Ce qui pourrait signifier que certains groupes d'utilisateurs dans d'autres cantons attendaient la nouvelle version de JANUS PV pour décider de leur éventuelle plus grande adhésion au système.

#### 4.2.1.2 Système plus performant → Plus d'intérêt ?

Le nombre de personnes et d'organisations enregistrées dans la base de données a augmenté de 8.4% en 10 mois depuis la migration de JANUS PV. Parallèlement le nombre d'antécédents augmentait de 6.5%.

Nombre d'enregistrements de JANUS PV			
	jusqu'au 31.08.2005	du 31.08.2005 au 30.06.2006	Augmentation
Personnes (physiques et organisations)	122'599	10'243	8.4%
Antécédents	178'675	11'580	6.5%

fig. 172 : Nombre total d'enregistrements dans JANUS PV en 2006

En 2002, une statistique partielle avait été faite au sein de la police de sûreté vaudoise<sup>355</sup>. Celle-ci avait montré qu'environ 10'000 nouvelles identités avaient été saisies cette année-là, dont environ 7'000 par les services de la Confédération. En 2005 - 2006, c'est un nombre légèrement supérieur puisqu'on dépasse les 10'000 nouvelles entités après 10 mois, ce qui représente une augmentation

<sup>355</sup> Voir point 2.1.2 – Situation actuelle

de 20% par rapport à 2002. Mais, il est difficile de se prononcer sur la raison de cette augmentation, comme nous ne disposons pas de chiffres pour la période 2003 à 2005, il est impossible de savoir si cette augmentation fait partie d'une tendance générale ou si elle est abruptement apparue depuis le passage à la nouvelle version.

Cet indicateur est en outre relativisé par d'autres éléments qui auraient permis de se prononcer plus finement sur l'intérêt qu'a suscité le nouveau système, comme le nombre et la fréquence des recherches, mais ces chiffres ne sont pas disponibles.

#### 4.2.1.3 Système plus convivial → Plus de participants ?

Le détail des saisies dans le système par juridiction avant et après la migration est le suivant :

	Jusqu'au 31.08.2005				Ratio (PJF -cantons)
	Personnes	Organisations	Personnes & Organisations	Antécédents	
ARGOVIE	2224	8	2232	3362	1.85%
APPENZELL	51	0	51	93	0.05%
BERNE (Canton)	1752	33	1785	1887	1.21%
BERNE (Ville)	205	1	206	123	0.11%
<b>PJF</b>	<b>80117</b>	<b>2627</b>	<b>82744</b>	<b>125527</b>	<b>68.88%</b>
BALE-CAMPAGNE	940	2	942	1335	0.75%
BALE-VILLE	1534	10	1544	1716	1.08%
FRIBOURG	354	65	419	529	0.31%
GENEVE	3703	36	3739	3715	2.47%
GLARIS	427	0	427	951	0.46%
GRISONS	426	15	441	447	0.29%
JURA	64	2	66	62	0.04%
LUCERNE	940	7	947	1059	0.66%
NEUCHATEL	898	3	901	1334	0.74%
NIDWALD	21	0	21	27	0.02%
OBWALD	58	0	58	94	0.05%
SAINT-GALL	2492	11	2503	3840	2.10%
SCHAFFHOUSE	428	1	429	486	0.30%
SOLEURE	638	10	648	821	0.49%
SCHWYZ	180	1	181	298	0.16%
THURGOVIE	905	5	910	1484	0.79%
TESSIN	1692	71	1763	2054	1.26%
URI	9	0	9	18	0.01%
VAUD (Canton)	6152	55	6207	8215	4.77%
VAUD (Lausanne)	269	0	269	548	0.27%
VALAIS	765	1	766	942	0.56%
ZOUG	90	2	92	138	0.08%
ZURICH (Canton)	6522	16	6538	8937	5.12%
ZURICH (Ville)	6856	2	6858	8633	5.12%
<b>Total</b>	<b>120712</b>	<b>2984</b>	<b>123696</b>	<b>178675</b>	<b>100.00%</b>

fig. 173 : Répartition des saisies JANUS PV jusqu'au 31.08.2005

La Confédération avait saisi près de 70% du total des informations présentes dans JANUS PV avant la migration. Ceci est grandement dû au fait qu'elle ne dispose d'aucun autre système d'information et que la grande majorité de ses activités d'enquête se rapporte très précisément à la criminalité organisée. Il faut encore rappeler que les anciens Offices centraux de police criminelle (OCPC) saisissaient eux-mêmes les informations transmises sous forme de rapports par les cantons dans JANUS, et que cette manière de faire perdure encore.

Il est toutefois intéressant de noter que tous les cantons sont représentés en 2005. Il n'y avait déjà plus de cantons qui ne participaient pas du tout au système. Cependant la participation de chacun est très disparate. Elle est peut-être justement en rapport avec la pénétration de la criminalité organisée.

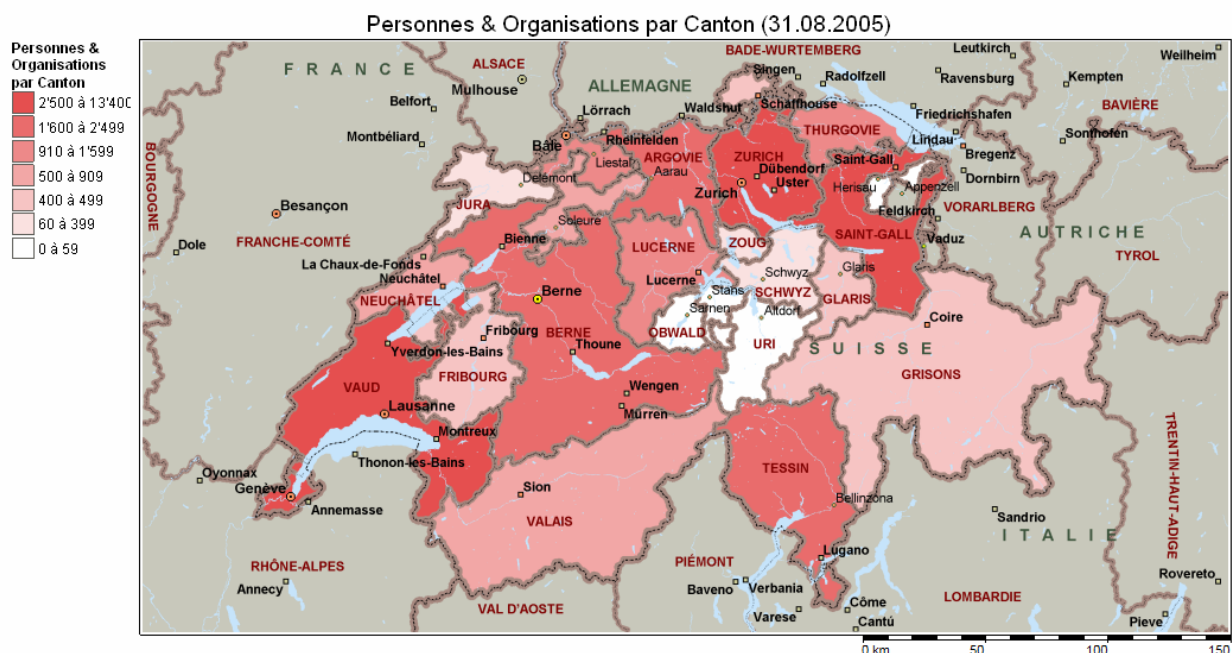


fig. 174 : Représentation du nombre des personnes saisies par canton jusqu'au 31.08.2005<sup>356</sup>

Si on compare cette situation avec les chiffres de 2005-2006, on remarque que les cantons qui avaient saisi le plus de données avant le changement de système sont restés les mêmes après la mise à niveau. Il s'agissait principalement de Zurich, Vaud, Genève, Saint-Gall, Argovie, Berne et le Tessin.

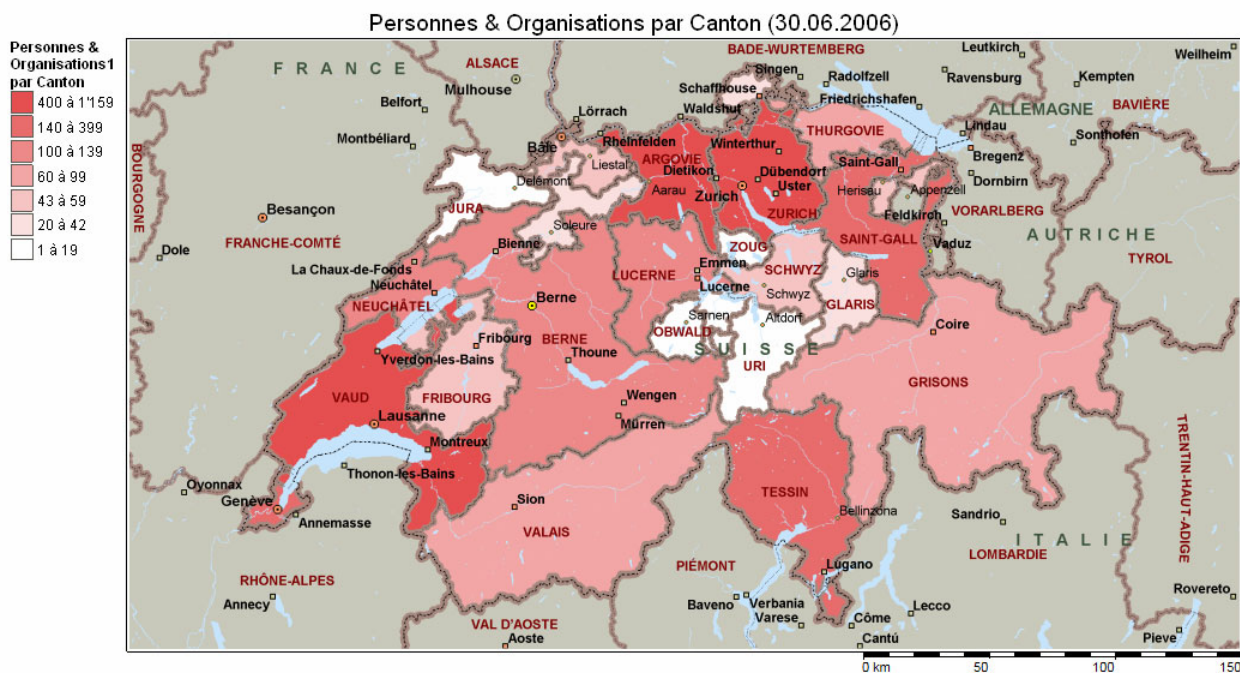


fig. 175 : Représentation du nombre des personnes saisies par canton entre le 31.08.2005 et le 30.06.2006

<sup>356</sup> Ces représentations géographiques ont été réalisées à l'aide de Microsoft MapPoint™ 2003.

Cependant depuis août 2005, on remarque une légère baisse de la part très prépondérante de la Confédération, qui diminue à env. 60%, alors que deux entités ont significativement augmenté leur participation. Il s'agit du canton d'Argovie et de la ville de Lausanne.

Ne connaissant pas les raisons qui ont favorisé la saisie en Argovie, plaçant ce canton en troisième position juste derrière Zurich et Vaud, on peut expliquer l'augmentation du nombre de saisies de la police de la ville de Lausanne par une meilleure formation de ses membres en regard de l'utilisation des moyens spéciaux d'enquête et l'intégration des données issues des contrôles téléphoniques rétroactifs<sup>357</sup>.

En ce qui concerne la part toujours très importante de la quantité totale d'informations saisies par la juridiction fédérale, il faut garder à l'esprit que celle-ci ne traite au vu de sa mission que des affaires se rapportant à la criminalité organisée et que ce faisant l'ensemble des personnes faisant l'objet d'une enquête vont de retrouver dans le système JANUS, la PJF ne disposant par ailleurs pas de base de données d'archives à proprement parler.

	du 31.08.2005 au 30.06.2006 (10 mois)				Ratio (PJF -cantons)
	Personnes	Organisations	Personnes & Organisations	Antécédents	
ARGOVIE	400	0	400	853	4.26%
APPENZELL	43	0	43	69	0.38%
BERNE (Canton)	93	1	94	125	0.74%
BERNE (Ville)	23	0	23	31	0.18%
<b>PJF</b>	<b>6107</b>	<b>311</b>	<b>6418</b>	<b>12198</b>	<b>63.30%</b>
BALE-CAMPAGNE	56	0	56	147	0.69%
BALE-VILLE	195	2	197	354	1.87%
FRIBOURG	55	0	55	82	0.47%
GENEVE	247	0	247	312	1.90%
GALRIS	20	0	20	45	0.22%
GRISONS	86	1	87	135	0.75%
JURA	1	0	1	1	0.01%
LUCERNE	103	33	136	182	1.08%
NEUCHATEL	113	0	113	264	1.28%
NIDWALD	1	0	1	1	0.01%
OBWALD	9	0	9	12	0.07%
SAINT-GALL	230	0	230	393	2.12%
SCHAFFHOUSE	42	0	42	70	0.38%
SOLEURE	39	0	39	72	0.38%
SCHWYZ	57	1	58	106	0.56%
THURGOVIE	94	3	97	255	1.20%
TESSIN	143	3	146	199	1.17%
URI	9	0	9	10	0.06%
VAUD (Canton)	432	5	437	822	4.28%
<b>VAUD (Lausanne)</b>	<b>144</b>	<b>0</b>	<b>144</b>	<b>305</b>	<b>1.53%</b>
VALAIS	66	0	66	140	0.70%
ZOUG	5	1	6	6	0.04%
ZURICH (Canton)	711	4	715	1010	5.87%
ZURICH (Ville)	437	7	444	877	4.49%
<b>Total</b>	<b>9961</b>	<b>372</b>	<b>10333</b>	<b>19076</b>	<b>100.00%</b>

fig. 176 : Répartition des saisies JANUS PV entre le 31.08.2005 et le 30.06.2006

<sup>357</sup> Depuis 2005, la Division d'appui opérationnel (DAO) de la BAAC dispense des cours sur les moyens spéciaux d'enquête à tous les policiers judiciaires du canton, ville de Lausanne comprise.

Enfin, si l'on rapporte le total des informations saisies (personnes physiques ou organisations et les antécédents) à la population des cantons, un petit canton qui passait inaperçu jusqu'ici prend la première place : il s'agit du canton de Glaris, qui a introduit de plus de 1400 informations, bien que sa population ne soit que d'environ 38'000 personnes. Peut-être ce canton a-t-il connu avant 2005 une affaire particulière qui a justifié à un certain moment l'usage intensif de JANUS PV ?

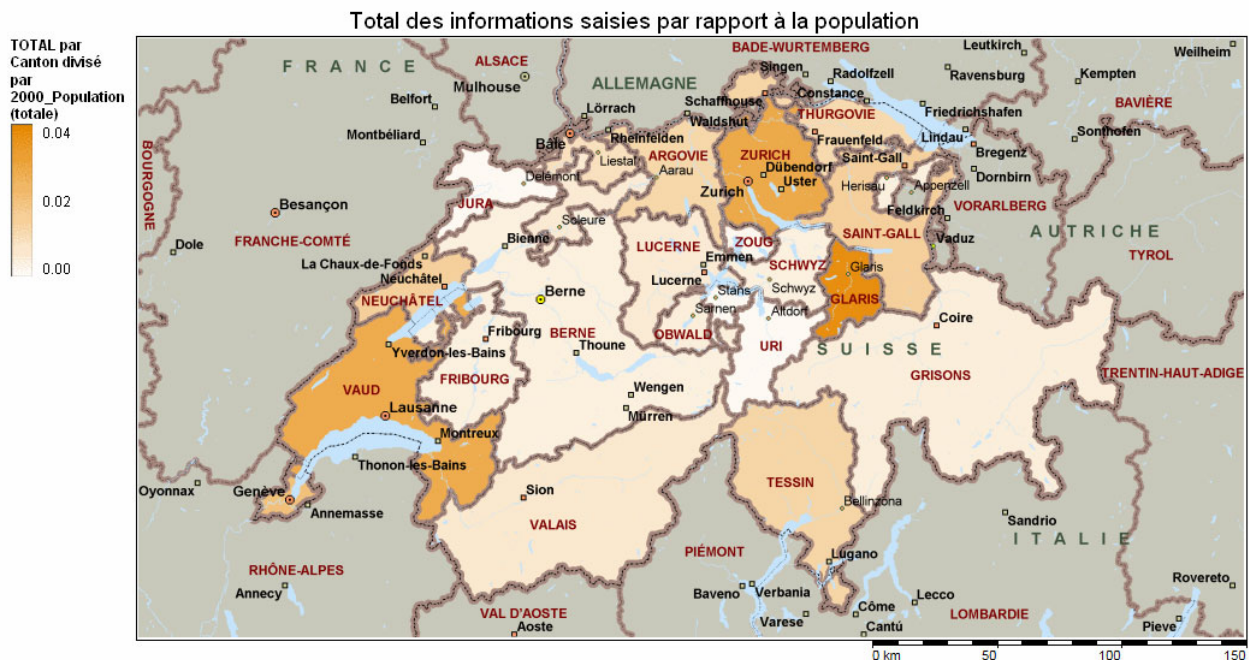


fig. 177 : Représentation du nombre total des saisies JANUS PV par rapport à la population

#### 4.2.1.4 Système plus précis → Plus de données structurées ?

Bien qu'il soit difficile de juger précisément cet élément en l'état de la réalisation du système, nous espérons que les utilisateurs profiteront à l'avenir des nouvelles possibilités qui leur sont offertes, en ce qui concerne la différenciation des « attributs » et des « sous-champs ».

Nous avons donc profité des données transmises par la Confédération pour calculer le rapport entre le nombre d'antécédents et le nombre de personnes saisies.

Ce rapport devrait nous permettre d'évaluer globalement si le souci d'une saisie précise et en cours d'enquête s'est fait ressentir auprès des utilisateurs. Avec l'ancienne version de JANUS PV, il n'était pas rare de tomber sur des antécédents très longs, qui reprenaient quasi *in extenso* le rapport final destiné au magistrat instructeur. Celui-ci était même repris tel quel pour l'ensemble des protagonistes principaux, ce qui rendait caduque toute tentative de visualisation. On avait donc un ratio de 1.00, soit un antécédent pour une personne.



Avant la nouvelle version de JANUS PV, le ratio moyen était de 1.38 antécédent par identité (personne ou organisation). Quelques cantons arrivaient même à avoir un ratio inférieur à 1.00, ce qui n'était normalement pas réglementaire (!).

Les données saisies après le 31 août 2005 présentent un rapport antécédent / identité bien meilleur, soit en progression de 27% à 1.69.

	Ratio (-> 2005)	Ratio (2005 - 2006)	Evolution
ARGOVIE	1.51	<b>2.13</b>	42%
APPENZELL	1.82	1.60	-12%
BERNE (Canton)	1.06	1.33	26%
BERNE (Ville)	<b>0.60</b>	1.35	126%
<b>PJF</b>	1.52	1.90	25%
BALE-CAMPAGNE	1.42	<b>2.63</b>	85%
BALE-VILLE	1.11	1.80	62%
FRIBOURG	1.26	1.49	18%
GENEVE	<b>0.99</b>	1.26	27%
GLARIS	<b>2.23</b>	<b>2.25</b>	1%
GRISONS	1.01	1.55	53%
JURA	<b>0.94</b>	1.00	6%
LUCERNE	1.12	1.34	20%
NEUCHATEL	1.48	<b>2.34</b>	58%
NIDWALD	1.29	1.00	-22%
OBWALD	1.62	1.33	-18%
SAINT-GALL	1.53	1.71	11%
SCHAFFHOUSE	1.13	1.67	47%
SOLEURE	1.27	1.85	46%
SCHWYZ	1.65	1.83	11%
THURGOVIE	1.63	<b>2.63</b>	61%
TESSIN	1.17	1.36	17%
URI	<b>2.00</b>	1.11	-44%
VAUD (Canton)	1.32	1.88	42%
VAUD (Lausanne)	<b>2.04</b>	<b>2.12</b>	4%
VALAIS	1.23	<b>2.12</b>	72%
ZOUG	1.50	1.00	-33%
ZURICH (Canton)	1.37	1.41	3%
ZURICH (Ville)	1.26	1.98	57%
<b>Moyenne</b>	<b>1.38</b>	<b>1.69</b>	27%

fig. 178 : Rapport entre les identités et les antécédents dans JANUS PV

Cette progression a été visible dans de nombreux cantons qui utilisent peu le système.

Ces chiffres sont réjouissants car ils semblent montrer que même les utilisateurs occasionnels prennent plus de soin à saisir leurs données dans JANUS PV. Ceci avant même que la comparaison, ou la visualisation ne tiennent compte des améliorations au niveau de la différenciation des liens directs et indirects.

Ceci veut sans doute dire que dès que ces fonctions seront correctement intégrées au système, cette augmentation du ratio antécédent / identité sera encore plus nette, puisque auparavant la structure même du fichier limitait cette possibilité d'analyse et rendait le système moins intéressant pour ses utilisateurs.

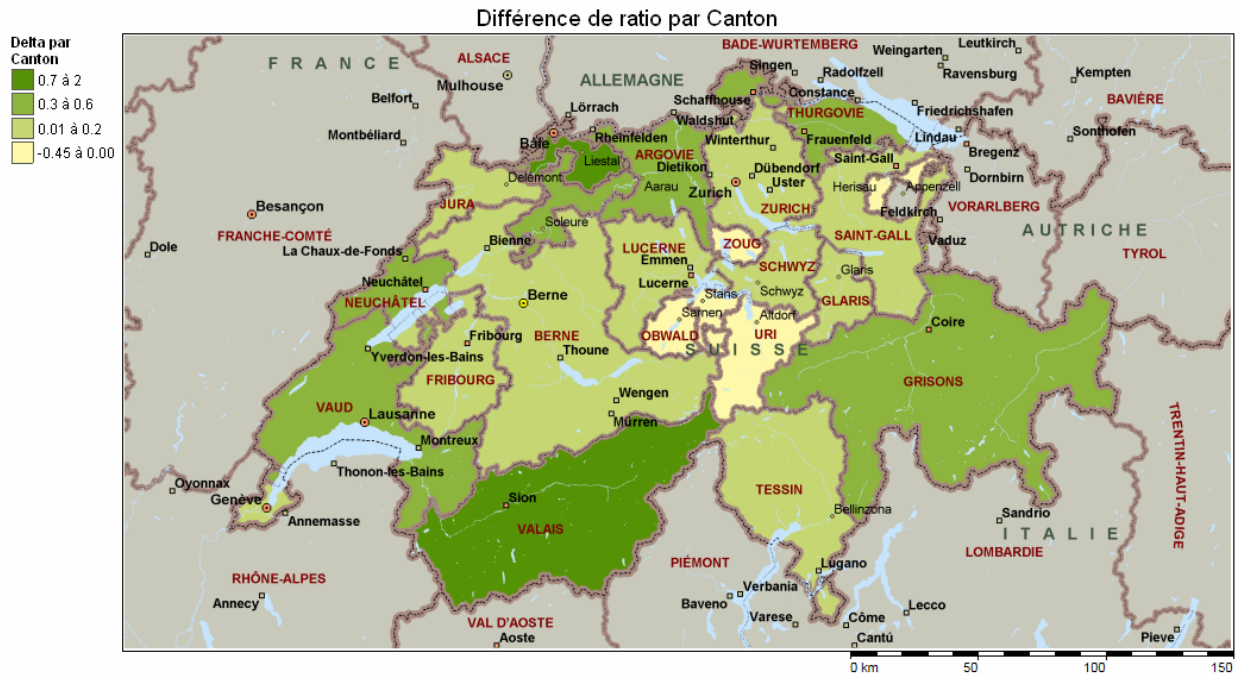


fig. 179 : Représentation de l'évolution du ratio entre les identités et les antécédents dans JANUS PV

#### 4.2.1.5 Synthèse

Les quelques chiffres qu'il a été possible de récupérer auprès de *fedpol* nous ont permis de présenter des résultats qui semblent indiquer que le gain d'information au niveau de la base de données commune est bien réel et qu'il devrait encore se renforcer avec le temps. Ces statistiques semblent indiquer une meilleure adhésion des policiers au système, une augmentation de la qualité de l'information saisie par un meilleur découpage des antécédents et une intégration déjà sensible des notions utiles à l'analyse.

Une fois que ces fonctions avancées seront réalisées, l'adhésion au système devrait encore aller en augmentant.

Le nombre annuel total d'informations saisies au niveau suisse, n'a toutefois progressé que de 20% en quatre ans. S'il ne nous est pas possible de déterminer si cette augmentation est directement liée à la nouvelle version de JANUS PV, ou si elle est due à la lente mais constante augmentation de l'adhésion des policiers au système JANUS PV, nous sommes d'avis qu'elle reflète aussi une certaine stabilité dans le traitement de l'information relative à la criminalité organisée. Cette stabilité est extrêmement positive, dans le sens qu'elle démontre que même si les outils changent, les méthodes de travail, définies en amont, elles, ne changent pas. Le groupe de travail ne cherchait d'ailleurs pas à changer le travail du policier de base, mais uniquement à améliorer l'outil à disposition.



## 4.2.2 Gain de temps ?

Le gain de temps devrait se situer à différents niveaux, que ce soit dans le système de mémoire à long terme et lors de l'utilisation de logiciels d'aide à l'analyse.

L'investissement en temps pour l'utilisation de ces outils n'est lui pas remis en cause. Sans mémoire à long terme, la lutte contre la criminalité organisée est vaine, de même, sans utilitaire d'analyse des données d'enquêtes la résolution d'affaires complexes et d'envergure est fortement compromise<sup>358</sup>.

Il s'agit donc de mesurer les progrès et les ralentissements induits par les nouveaux systèmes.

### 4.2.2.1 Système plus simple → Moins de saisies intermédiaires ?

#### JANUS PV 2.0 :

Le nouveau JANUS PV 2.0 est plus simple d'utilisation grâce à l'évolution technologique. Il est plus convivial et des contenus multimédia peuvent y être intégrés. Mais, cette plus grande simplicité a-t-elle permis de diminuer les saisies intermédiaires d'information dans des fichiers tampons, comme c'était le cas à la police cantonale vaudoise avec l'ancienne version ? La réponse est assez contrastée. D'une part les utilisateurs ont effectivement plus tendance à adhérer au système et à faire eux-mêmes la saisie d'informations simples, mais, d'autre part, dès que ces informations deviennent plus complexes, ou qu'une importation de données sous la forme de « sous-champs » est nécessaire, l'expérience montre qu'ils font alors encore souvent appel à du personnel spécialisé.

Il y a donc moins de saisies intermédiaires, mais le recours à du personnel spécialisé pour l'utilisation « avancée » de la base de données centrale est toujours nécessaire.

#### Prototype $\beta$ :

Le principal problème de ce projet se situe aujourd'hui exactement ici, l'interface entre JANUS et le *prototype  $\beta$*  n'étant pas encore réalisée. Si l'on désire tout de même utiliser le composant d'analyse pour la résolution d'une affaire, comme on l'a fait en test dans l'affaire VO décrite précédemment, trois solutions s'offrent à nous : soit l'analyste ressaisit lui-même les données de JANUS, comme il l'aurait fait pour une visualisation simple à l'aide de l'*Analyst's Notebook*<sup>TM</sup>, ce qui constitue manifestement une double saisie et une perte de temps ; soit il ressaisit ces informations dans un fichier temporaire, ce qui constitue un fichier intermédiaire en vue d'une importation ; soit enfin il reformate et importe des données extraites de JANUS pour une visualisation, ce qui implique des manipulations souvent relativement difficiles et rébarbatives. Il n'y a donc actuellement pas de progrès sur ce plan-ci.

---

<sup>358</sup> Voir chapitres 2.1 à 2.3 - Postulats

#### 4.2.2.2 Système plus ouvert → Moins de double saisie ?

##### JANUS PV 2.0 :

En ce qui concerne le nouveau JANUS PV 2.0, au stade actuel des développements de JANUS 3.0, le système n'est pas plus interfacé que le précédent, puisque seule l'importation des « sous-champs » KOM (*moyens de communication*) est possible. Il est même moins interfacé, puisque auparavant, il était possible de préparer des listes de « sous-champs » de tous types et de les coller simplement dans le corps du texte. Or, aujourd'hui, ces autres données doivent être saisies une à une dans le système. Peut-être qu'à l'avenir, d'autres interfaces d'importation seront également développées pour les autres « sous-champs », mais tout ceci nécessite encore plus de ressources de développement pour une amélioration qui sera sans doute jugée non prioritaire.

D'autre part, il était question au début du projet de prévoir des passerelles entre JANUS et les systèmes cantonaux d'archives de police (ABI et POLIS notamment). Aujourd'hui, ces passerelles sont en cours de réalisation. Les données doivent donc encore être saisies à double dans les systèmes cantonaux et dans JANUS.

On ne note donc pas encore d'amélioration dans le secteur de la double saisie des informations.

##### Prototype $\beta$ :

Comme on l'a dit précédemment, l'interface entre JANUS et le *prototype  $\beta$*  n'ayant pas pu être entièrement finalisée, la double saisie existe encore. Mais la réalisation de l'exportation des données de JANUS pour leur analyse dans cette base d'analyse devrait bien évidemment corriger cette lacune.

#### 4.2.2.3 Système plus intégré → Moins de manipulations ?

##### JANUS PV 2.0 :

L'intégration même de JANUS PV a peu changé, puisqu'il n'est que très peu interfacé avec des systèmes externes. Par contre, l'intégration des deux sous-systèmes PV et JO à la même plateforme informatique les a fait redevenir très performants, comme ce fut le cas à l'origine. Il ne devrait, par exemple, plus être nécessaire de recourir à des fichiers temporaires pour reformater et réimporter des données de JO dans PV. De même, il serait souhaitable que le système JO soit directement ou indirectement lié au système d'écoute centralisé et utilisé par toutes les polices de Suisse<sup>359</sup>. Cette liaison, une fois effective, permettra de diminuer drastiquement les manipulations nécessaires à la saisie des données d'écoutes dans JANUS JO.

L'utilisation interne aux systèmes JANUS des objets en XML devrait permettre à l'avenir une intégration facilitée.

---

<sup>359</sup> Depuis 2005, ce système est le LIS (Lawful Interception System). Mais, un nouveau projet démarre à fin 2008 pour le remplacer. Il s'agit du projet ISS (Interception System Suisse).

Prototype  $\beta$  :

De ce côté-ci, par contre, l'utilisation du métalangage XML n'est pas directement la source d'une plus grande intégration des données. XML permettant de définir la structure des données, il porte en lui également le défaut de son avantage : chacun définit la structure que doit avoir le fichier XML pour être intégrable à son propre système. Ainsi, tant JANUS que *iBase*<sup>TM</sup> ont leur standard. La transformation d'une structure à l'autre que ce soit dans un sens ou dans l'autre n'est pas simple, comme énoncé au chapitre 3.4.

Mais, si une intégration entièrement automatique n'est pas réalisée, les manipulations s'en trouveront décuplées, rendant peut-être même le travail manuel d'exportation et d'importation plus long et difficile que la simple re-saisie.

**4.2.2.4 Système plus précis → Moins de formatage ?**JANUS PV 2.0 :

La structuration des « sous-champs » et des « attributs » a amélioré de manière importante la précision des données introduites dans JANUS. De même, les standards internationaux (norme ISO) ont été pris en compte pour un maximum de listes de choix.

Le reformatage des données de ce point de vue est donc diminué, pour autant que les systèmes qui désirent utiliser les données de JANUS reprennent ces mêmes standards, ce qui est encore loin d'être le cas.

Prototype  $\beta$  :

Bien que la précision des données de JANUS ait augmenté, le reformatage des documents XML, langage bavard s'il en est, doit absolument être automatisé, au vu du nombre de manipulations individuelles à réaliser. Pour ce faire, l'usage d'un *parseur XML* est indispensable.

Enfin, *iBase*<sup>TM</sup> présente encore un inconvénient majeur, qui est son système d'importation de données XML qui permet d'importer qu'un seul type de lien à la fois, multipliant le nombre de manipulations d'importation par le nombre de types de liens différents présents dans le jeu des données à importer.

**4.2.2.5 Synthèse**

La partie pratique de cette recherche n'ayant pas pu être totalement menée à son terme, le facteur temps n'est, en l'état des développements, pas encore influencé positivement.

Les différentes possibilités d'interface et d'intégration avec divers autres systèmes tels que les bases de données de police des cantons, du système de surveillance des télécommunications centralisé et des bases de données d'analyse ont pourtant été définies lors de la conceptualisation des nouveaux JANUS PV et JO. L'adhésion des utilisateurs, la qualité de l'information saisie et la centralisation de l'information s'en trouveront directement améliorées. Après trois ans de fonctionnement du nouveau sous-système JANUS PV et une année du nouveau sous-système JANUS JO, les utilisateurs s'impatientent de la réalisation de ces interfaces.

Nous espérons que les personnes en charge des projets de développement des systèmes de gestion des données de police auront pris conscience du potentiel d'un système interfacé avec d'autres sources d'information et des systèmes d'analyse et que des efforts seront enfin consentis pour aller dans ce sens.

### **4.2.3 Gain de capacité d'analyse ?**

Ce dont nous devons discuter ici est de savoir si ces nouveaux systèmes permettent de mieux comprendre les données contenues tant dans la base de données centralisée que dans la base de données d'analyse. Les expériences préliminaires seront la base principale de cette réflexion.

#### **4.2.3.1 Gain d'intégration → L'analyste analyse ?**

##### JANUS PV 2.0 :

Le système devant être plus intégré, l'analyste devait pouvoir se concentrer sur l'analyse en elle-même plutôt que dans le traitement des données. Malheureusement, le système de visualisation « interne » à JANUS PV n'a pas été, loin s'en est fallu, une réussite du premier coup. En effet, la visualisation des données ne correspondait pas à la réalité des données (liens directs et indirects) et ne permettait pas d'obtenir une image interprétable par l'enquêteur ou l'analyste. Cette situation insatisfaisante doit être corrigée au plus vite.

##### Prototype $\beta$ :

Ici, à nouveau, si le système avait pu être entièrement interconnecté, il y a fort à parier que l'analyste aurait eu beaucoup plus de temps pour analyser réellement les données présentes. Or, comme on l'a vu au chapitre précédent, ce n'est pas encore le cas.

Mais, en dehors de ces considérations techniques, il ressort de mon expérience de l'opération DK, que lorsque l'on demande à un analyste de « juste » analyser, sans qu'il y ait de travail de « saisie » ou tout du moins de « manipulation » de données, sa tâche en est, en fait, compliquée pour plusieurs raisons.

Premièrement, la « simple » représentation manuelle de données est un acte intelligent (au sens propre), l'analyste devant prendre connaissance du dossier, comprendre les choses et les faits, et ensuite choisir la manière appropriée de représenter le jeu de données présent afin d'en retirer une valeur ajoutée.

Deuxièmement, le temps qui est utilisé par l'analyste pour traiter les données lui permet de réfléchir sur le cas et de développer ses hypothèses. Ce n'est donc pas du temps « perdu » à saisir ou manipuler ou formater des données, mais investi à une activité annexe qu'est la réflexion sur le cas présent. Donc, l'analyste qui ne fait qu'« analyser » a ensuite besoin d'un temps qui pourrait être estimé au moins à la moitié du temps nécessaire à la création des visualisations pour effectuer réellement et « uniquement » le travail cognitif d'analyse.

Or, bien souvent, l'enquêteur imagine que sur la base de ses visualisations (automatiques ou manuelles) l'analyste pourra lui donner son opinion très rapidement, ce qui est faux dans la

pratique. Plus l'analyse doit aller en profondeur, plus le temps nécessaire est long. Et l'appréciation d'une représentation bien décomposée (ce qui devrait être le cas avec le nouveau JANUS) est souvent coûteuse en termes de temps de réflexion.

#### 4.2.3.2 Gain de précision → L'analyse est meilleure ?

##### JANUS PV 2.0 :

La précision influence directement la qualité des données. Ainsi, elle influence également directement la qualité de l'analyse se basant sur ce jeu d'informations. Des liens qui n'étaient pas détectés précédemment par un manque de précision (par exemple par la saisie différente de mêmes données telles que des numéros de plaque ou de téléphone) pouvaient drastiquement influencer une analyse. Le nouveau JANUS PV 2.0 est beaucoup plus strict, notamment sur tous les identifiants des entités, qu'il s'agisse de « sous-champs » ou d'« attributs ». On peut donc s'attendre à une nette amélioration sur ce plan.

##### Prototype β :

Il est possible de faire exactement les mêmes remarques par rapport au *prototype β*. Ici se sont les besoins de l'analyste qui ont été pris en compte et qui ont même parfois directement influencé la base de données centralisée. Ces notions sont bien présentes dans les bases de données d'analyse et constituent un avantage réel.

#### 4.2.3.3 Gain de décomposition → L'analyse est plus fine ?

##### JANUS PV 2.0 :

Un des problèmes majeurs dans l'analyse des données contenues dans l'ancienne version de JANUS PV était le manque de différenciation entre les liens directs ou indirects<sup>360</sup>. De plus, de nombreuses informations « enchâssées » dans les « sous-champs » faisaient perdre au système son potentiel de liaison.

Ces défauts ont été corrigés en partie et la situation actuelle est sensiblement meilleure, sans toutefois que le système soit devenu beaucoup plus contraignant pour l'utilisateur.

##### Prototype β :

Ici encore, il s'agit, si possible, de corriger les derniers enchâssements de données contenus dans des « sous-champs » et des « attributs ». Ceci devrait être possible en passant par un fichier d'échange XML, mais la réalisation du parseur s'en trouvera encore compliquée.

---

<sup>360</sup> Ce point a été largement détaillé au point 2.5.2 – Structure détaillée de JANUS PV

#### 4.2.3.4 Gain de structuration → L'analyse est plus standardisée ?

##### JANUS PV 2.0 :

Dans cette nouvelle version, on peut compter sur des entités mieux structurées et dont l'identifiant est, sauf exception<sup>361</sup>, facilement identifiable. Les besoins des analystes ont été entendus par le groupe de travail chargé de la nouvelle version de JANUS PV.

Toutefois, sans visualisations, l'analyse de liens nombreux et complexes est très difficile.

##### Prototype $\beta$ :

Le *prototype  $\beta$*  apporte encore plus de structure aux entités présentes. Non seulement le type d'entités présentes est défini de manière standard, mais également le type des liens les mettant en connexion. Ceci étant réalisé, les nombreuses fonctions de recherche ciblées et d'analyse décrites au chapitre 3.3.5<sup>362</sup> sont prêtes à l'emploi. Ces fonctions ont été largement utilisées avec succès dans les exercices de la sécurité militaire et lors de l'opération DK.

#### 4.2.3.5 Synthèse

Il est indéniable que la qualité et la structure des données à disposition pour l'analyse de la situation a évolué favorablement avec ces nouveaux outils et même si l'interface entre les deux composants n'est pas encore achevée, cela constitue déjà un progrès.

Cependant, il ne faut pas croire que le temps gagné par une intégration complète serait égal au temps passé encore aujourd'hui par l'analyste à manipuler ses données. Notre propre expérience nous montre qu'il utilise aujourd'hui environ au moins la moitié de ce temps pour réfléchir à la situation qui lui est présentée.

Le gain en capacité d'analyse est donc réel, mais ne représente pas un gain de temps phénoménal. Par contre, il peut amener beaucoup plus d'enquêteurs, à faire leur propre appréciation de la situation en se basant sur des éléments fiables et de meilleure facture.

#### 4.2.4 Problèmes nouveaux ou récurrents

La partie précédente a décrit en détail les améliorations techniques potentielles ou réelles de l'utilisation du système en deux composants proposé par ce projet de recherche.

Plus que l'outil lui-même mis à disposition des enquêteurs, analystes ou toute autre personne participant au processus de lutte contre la criminalité organisée, il apparaît clairement que les structures opérationnelles et l'organisation du travail devront s'adapter à la méthode de travail proposée ici et induite par l'analyse criminelle opérationnelle. En particulier lorsqu'un système d'aide à l'enquête tel que celui proposé par cette recherche veut être utilisé. Nous traiterons donc ici de ses implications aux niveaux structurel et organisationnel.

---

<sup>361</sup> Voir notamment les « sous-champs » / « attributs » *Moyens de communication* et *Objets* de PV2

<sup>362</sup> Chapitre 3.3.5 – Autres fonctions d'analyse propres à iBase et utiles au prototype  $\beta$

#### 4.2.4.1 Problème récurrent : la place des analystes

L'utilisation d'une base de données d'analyse ne remplace pas les méthodes traditionnelles d'enquête, tout comme les systèmes plus simples de visualisations ponctuelles de données. Il s'agit toujours d'outils auxiliaires. Pour qu'elle puisse apporter un bénéfice, la base de données d'analyse doit pouvoir évoluer parallèlement et au même rythme que l'investigation en cours. L'exploitation de cette base de données d'analyse, de surcroît idéalement couplée à un système partagé de mémoire à long terme, nécessite des connaissances techniques nouvelles et donc une formation spécifique.

S'agit-il de former des enquêteurs chevronnés à ces nouveaux outils, ceux-ci bénéficiant de la reconnaissance de leurs pairs, au risque de les voir malgré tout conditionnés par leurs habitudes et se comporter en « enquêteur » plutôt qu'en « analyste » ? Ou faut-il profiter des connaissances techniques pointues d'académiciens disposant d'une expérience policière bien moindre, mais ayant un regard neuf et ne risquant pas de prendre le rôle de l'enquêteur ?

La question reste ouverte. Mais, comme l'exploitation de ce moyen spécial d'enquête nécessite une spécialisation du personnel, nous ne pouvons que recommander de composer des équipes mixtes qui regroupent des personnes répondant aux deux profils évoqués ci-dessus.

Différentes doctrines d'intégration des méthodes et des outils d'analyse criminelle sont apparues ces dernières années. Jusqu'à la fin des années 1990, Interpol recommandait un travail en séquence, l'analyste devant travailler après les enquêteurs, sur dossier, et quasi uniquement sur les cas non-résolus. Plus récemment, un document du Conseil de l'Europe<sup>363</sup> sur les meilleures pratiques en matière d'analyse criminelle, constate que dans certains pays, à l'instar de ce qui a été fait dans le Canton de Vaud, les ressources d'analyse criminelle, tant humaines que matérielles, devaient être intégrées aux processus d'enquête le plus tôt possible.

##### « Conclusion n°7 :

Il n'y a pas de solution idéale pour organiser l'analyse criminelle, mais l'intégration de l'analyse opérationnelle dans le processus d'enquête, et de l'analyse stratégique dans le cycle d'élaboration des politiques publiques est d'une très grande importance. Dans le cas de l'analyse opérationnelle, en particulier, il convient au plus haut point de l'associer d'emblée à une enquête complexe ou dès que sa complexité est manifeste. » (p.26)

A la police de sûreté vaudoise précisément, trois différents niveaux de formation et de qualification ont été définis afin de répondre aux besoins en analyse criminelle. De nombreux enquêteurs ont reçu une formation de base, leur permettant de réaliser des clarifications simples au profit de leurs propres enquêtes. Les situations pour lesquelles un appui ponctuel et relativement simple est

<sup>363</sup> CONSEIL DE L'EUROPE, Analyse Criminelle – Crime organisé – Etude des meilleures pratiques nos. 4, 2002

nécessaire sont nombreuses (dans le cadre de la lutte criminalité organisée ou non). Pour cette raison le pool d'enquêteurs formés représente environ un quart du personnel judiciaire du canton. Une plus petite équipe de spécialistes (regroupés à la BAAC<sup>364</sup>), soit des analystes civils et des policiers, constituent les deux niveaux supérieurs. Le deuxième niveau est encore renforcé par des enquêteurs des brigades spécialisées formés à l'utilisation complète des logiciels de visualisation et à l'exploitation des bases de données d'analyse. Les analystes civils de la BAAC ayant encore pour mission de développer et de maintenir des systèmes tels que présentés dans ce projet de recherche. L'intégration d'un enquêteur spécialisé ou d'un analyste à une équipe d'enquête est donc un modus connu et pratiqué dans certains corps de police judiciaire en Suisse et en Europe. Mais l'intégration d'outils aussi spécifiques que des bases de données d'analyse requiert une collaboration encore plus étroite et durable.

#### **4.2.4.2 Problème nouveau : une collaboration durable**

Si l'évolution de la société a poussé les corps de police à se spécialiser dans la seconde moitié du XX<sup>e</sup> siècle, les méthodes d'analyse criminelle, par l'intégration d'outils de visualisation graphique qui permettent des appuis ponctuels durant l'enquête, et *a fortiori* par l'utilisation d'une base de données d'analyse durant l'enquête rend nécessaire l'intégration d'un analyste à plein temps à l'équipe d'enquête. La relative complexité des outils impose désormais des spécialistes pour la saisie et le traitement des données dans la base d'analyse, ainsi que pour leur interprétation. Il est illusoire de pouvoir mettre ces outils directement dans les mains d'enquêteurs, sans que les mesures structurelles et une formation spécifique leur soit donnée, d'autant plus que d'autres missions et responsabilités leur sont traditionnellement dévolues par leur hiérarchie.

Cette constatation pose donc le problème de la gestion des ressources humaines au sein de l'organisme qui traite de la lutte contre la criminalité organisée, au sens large.

Jusqu'à présent, les organisations des différentes polices judiciaires n'ont que rarement mis en place de telles structures ou alors encore trop timidement. Par exemple, au sein de la police fédérale, ce n'est que depuis peu qu'une réelle *Task Force* a été mise en place pour lutter contre le terrorisme et que deux analystes ont été intégrés à un groupe d'enquêteurs de manière permanente.

Il n'est toutefois pas forcément nécessaire de rigidifier les structures en intégrant de manière fixe des analystes à chaque groupe d'enquête. Il est également possible de disposer de suffisamment de personnes capables de renforcer ou de rejoindre des équipes lors d'enquêtes d'envergure. Il ne s'agit pas forcément uniquement d'analystes criminels, mais également de spécialistes compétents dans d'autres domaines comme l'analyse comptable ou économique, des spécialistes de l'identité judiciaire ou de la recherche de traces informatiques, ou encore de spécialistes d'autres moyens spéciaux d'enquête.

---

<sup>364</sup> BAAC : Brigade d'Appui, d'Analyse et de Coordination



Dans ces enquêtes complexes, il devient impossible au meilleur des enquêteurs de gérer lui-même l'ensemble des informations et de conduire seul les opérations de manière optimale. Il est indispensable de créer des équipes d'enquête, composées d'enquêteurs et disposant de support en matériel et en personnel spécialisé pour mener à bien les investigations.

Cette manière de gérer le personnel en fonction des affaires à traiter rejoint une organisation qui a déjà cours dans certains grands services de police anglo-saxons.

Le problème évident pour la Suisse est sa taille modeste, encore amplifié par le compartimentage des forces disponibles dans les cantons. Ceci a pour conséquence de pénaliser ce type d'organisation en *Task Force*, nécessitant des spécialisations et par voie de conséquence une taille critique supérieure.

Il serait évidemment possible d'imaginer regrouper certaines spécialités en des moyens disponibles pour plusieurs cantons, mais là encore, le découpage linguistique réduit les potentialités de mise en commun. C'est toutefois une piste à étudier, par exemple en se basant sur les quatre différents concordats de police suisses.

Une solution de ce type serait évidemment plus productive, elle éviterait des redondances inutiles et amènerait une plus grande standardisation dans les méthodes d'enquêtes. Par contre, il n'est pas certain que la disponibilité permanente des moyens soit immédiatement assurée, ce qui pourrait être un argument pour ses détracteurs. De plus, les disparités des procédures pénales dans les cantons (même au niveau romand) rendent ce type de coopération pour l'instant encore trop difficile.

Cette problématique rejoint parfaitement les démarches actuellement en cours au niveau suisse, puisque le groupe de travail sur l'analyse criminelle opérationnelle<sup>365</sup> de la commission de police judiciaire (CPJ) de la conférence des commandants des polices cantonales suisses (CCPCS), par l'intermédiaire de l'ACPJS (association des chefs de police judiciaire suisses), propose un modèle harmonisé de l'intégration de l'analyse criminelle opérationnelle en Suisse.

Le groupe de travail constatait qu'après dix ans de formation d'enquêteurs suisses à l'analyse criminelle opérationnelle, son intégration et son utilisation était encore très médiocre. La formation en elle-même n'était pas directement remise en cause, mais ce qui posait problème était l'absence de structure et d'organisation au sein des corps de police judiciaire. Seuls ces aménagements auraient permis de valoriser les compétences acquises lors de la formation de leurs enquêteurs. Parfois, la structure des corps avait été adaptée, mais sans modifier aussi l'organisation du travail,

---

<sup>365</sup> Ce groupe de travail, formé à fin 2004, a remplacé l'ancien « Kerngruppe » qui comptait les personnes qui avaient suivi la première formation suisse à ce sujet en 1997, mais qui n'avait, en fait, aucune légitimité vis-à-vis des chefs de police judiciaire.

ce qui a débouché sur le dysfonctionnement des cellules ainsi spécialement créées. Il n'y avait pas de collaboration effective entre enquêteurs et analystes.

Le projet, soumis au préavis de l'ACPJS pour la CPJ, est basé sur un modèle d'intégration en trois niveaux<sup>366</sup>, selon les compétences en analyse criminelle opérationnelle des personnes spécialisées et selon leur taux d'activité réservé à cette discipline. Ainsi, le premier niveau qui devrait compter environ 25% de l'effectif du corps serait composé d'enquêteurs qui auraient suivi une formation de base d'une semaine et qui utiliseraient leurs compétences d'analyse pour leur propres enquêtes ou ponctuellement au bénéfice de collègues de la même unité. Le deuxième niveau serait toujours composé d'enquêteurs, mais qui auraient cette fois reçu une formation pour spécialiste de deux semaines supplémentaires et qui pourraient fonctionner comme analystes au sein de leur unité, ceci pour des analyses étendues. Ils devraient utiliser au plus 30% de leur temps à ces analyses et représenteraient environ 5% de l'effectif du corps. Enfin, le troisième et dernier niveau serait composé d'analystes à plein temps qui en sus des tâches de soutien aux enquêtes auraient des missions de recherche et de développement. Ces analystes « professionnels » auraient suivi la même formation spécialisée que les enquêteurs de niveau 2, bien qu'une formation universitaire et une spécialisation dans ce domaine soient des atouts. Ils devraient représenter environ 1 à 2 % de l'effectif du corps de police judiciaire.

Ce concept d'intégration a reçu en 2008 un accueil favorable auprès de l'ACPJS. La CPJ l'a accepté quelques semaines plus tard. La transition pourrait alors se faire sur cinq ans entre 2009 et 2014.

Cette réforme devrait permettre de donner accès à des ressources spécialisées même aux cantons de petite taille par leur mise en commun au niveau des concordats. Ces concordats seront en outre responsables de la standardisation de la formation de niveau 1, la formation de niveau 2 étant réservée au groupe de travail sur l'analyse criminelle opérationnelle qui doit veiller à l'harmonisation au niveau suisse.

Cette réforme réalisée, on devrait alors pouvoir disposer, en Suisse, des conditions-cadre harmonisées aux niveaux structurels et organisationnels tout à fait favorables à la mise en pratique de méthodes de travail basées sur les processus fondamentaux d'investigation et mis en évidence grâce à l'analyse criminelle. L'utilisation de nouveaux outils basés sur ces méthodologies devrait alors être grandement facilitée.

---

<sup>366</sup> Ce modèle d'intégration en trois niveaux a été appliqué dans le canton de Vaud depuis 2000 et les résultats obtenus sont très satisfaisants. Le groupe de travail de la CPJ sur l'analyse criminelle opérationnelle s'en est donc largement inspiré.

### 4.3 *Perspectives pour l'analyse criminelle opérationnelle*

Dans cette dernière partie de la discussion, nous allons prendre le temps de discuter de la phase d'analyse en tant que telle. En effet, la littérature spécialisée sur l'analyse criminelle<sup>367</sup> est encore souvent axée sur la description de procédés, par exemple sur les différents types de visualisations graphiques relationnelles ou chronologiques. Ces marches à suivre sont principalement basées sur des bonnes pratiques, souvent sous le couvert de la méthodologie générale de l'analyse criminelle qu'est le cycle du renseignement.

On se rend finalement compte qu'il existe en matière d'analyse criminelle un certain nombre de vides méthodologiques importants qu'il faudrait s'efforcer de combler, tant au niveau de la validation des bonnes pratiques, si souvent rencontrées et décrites dans les ouvrages d'analyse criminelle<sup>368</sup>, qu'au sujet de l'analyse en tant que telle et décrite comme une phase à part entière du cycle du renseignement.

Nous n'allons pas discuter de la validation méthodologique des bonnes pratiques qui demande un investissement qu'il n'est plus raisonnable de consacrer dans cette présente recherche. Il nous paraît toutefois encore utile d'aborder la problématique de la phase d'analyse.

Nous avons déjà introduit dans la première partie de cette recherche un certain nombre de notions relatives à ce sujet, notamment la nature des raisonnements qui entrent en jeu, souvent décrits comme *non démonstratifs*<sup>369</sup> (inductifs ou abductifs). Cependant, sans vouloir être exhaustif ou même catégorique, des disciplines comme la Logique ou la cognition étant des sujets d'étude de recherche et de discussion sur lesquels de nombreux philosophes et chercheurs ont passé tout ou partie de leur vie, nous sommes d'avis qu'une réflexion prospective peut être conduite sur les moyens envisageables pour encadrer cette phase particulière et visiblement si complexe à décrire et à modéliser.

Ainsi, comme nous l'avons fait tout au long de cette recherche, nous prendrons les éléments qui nous paraissent utiles à cette discussion dans différentes disciplines, comme l'étude de la criminalité organisée, le droit pénal, l'enquête criminelle, la question de la modélisation, l'informatique, la logique.

Nous espérons alors pouvoir présenter une démarche qui permette de mieux cerner la phase d'analyse et en particulier l'analyse d'hypothèses concurrentes. Nous nous poserons ensuite la

---

<sup>367</sup> Comme par exemple, l'ouvrage de référence de PETERSON *et al*, Intelligence 2000 : Revising the Basic Elements, 2000.

<sup>368</sup> Ainsi que dans le chapitre 2.3 de cette recherche.

<sup>369</sup> Cf, chapitres 1.4.5.2 – Raisonnements et 1.4.5.3 – Décomposition et interprétation des informations

question de l'influence que peut ou doit avoir cet éclairage sur la méthode générale qu'est le cycle du renseignement. Par exemple, nous discuterons de l'automatisation de certains processus.

#### **4.3.1 Encadrement de l'étape d'analyse**

La méthodologie générale proposée par l'analyse criminelle, soit le traitement de l'information selon un processus cyclique itératif, permet s'il est suivi, comme toute démarche qualité, de diminuer les risques d'erreur d'interprétation des informations.

La méthode de travail étudiée et proposée par cette recherche voudrait mettre à disposition des praticiens un outil qui s'inscrive dans ce processus. Les informations connues de la police, enregistrées dans une mémoire à long terme, selon un modèle structurel suffisamment précis devaient pouvoir être intégrées à une mémoire à court terme, base d'analyse, répondant au moins à la même précision dans sa structure. Ainsi, les nouveaux éléments devant être pris en compte dans l'enquête suivent dans la pratique une procédure compatible avec la méthodologie décrite en ce qui concerne les phases de collecte, d'évaluation et de traitement des données. Ils devraient donc arriver dans les meilleures conditions au stade de l'analyse.

On peut donc légitimement s'attendre à ce que la mise en place d'un tel système, répondant aux standards de l'analyse criminelle opérationnelle (intégration au processus général par l'utilisation d'outils adéquats) puisse permettre d'augmenter la qualité des éléments soumis aux interprétations lors des analyses qui en découlent.

Par exemple, la gestion des liens n'est plus laissée à la seule mémoire du ou des enquêteurs en charge d'une enquête. Jadis, une excellente mémoire était une qualité unanimement appréciée. Aujourd'hui, les bases de données ont pris le relais. Elles permettent en outre de ne plus devoir uniquement se fier à des souvenirs plus ou moins précis, mais de pouvoir retrouver rapidement l'information originale et s'y référer. Le système proposé dans cette recherche permet de remonter à l'information originale et d'en disposer immédiatement dans sa forme factuelle (décomposée et individualisable).

Les interprétations qui en découlent peuvent donc se baser sur des éléments disponibles et correctement énoncés. Ceci est un gain indéniable de qualité. Le risque de baser ses réflexions sur des souvenirs incorrects ou inconsciemment biaisés devrait diminuer de façon drastique.

Le système proposé permet donc d'amener à l'enquêteur ou à l'analyste des éléments et des informations d'une manière la plus objective possible, leur permettant de les interpréter dans des conditions optimales. Peu de marge de manœuvre est laissée aux utilisateurs, la base de données d'analyse proposée étant même encore beaucoup plus stricte qu'une simple visualisation, chaque information (entité) intégrée au système d'analyse devant être décomposée, évaluée et correctement liée aux éléments connexes.

Le cycle du renseignement apporte bien un gage de qualité dans le processus général du traitement de l'information. Cette méthode documentée et reconnue doit être appliquée par chaque analyste.

Reste à discuter de l'analyse, étape cruciale, souvent perçue comme une boîte noire. Souvent, la phase d'analyse est simplement décrite comme la génération d'hypothèses par des processus cognitifs analytiques (inductifs ou abductifs). C'est une phase par conséquent très subjective, que ce soit lors d'un raisonnement inductif (par analogie ou par généralisation) ou *a fortiori* lors de raisonnements abductifs (explicatif) devant amener « l'analyste » à rechercher un maximum d'hypothèses pouvant expliquer le résultat constaté. La personne qui « analyse » fait ainsi à tout moment référence à son expérience personnelle et à ses connaissances *a priori*. Il est toutefois possible et fréquent que plusieurs personnes partagent la même expérience ou les mêmes connaissances acquises et qu'elles arrivent donc une interprétation proche ou similaire. C'est ce que l'on peut définir comme de l'intersubjectivité.

Cependant, l'analyse ne se réduit pas à la génération d'hypothèse, elle implique également qu'on utilise ces renseignements pour en faire quelque-chose, faute de quoi, ce processus serait stérile. Une fois les hypothèses posées, il va être nécessaire de les tester, soit en agissant à nouveau et en allant chercher de nouvelles données lorsque cela est encore possible. C'est à dire en testant les hypothèses développées précédemment en fonction des éléments qui les supportent ou les infirment.

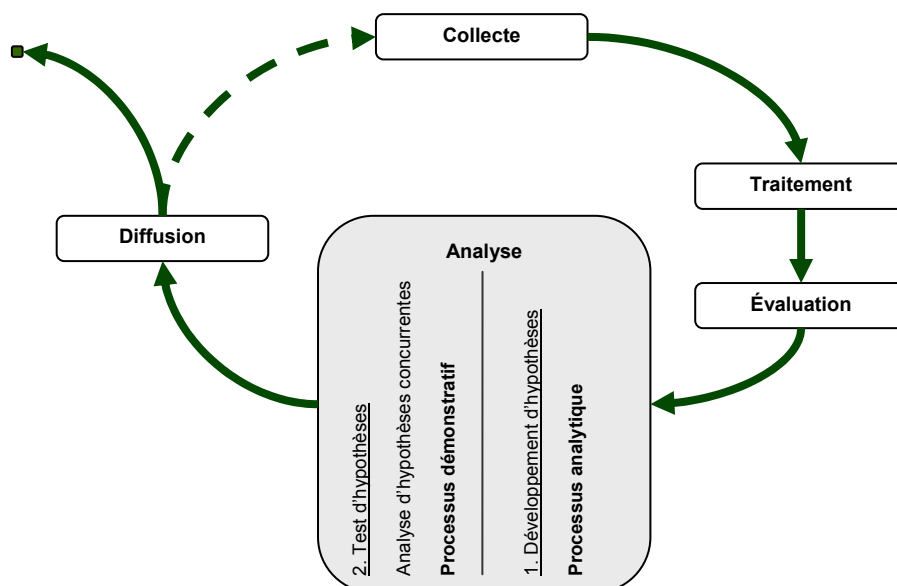


fig. 180 : Cycle du renseignement : deux phases nécessaires dans l'étape d'analyse

Les raisonnements qui entrent alors en jeu doivent à nouveau être de type démonstratif. Ils doivent pouvoir se baser sur des éléments factuels objectifs dans le but de démontrer que telle ou telle hypothèse est ou n'est pas « la bonne », soit la seule qui corresponde aux faits établis, ou la plus

probable, ou encore celle qui présente le plus grand risque, suivant le contexte de l'analyse elle-même.

La question que l'on doit désormais légitimement se poser ici est de savoir s'il est possible de normer, autrement dit d'encadrer, cette seconde phase d'analyse qui suit celle du développement d'hypothèses, soit l'analyse de la concurrence de ces mêmes hypothèses.

BERNIER<sup>370</sup> dans son discours sur la normativité du raisonnement non démonstratif, fait directement référence à BAYES<sup>371</sup> avant d'aborder le falsificationnisme de POPPER. Il s'y intéresse dans ce qu'il dénomme le *processus de révision des croyances* :

« L'objectif fondamental de l'approche bayésienne est de donner une mesure probabiliste de la révision des croyances sur la base de l'observation ou de l'expérimentation et, du même coup, une mesure du degré de confirmation qu'une observation ou un test empirique confère à une certaine hypothèse. L'intérêt d'une telle approche est manifeste, puisqu'elle propose précisément une certaine règle, à savoir la règle de conditionnalisation, comme norme guidant la révision rationnelle des croyances. L'approche bayésienne repose sur un postulat fondamental, intuitivement plausible, qui correspond à la notion de probabilité épistémique<sup>372</sup>. Intuitivement, l'idée est tout simplement que nous assignons des degrés de vérité (ou de fausseté) *subjectifs* à nos diverses croyances, degrés qui se situent sur une échelle continue entre 0 et 1. » (p. 78)

Les sciences forensiques, qui s'interrogent depuis de longues années sur la phase interprétative des résultats des analyses scientifiques, usent de l'approche bayésienne<sup>373</sup>. La théorie probabiliste qui est reconnue en sciences forensiques découle en effet des travaux de BAYES. Cette approche probabiliste a pour but de produire un rapport de vraisemblance conditionnelle appelé *Likelihood Ratio* (LR) qui est calculé sur la base du rapport entre la probabilité d'observer un certain résultat *r* sachant qu'une personne ou un événement *X* est la source de l'indice *I*, et la probabilité d'obtenir le même résultat *r* sachant que cet indice *I* est dû à une autre personne ou événement que *X*.

$$LR = \frac{p(r | I, X)}{p(r | \bar{I}, X)}$$

---

<sup>370</sup> BERNIER, La normativité du raisonnement non démonstrative, in POLITZER, *op. cit.*, 2002

<sup>371</sup> Thomas BAYES (1702-1761), mathématicien britannique.

<sup>372</sup> Ou autrement dit : « *La probabilité épistémique, quant à elle, décrit notre connaissance. Dans son aspect subjectif, la probabilité est la structure de l'opinion. La probabilité épistémique est généralement un nombre qui représente le degré de notre certitude d'un événement, ou encore le degré de notre croyance en une proposition.* » BOUKRIS, *Induction, probabilités et confirmation chez Carnap*, 2006

<sup>373</sup> Voir entre autres AITKEN et TARONI, *Statistics and the Evaluation of Evidence for Forensic Scientists*, 2004

Cette approche probabiliste ne s'applique généralement en sciences forensiques qu'à l'interprétation d'un seul résultat d'analyse. Il est donc apparu nécessaire d'inscrire cette démarche à un niveau contextuel supérieur, en tentant de prendre en compte différentes hypothèses de travail, en modélisant des situations devant représenter le monde réel. C'est là qu'interviennent les *Réseaux bayésiens*. Ceux-ci permettent d'enchaîner selon la même approche probabiliste des étapes d'un processus pouvant amener à un ou plusieurs résultats. Ces réseaux autorisent notamment de structurer les processus inférentiels, permettant de les approcher d'une manière logique et séquentielle.

Par exemple, il est possible de représenter des éléments d'intérêt (*nodes*) et leurs liens de causalité (*edges*) pour un scénario déterminé.

Cette étape de structuration, soit de création du réseau, reste toutefois une démarche *subjective*<sup>374</sup> :

« This means that through the use of a BN (Bayesian Network), a human expert can graphically and numerically articulate his subjective view of the real world system. Therefore, the task of modelling as well as a model that is obtained as a result of this process will principally be influenced by both, the *properties* and the expert's *individual view, perception*, and ultimately, extent of *understanding*, of a domain of interest. (...)

It has also been reported that different models can be encountered for representing the questions surrounding the same problematic, because:

- the same problem can be approached at different levels of detail;
- existing opinions about domain properties are diverging. (...)

These disagreements explain why we can offer different Bayesian network models for the same hypothesis» (p. 6)

Ceci montre bien que si cette forme complexe de probabilités conditionnelles permet d'utiliser des règles de raisonnement performantes, qui peuvent être à leur tour implémentées dans des logiciels d'aide à la décision, le processus de modélisation reste malgré tout encore très subjectif, même à l'aide d'outils spécialisés comme les *Réseaux bayésiens*. Ces derniers sont, en outre, vraisemblablement trop complexes à mettre en œuvre dans le quotidien du contexte judiciaire.

Toutefois, il peut être très utile de s'intéresser à la logique de l'incertitude, car comme le disait SHAFER<sup>375</sup> : « *Probability is not really about numbers, it is about the structure of reasoning* ».

Ainsi, il devient envisageable de tester des hypothèses concurrentes à l'aide d'outils probabilistes de ce type. Cela requiert toutefois quelques notions en statistique et de disposer des données nécessaires (autant que possible intersubjectives), ce qui n'est à l'évidence pas toujours le cas. Nous

---

<sup>374</sup> TARONI *et al.*, A general approach to Bayesian networks for the interpretation of evidence, 2004

<sup>375</sup> Voir chapitre 1, page 2 de TARONI *et al.*, *op. cit.*, 2006

reviendrons plus loin sur des propositions pour encadrer les processus d'analyse qui font appel aux développements d'hypothèses et à leurs tests de confirmation.

Mais auparavant, il est encore utile de rappeler certains biais cognitifs connus et effets psychologiques qui peuvent fortement limiter et influencer le raisonnement humain, et donc, l'analyse elle-même.

#### **4.3.1.1 Limites et biais de la cognition**

HEUER<sup>376</sup> présente dans un ouvrage de 1999 un certain nombre de réflexions qu'il a pu faire lors de sa longue carrière au sein de la CIA. Bien que cette agence ne soit pas directement concernée par le contexte judiciaire, il faut se rappeler que la méthode utilisée dans l'analyse criminelle tire ses origines du milieu du renseignement et que ses analystes sont donc confrontés aux mêmes problèmes lorsqu'il s'agit de générer des hypothèses et de les tester. Son ouvrage traite de certaines limites qui ont pu être observées, ainsi que de certains biais qui ont d'ailleurs aussi été relevés par d'autres auteurs dans le domaine des sciences forensiques<sup>377</sup>.

HEUER déplore en préambule le peu d'attention qui est généralement donné aux processus cognitifs lorsque l'on tente d'améliorer la qualité de l'analyse :

« When we speak of improving intelligence analysis, we are usually referring to the quality of writing, types of analytical products, relations between intelligence analysts and intelligence consumers, or organization of the analytical process. Little attention is devoted to improving how analysts think. » (p.1)

Selon lui, il est possible d'apprendre aux analystes à réfléchir correctement, et il est possible d'améliorer leurs capacités par l'entraînement. Un certain nombre de pièges sont à prendre en compte lors des analyses, au moins pour être conscient de ses propres limites et des biais découlant de sa propre cognition. Ainsi, comme le psychanalyste, l'analyste criminel averti doit, en plus des faits qui lui sont soumis, analyser en permanence son propre raisonnement, et si nécessaire en corriger les biais.

#### **4.3.1.2 Limites du processus d'analyse**

Se basant sur les travaux antérieurs de psychanalystes, LINDSAY et NORMANN<sup>378</sup> notamment, HEUER rappelle que les processus cognitifs fonctionneraient avec différents types de mémoire, un peu comme les ordinateurs actuels. Les informations sensorielles seraient stockées dans une mémoire spécifique, le reste de la mémoire étant constituée d'une mémoire à court terme et une

---

<sup>376</sup> HEUER, *Psychology of Intelligence Analysis*, 1999

<sup>377</sup> SACHS *et al.*, *Context effects in forensic science : A review and application of the science of science to crime laboratory practice in the United States*, 2003

<sup>378</sup> LINSAY & NORMANN, *Human Information Processing*, 1977 *in* HEUER, *op. cit.*, 1999



mémoire à long terme. Cette dernière correspondant à ce qu'on appelle communément la *mémoire*. La mémoire à court terme est utilisée pour le traitement des informations qu'elles soient sensorielles ou issues de la mémoire à long terme.

Cette mémoire de travail est donc continuellement mise à profit lors du processus analytique. Or, la capacité de la mémoire à court terme humaine n'est pas infinie, loin s'en faut. Des travaux de MILLER<sup>379</sup> dans les années 1950 ont montré ses limites :

« A well-known article written over 40 years ago, titled "The Magic Number Seven--Plus or Minus Two," contends that seven--plus or minus two--is the number of things people can keep in their head all at once. That limitation on working memory is the source of many problems. People have difficulty grasping a problem in all its complexity. This is why we sometimes have trouble making up our minds. For example, we think first about the arguments in favor, and then about the arguments against, and we can't keep all those pros and cons in our head at the same time to get an overview of how they balance off against each other. » (p. 27)

Il nous serait donc difficile d'apprécier une situation qui contienne plus de sept éléments ( $\pm 2$ ). Ce nombre peut paraître faible, mais il semble tout à fait crédible. Des techniques simples sont d'ailleurs naturellement mises en place par chacun de nous pour s'en contenter. Par exemple, nous décomposons intuitivement les situations complexes en sous-problématiques qui peuvent, elles, être appréciées, ou alors, ces situations sont modélisées, schématisées, visualisées (ce qui est d'ailleurs une étape du traitement de l'information dans le contexte de la criminalité organisée), afin de limiter les échanges entre les mémoires à court et à long terme, permettant aussi de se concentrer sur une partie, puis sur une autre. Les résultats des réflexions en sous-problèmes permettent ensuite de remonter à l'image globale des éléments présents. Enfin, on constate que l'utilisation de la prise de notes lors des processus cognitifs permet de se libérer l'esprit tout en conservant les pistes disponibles pour la suite des réflexions.

#### 4.3.1.3 Effets de contexte

Il nous paraît important de rappeler ici la portée des effets de contexte, biais cognitifs qui peuvent avoir plusieurs origines. Celui qui est décrit ici, est bien connu en sciences naturelles et humaines. Il s'agit de l'effet de l'observateur. Ce biais se manifeste à différents niveaux.

#### On perçoit et on retient mieux ce que l'on connaît.

La mémoire semblant être organisée en schémas de relations (*pattern of relationships*), des éléments correspondant à ces schémas seront plus facilement perçus et mieux retenus.

---

<sup>379</sup> MILLER, The Magical Number Seven--Plus or Minus Two: Some Limits on our Capacity for Processing Information, 1956 in HEUER, *op. cit.*, 1999

On peut donner l'exemple de l'expérience faite par de GROOT<sup>380</sup> en 1965, qui a présenté pendant 10 secondes à des Grands Maîtres et à des joueurs d'échecs ordinaires des plateaux de jeu contenant 20 à 25 pièces. Les personnes testées devaient ensuite replacer de mémoire lesdites pièces. Lorsque celles-ci étaient disposées de manière aléatoire, les deux catégories de personnes ne pouvaient replacer qu'environ 6 pièces correctement. Mais, lorsque les pièces étaient disposées selon des parties réelles qui avaient été jouées, les Grands Maîtres étaient capables de reproduire la quasi-totalité du plateau de jeu sans erreur, alors que les joueurs normaux restaient au niveau d'une demi-douzaine de pièces correctement remises à leur place.

Les observateurs prêtent plus d'attention aux éléments qui confirment leur hypothèse de départ.

Ce biais était déjà remarqué par BACON<sup>381</sup> au XVII<sup>e</sup> siècle. Il décrivait ce que nous appelons aujourd'hui le *biais de la confirmation*<sup>382</sup>. Ce biais est la tendance des observateurs à accepter plus facilement et plus rapidement les informations qui soutiennent les opinions originales. Ainsi, un analyste ou un enquêteur aura plus facilement tendance à tester positivement son hypothèse ou ses hypothèses, en recherchant des éléments qui la ou les confirment, plutôt que de rechercher et de mettre en évidence les éléments qui les contredisent.

Une fois qu'un élément a été vu, perçu et mémorisé, il se produit un *effet d'ancrage*.

L'observateur est généralement conditionné par sa première impression et celle-ci va persister, malgré ses tentatives de s'en défaire. De même, si un avis lui est donné *a priori*, il va avoir tendance à influencer son jugement de manière significative.

Par exemple, si l'on demande ce que représentent les deux images centrales (encadrées) dans la figure qui suit, l'observateur sera influencé s'il commence à la regarder depuis la droite ou depuis la gauche.

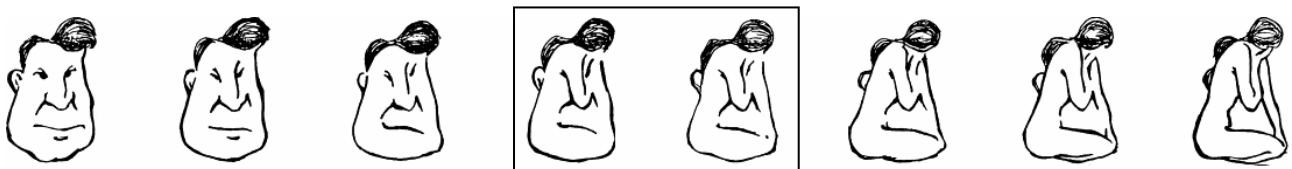


fig. 181 : Effet d'ancrage<sup>383</sup>

Ainsi, si l'observateur commence par regarder la séquence par la gauche, il aura plus facilement tendance à reconnaître un visage, alors que s'il commence par la droite, il y verra plutôt une silhouette de femme.

<sup>380</sup> de GROOT, Thought and Choice in Chess, 1965, in HEUER, *op.cit*, 1999

<sup>381</sup> BACON F., *Novum Organum*, originally published in 1620, in SAKS *et al.*, *op. cit.*, 2003

<sup>382</sup> Le biais de la confirmation sert de base à plus de 200 ans d'épistémologie et de philosophie des sciences. Il explique en partie le critère de Popper pour qualifier la science. Pour approfondir ces notions dans le contexte forensique : CRISPINO, Le principe de Locard est-il scientifique ? Ou analyse de la scientificité des principes fondamentaux de la criminalistique, 2006

<sup>383</sup> Images créées par Gerald FISHER en 1967

Des effets d’ancrage ou des distorsions de raisonnement peuvent aussi apparaître en fonction de stimuli externes, soit de l’environnement de l’observateur, des émotions qu’il ressent, ou encore d’avis préexistants fournis en même temps que les informations brutes à analyser.

Ces influences peuvent avoir des conséquences importantes, surtout lorsque les problématiques abordées sont ambiguës.

Des recherches récentes de DROR<sup>384</sup> en 2005 et 2006 ont montré que l’état émotionnel d’un expert forensique, ainsi que les informations qui lui sont transmises *a priori* peuvent même influencer de manière significative les résultats des identifications d’empreintes digitales lorsqu’on se trouve en présence de traces de mauvaise qualité, ce qui est souvent le cas lorsque l’on traite des traces indiciaries.

Dans le contexte de l’enquête judiciaire elle-même, SAKS<sup>385</sup> relève une recherche qui a été faite sur des auditions lors d’affaires de viol. Les auteurs de cette recherche ont pu démontrer que les *a priori* des enquêteurs influençaient leur attitude durant l’audition, attitude qui influençait à son tour les résultats des auditions elles-mêmes.

Enfin, nous utiliserons un exemple récent, suisse et qui illustre parfaitement ce type de biais, le cas célèbre du sadique zoophile qui aurait sévi dans le Nord-Ouest de la Suisse entre mai et septembre 2005<sup>386</sup>.

La thèse initiale du sadique a été très rapidement privilégiée. L’effet émotionnel a été, on s’en doute, très important. Le fait qu’un sadique s’attaque à des bêtes sans défense a largement choqué l’opinion publique. Des éléments techniques et circonstanciels qui contredisaient cette hypothèse ont été « inconsciemment » ignorés par les enquêteurs. Si bien que des éléments contradictoires trop manifestes étaient systématiquement expliqués par de nouvelles hypothèses qui correspondaient à la thèse générale d’une intervention humaine. Ainsi, lorsque l’étendue géographique est devenue telle que les agissements d’un seul homme ne devenaient plus crédibles, les enquêteurs ont alors imaginé que ces nouveaux méfaits ne pouvaient être que dus à plusieurs sadiques, agissant de concert ou en ayant pris exemple sur le premier. Il s’agissait là d’un biais *de confirmation* d’hypothèse évident.

On notera encore que les premières constatations faites par les services techniques de la police neuchâteloise ont recherché des traces qui pouvaient corroborer la thèse du sadique. La

---

<sup>384</sup> DROR *et al.*, When emotions get the better of us: the effect of contextual top-down processing on matching fingerprints, 2005 et DROR *et al.*, Contextual information renders experts vulnerable to making erroneous identifications, 2006

<sup>385</sup> SAKS *et al.*, *op. cit.*, 2003

<sup>386</sup> GUÉNIAT, Le sadique zoophile a surtout sévi dans les journaux ! Autopsie d’une vache, 2006

connaissance *a priori* de l'existence présumée d'un sadique et les émotions ressenties lors du constat expliquent ce biais contextuel (*effet d'ancrage*) lors de la perception de la scène de crime. Ce n'est qu'après une analyse systématique et complète, habituellement réservée aux homicides (autopsies, examens toxicologiques, reconstitution des blessures sur des animaux morts et même des observations policières), de plusieurs cas survenus dans le canton de Neuchâtel que la thèse du sadique a pu être définitivement exclue et que des morts naturelles suivies de blessures dues à des animaux carnivores tels que le renard ont pu être enfin démontrées. Une grande résistance a toutefois été ressentie, tant par les enquêteurs des autres cantons touchés (qui avaient été jusqu'à monter une cellule d'analyse criminelle, renforcée par un *profiler*) que par le grand public et, *a fortiori*, par les habitants des régions touchées qui restaient persuadés de l'existence d'un sadique.

#### 4.3.1.4 Procédure de production et de test d'hypothèses

Nous l'avons vu, la génération d'hypothèses reste et restera un processus essentiellement créatif et subjectif à cause des raisonnements et des référentiels utilisés. Le but de l'analyste est de traiter ses informations préalablement avec méthode et rigueur afin de les décomposer en éléments réellement objectifs, ceux-ci pouvant alors entrer en jeu dans les processus cognitifs récurifs.

Nous reproduisons à la page suivante une procédure proposée par HEUER<sup>387</sup> dans son chapitre dédié à *l'analyse d'hypothèses concurrentes (Analysis of Competing Hypotheses – ACH)*

Cette procédure nous paraît être un excellent canevas pour le développement et l'évaluation d'hypothèses, et je ne peux que recommander à chaque analyste de la mettre en pratique et de l'expérimenter pour en mesurer tout le bénéfice.

Les points 1 et 2 de la procédure décrivent la méthode proposée pour la génération d'hypothèses, HEUER recommande ici de faire appel à un groupe d'analystes avec des expériences et des profils différents. Cette recommandation permet de minimiser le risque de ne pas générer une hypothèse qui pourrait être la bonne simplement parce que celle-ci n'était pas imaginable par un analyste avec un certain profil. Rappelons toutefois que HEUER recommande de ne pas dépasser sept hypothèses concurrentes, faute de quoi leur évaluation devient rapidement ingérable. Lors de la collecte et du rassemblement des éléments probants (*evidence* dans le texte original), il faut relever autant la présence d'un élément probant que son absence. L'absence d'un élément probant est souvent négligée, voire même inconsciemment occultée des réflexions.

---

<sup>387</sup> HEUER, *op. cit.*, 1999, (p. 97). Nous renvoyons le lecteur au chapitre 8 de cet ouvrage de référence s'il désire avoir un commentaire complet sur cette procédure.

***Step-by-Step Outline of Analysis of Competing Hypotheses***

1. *Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.*
2. *Make a list of significant evidence and arguments for and against each hypothesis.*
3. *Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the “diagnosticity” of the evidence and arguments—that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.*
4. *Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.*
5. *Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.*
6. *Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.*
7. *Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.*
8. *Identify milestones for future observation that may indicate events are taking a different course than expected.*

*fig. 182 : Procédure d'analyse d'hypothèses concurrentes*

Le point 3 nous paraît être le plus important. La représentation matricielle des hypothèses et des éléments probants est un procédé qui permettra à l'analyste de suivre le protocole jusqu'au bout et lui évitera de faire trop rapidement des choix en fonction de l'hypothèse la plus probable, la plus dangereuse, la plus satisfaisante ou la plus consensuelle, en fonction des besoins ou des sentiments du moment.

HEUER propose de peupler sa matrice en se posant la question pour chaque élément probant, s'il est conforme, contradictoire ou s'il ne s'applique pas avec chacune des hypothèses. Bien que la liberté soit laissée à l'analyste pour le choix des marqueurs qui seront utilisés, HEUER propose d'utiliser les signes « + », « - » et « ? » pour résumer les évaluations, aussi complexes qu'elles puissent être.

L'auteur signale encore que si le besoin se faisait sentir, il peut être nécessaire d'ajouter une colonne contenant une pondération des éléments probants entre eux, sur le modèle de ce qui est fait pour les matrices d'aide à la décision, ou d'une autre colonne qui permette d'ajouter la qualification de la qualité de l'élément probant. Ce dernier point nous semble fort à propos dans notre contexte, puisque cette évaluation est une des tâches qui fait partie du cycle du renseignement, il serait donc stupide de ne pas en tenir compte lors de l'analyse.

La question de la « diagnosticité » (*diagnosticity* dans le texte original) consiste à sélectionner les éléments probants qui ont la même valeur pour l'ensemble des hypothèses. Si c'est le cas, cet élément n'apporte rien et peut être éliminé à l'étape suivante.

La figure ci-dessous reproduit l'exemple qui est donné par HEUER. Le sujet traité est l'estimation de la réaction irakienne suite au bombardement Etats-unien du Quartier général des services secrets irakiens en 1993.

**Figure 15**  
**Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?**

Hypotheses:  
H1 - Iraq will not retaliate.  
H2 - It will sponsor some minor terrorist actions.  
H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate.	+	+	+
E2. Absence of terrorist offensive during the 1991 Gulf War.	+	+	-
E3. Assumption that Iraq would not want to provoke another US attack.	+	+	-
E4. Increase in frequency/length of monitored Iraqi agent radio broadcasts.	-	+	+
E5. Iraqi embassies instructed to take increased security precautions.	-	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.	--	+	+

fig. 183 : Exemple de matrice d'analyse d'hypothèses concurrentes<sup>388</sup>

Les étapes suivantes de la procédure d'analyse d'hypothèses concurrentes d'HEUER consistent en l'affinage de la matrice à l'étape 4 par la reformulation des hypothèses (si cela est nécessaire), ainsi qu'à l'élimination des éléments qui sont équiprobants. Le point 5 propose d'évaluer la vraisemblance relative des hypothèses les unes par rapport aux autres en travaillant dans les colonnes de la matrice. La méthode scientifique veut qu'une hypothèse corroborée par des faits puisse être considérée comme vraie tant qu'elle n'a pas été falsifiée, c'est à dire mise en défaut par une observation ou une expérimentation contraire à ses prédictions. Pour HEUER, c'est ce même principe qu'il faut appliquer, en recherchant des éléments contraires plutôt que corroboratifs.

Le point 6 sert à affiner l'analyse en mettant en avant les éléments probants sensibles, soit parce qu'ils ne sont pas encore confirmés mais que leur rôle est capital, soit parce qu'ils peuvent être sujets d'une autre interprétation, par exemple si on ne peut déterminer si un élément est la cause ou

<sup>388</sup> Tiré de HEUER, *op. cit.*, 1999 (p. 101)

la source d'un événement. Ensuite, l'étape 7 demande de tirer ses conclusions, en ne commentant pas uniquement l'hypothèse privilégiée, mais en tenant aussi compte des autres.

Enfin la dernière recommandation propose de mettre en avant des repères auxquels il faut s'attendre ou des éléments déterminants à rechercher activement qui permettraient de favoriser telle ou telle hypothèse.

L'*analyse d'hypothèses concurrentes* telle que décrite ici ne permet pas de garantir que la bonne solution sera trouvée. Cependant, elle permet, encore une fois de suivre une procédure éprouvée. Elle permet également de décomposer les étapes du processus analytique et de pouvoir retourner à un point de désaccord précis. HEUER concluait de la sorte :

« Analysis of competing hypotheses does, however, guarantee an appropriate process of analysis. This procedure leads you through a rational, systematic process that avoids some common analytical pitfalls. It increases the odds of getting the right answer, and it leaves an audit trail showing the evidence used in your analysis and how this evidence was interpreted. If others disagree with your judgment, the matrix can be used to highlight the precise area of disagreement. Subsequent discussion can then focus productively on the ultimate source of the differences. » (p. 109)

Bien que toutes ces recommandations paraissent excellentes, nous ne pouvons nous empêcher de faire écho aux sciences forensiques. Comme nous l'avons vu plus avant, les criminalistes ont mis en place toute une stratégie pour pouvoir évaluer la valeur probante des indices qui leur sont soumis. L'approche bayésienne est aujourd'hui largement acceptée dans cette communauté scientifique. Ainsi, même des situations complexes décrivant des suites d'événements peuvent être modélisées et résolues à l'aide de *Réseaux bayésiens*.

Nous pensons que cette approche pourrait être utilisée dans l'*analyse des hypothèses concurrentes*. Ainsi, plutôt que d'utiliser des estimations de la valeur probante d'un élément sous la forme de « + », « - » et « ? », il serait peut-être judicieux de tenter d'utiliser des probabilités conditionnelles, sous la forme de rapports de vraisemblance (LR<sup>389</sup>), selon l'application de la théorie de Bayes.

Cette approche bayésienne dans l'analyse du renseignement a déjà été évaluée dans les années 1970, mais un document déclassifié de ZLOTNICK<sup>390</sup> n'y est pas très favorable et il doute des améliorations qu'elle pourrait apporter.

---

<sup>389</sup> LR = *Likelihood Ratio*

<sup>390</sup> ZLOTNICK, *Bayes' Theorem for Intelligence Analysis*, 1972. Ce document a été déclassifié par le CIA en 1995.

Plus récemment, dans une thèse de l'Université de Stanford, McLAUGHLIN<sup>391</sup> remet l'approche probabiliste sur le devant de la scène. Son travail a, par exemple, consisté à reconsidérer les éléments en possession des analystes sur la période 1991 – 2003 au sujet du programme nucléaire irakien et des armes de destruction massive qui ont été à l'origine de la deuxième guerre d'Irak en 2003.

Chacun des éléments à disposition a été évalué selon la méthode probabiliste bayésienne en enchaînant les probabilités conditionnelles. Le résultat a été que rapidement en appliquant cette méthode de « mise à jour bayésienne » (*Bayesian updating model* dans le texte original issu des travaux de PATE-CORNELL<sup>392</sup>), la vraisemblance de l'hypothèse d'un programme nucléaire irakien a rapidement baissé pour finir avec un rapport proche de zéro.

L'approche de McLAUGHLIN est la suivante :

« The Bayesian method is based on a definition of probability as the degree of belief of a decision maker (see for example, Savage, 1954; Bunn, 1984).

It relies first on the choice of hypotheses, structured as a mutually exclusive, collectively exhaustive set, regarding a phenomenon. Second, it requires the assessment of the prior probabilities of these hypotheses, before updating on the basis of a succession of events (signals). Third, one needs to encode the likelihood of these observed events given these different hypotheses and the evidence so far. One can then compute a posterior probability of each hypothesis given the observed event at a given time.

This probability then becomes the “prior” to be updated in the next periods given new events. One can thus compute a sequentially updated estimate of the probability of each hypothesis. The Bayesian method thus offers a quantitative alternative to the current analysis of competing hypotheses by estimating their probabilities conditional on evolving information. Its application to the analysis and the fusion of intelligence information was described elsewhere (Paté-Cornell, 2001).

The notation is as follows:

E = an event or signal relating (in this hypothetical example) to the Iraqi nuclear weapons program

NE = the negation of the event E

A = a hypothesis describing the uncertainty about the state of that program

p(A) = prior probability of A before updating on the basis of signal E

p(NA) = probability of NOT A, i.e., of the set of scenarios that do not include A

---

<sup>391</sup> McLAUGHLIN, A Bayesian Updating Model for Intelligence Analysis: A Case Study of Iraq's Nuclear Weapons Program, 2005. Ce travail a reçu le prix 2005 du Center for International Security and Cooperation et a été présenté lors de l'International Conference on Intelligence Analysis, du 2-4 mai 2005.

<sup>392</sup> PATE-CORNELL, Fusion of Intelligence Information: a Bayesian Approach, Risk Analysis Vol. 22, No. 3, 2001, pp.445-454, cité par McLAUGHLIN, *op.cit.*, 2005



$p(E)$  = probability of event (signal) E, or preposterior probability of the evidence

$p(E|A)$  = likelihood function i.e., conditional probability of event (signal) E given that A is true

$p(A,E)$  = joint probability of both E and A

$p(A|E)$  = posterior probability of hypothesis A conditional on the observation of event or signal E.

$\{E\}_t$  = set of events observed up to and including time t

$E_{t+1}$  = event observed at time t+1

X = any of the hypotheses (A, B, or C ) considered here

According to Bayes' theorem (or the definition of conditional probability), the probability that hypothesis A is true given an event E is:

$$p(A|E) = p(A,E) / p(E) \quad \text{Eq. 1}$$

$$p(A | E) = \frac{p(A) \times p(E | A)}{p(A) \times p(E | A) + p(NA) \times p(E | NA)} \quad \text{Eq. 2}$$

This method offers several advantages. First, it requires that the analysts generate and consider the possibility of an exhaustive set of alternative hypotheses. Second, it requires that they explicitly quantify their judgments about priors and likelihoods, making the analysis process more transparent and reducing the tendency to favor a single hypothesis or to support previously held positions. This process demands consideration of the possibility of false positives and false negatives. Third, it enables the analyst to focus on the accurate representation of uncertainties given the current evidence and the fusion of all previous data.

Equations 1 and 2 only represent the first step of analysis at time  $t_0$ . This step is repeated every time a new signal (event) is observed. The previous posterior then becomes the prior for a new round of updating. At time t, the result of this iterative process thus represents the evidence accumulated so far. Because the observed events are generally not independent, the updating needs to be made based on the conjunction of all previously available events, including the one that was observed at time t. (...)

Since the events observed relating to a given hypothesis are not independent, the likelihood functions must account for the fact that  $E_t$  may be dependent on some events that have always been accounted for in previous updating steps up to time t-1. This prevents doublecounting of overlapping events (signals) and assesses the informational value added by each one. For instance, the probability of event 4 conditional on event 1 and 2 and hypothesis A (or B) is higher than the conditional probability of event 4 conditional on A alone because the information in event 4 reinforces that contained in events 1 and 2 given hypothesis A. For the simple case of two events (or signals), E1 and E2, it was shown in earlier work (Paté-Cornell, 2001) that the results of the updating can be very different if one assumes independence vs. dependence of the two pieces of information.

Note, for example, that if an event  $E_t$  is already contained in the set  $\{E\}_{t-1}$ , it has no value of information because the set  $\{\{E\}_{t-1} \text{ and } E_t\} = \{E\}_{t-1}$ . Therefore, they have the same probability. This implies that repeating the observation of the same event would not affect the updated probability of the hypotheses. Note also that for an expert to estimate the conditional probability of an event given a hypothesis and all previously available information is generally not more complex than thinking about  $p(E|A)$  alone. In fact intuitively, it may be the most natural way to process the information.

The likelihood functions assigned in this paper are meant for illustrative purposes only, and are not meant to challenge the estimate produced by the intelligence community because it is not based on the same information. An experienced analyst would likely be able to assign more accurate values of these estimates; but such estimates represent only the degrees of belief of the analysts as opposed to “exact” percentages because there is generally no statistical sample allowing a “frequentist” analysis of the evidence. The challenge may be to reach a consensus on these figures; but in any case, the exercise will clearly reveal the sources of disagreement.

The figures in second column of Table 2 [*note: l’auteur fait ici référence à une table qui illustre ses propos*], the likelihood (conditional probability) that the event occurs given that the hypothesis X is NOT true and given the set of events observed previously,  $p(E_{t+1}|NX, \{E\}_t)$ , is computed based on the values assigned in the first column. It is derived from the Bayesian formula described above and the mutually exclusive and collectively exhaustive relationship among the three hypotheses. This implies that  $p(A) + p(B) + p(C) = 1$ , and that  $p(NA) = p(B) + p(C)$ .

Combining Bayes’ theorem and these relationships:

$$p(E_{t+1}|NA, \{E\}_t) = p(E_{t+1}, NA, \{E\}_t) / p(NA, \{E\}_t) \tag{Eq. 3}$$

Dividing the numerator and denominator by  $p(\{E\}_t)$  and making substitutions according to the relationships among hypotheses:

$$p(E_{t+1} | NA, \{E\}_t) = \frac{p(E_{t+1}, B) + p(E_{t+1}, C)}{p(B) + p(C)} \tag{Eq. 4}$$

$$= \frac{p(E_{t+1} | B) \times p(B) + p(E_{t+1} | C) \times p(C)}{p(B) + p(C)} \tag{Eq. 5}$$

Symmetric relationships are obtained for the other two hypotheses NB and NC.

The third column of Table 2 represents the posterior probability of each hypothesis as a function of its prior probability - before the most recent event - and the likelihoods of the event (signal) given that hypothesis or its negation and the previous observations. By propagating these assessments down the model, we obtain a sequentially updated posterior probability for each of the three hypotheses, according to the following formula derived from Bayes’ theorem. The updating at time t is:

$$p_t(A) = p(A | \{E\}_t) \tag{Eq. 6}$$

$$p_{t+1}(A) = p(A | \{E\}_t, E_{t+1}) \tag{Eq. 7}$$

$$p_{t+1}(A) = \frac{p(\{E\}_t) \times p(A | \{E_t\}) \times p(E_{t+1} | A, \{E\}_t)}{p(\{E\}_t, E_{t+1})} \tag{Eq. 8}$$

$$p_{t+1}(A) = \frac{p(\{E\}_t) \times p_t(A) \times p(E_{t+1} | A, \{E\}_t)}{p(\{E\}_t) \times p_t(A) \times p(E_{t+1} | A, \{E\}_t) + p(\{E\}_t) \times p_t(NA) \times p(E_{t+1} | NA, \{E\}_t)} \tag{Eq. 9}$$

Dividing the numerator and the denominator by  $p(\{E\}_t)$ :

$$p_{t+1}(A) = \frac{p_t(A) \times p(E_{t+1} | A, \{E\}_t)}{p_t(A) \times p(E_{t+1} | A, \{E\}_t) + p_t(NA) \times p(E_{t+1} | NA, \{E\}_t)} \tag{Eq. 10}$$

Note:  $\{E\}_t$  is the set of signals observed before  $t+1$ , and  $p_{t+1}(A)$  is the posterior probability of  $A$  after updating at time  $t$  based on  $E_{t+1}$ . » (p. 1-4)

#### 4.3.1.5 Matrice d’analyse bayésienne d’hypothèses concurrentes

Nous préconisons un modèle qui combine la matrice d’analyse d’hypothèse concurrente, avec la méthode de mise à jour bayésienne des connaissances décrite ci-dessus, bien que nous ne sommes en général pas en présence d’un enchaînement d’événements probants, mais confrontés à l’analyse de plusieurs éléments qui n’ont pas forcément de relation chronologique, si ce n’est le moment où l’analyste en a pris connaissance, ce qui n’est pas réellement pertinent.

	p	H <sub>1</sub>	H <sub>2</sub>	...	H <sub>n</sub>
E <sub>1</sub>	p(E <sub>1</sub> )	p(E <sub>1</sub> )·[LR(H <sub>1</sub>   E <sub>1</sub> )]	p(E <sub>1</sub> )·[LR(H <sub>2</sub>   E <sub>1</sub> )]		p(E <sub>1</sub> )·[LR(H <sub>n</sub>   E <sub>1</sub> )]
E <sub>2</sub>	p(E <sub>2</sub> )	p(E <sub>2</sub> )·[LR(H <sub>1</sub>   E <sub>2</sub> )]	p(E <sub>2</sub> )·[LR(H <sub>2</sub>   E <sub>2</sub> )]		p(E <sub>2</sub> )·[LR(H <sub>n</sub>   E <sub>2</sub> )]
E <sub>3</sub>	p(E <sub>3</sub> )	p(E <sub>3</sub> )·[LR(H <sub>1</sub>   E <sub>3</sub> )]	p(E <sub>3</sub> )·[LR(H <sub>2</sub>   E <sub>3</sub> )]		p(E <sub>3</sub> )·[LR(H <sub>n</sub>   E <sub>3</sub> )]
E <sub>4</sub>	p(E <sub>4</sub> )	p(E <sub>4</sub> )·[LR(H <sub>1</sub>   E <sub>4</sub> )]	p(E <sub>4</sub> )·[LR(H <sub>2</sub>   E <sub>4</sub> )]		p(E <sub>4</sub> )·[LR(H <sub>n</sub>   E <sub>4</sub> )]
...					
E <sub>n</sub>	p(E <sub>n</sub> )	p(E <sub>n</sub> )·[LR(H <sub>1</sub>   E <sub>n</sub> )]	p(E <sub>n</sub> )·[LR(H <sub>2</sub>   E <sub>n</sub> )]		p(E <sub>n</sub> )·[LR(H <sub>n</sub>   E <sub>n</sub> )]
		V(H <sub>1</sub> )	V(H <sub>2</sub> )		V(H <sub>n</sub> )

fig. 184 : Matrice d’analyse bayésienne d’hypothèses concurrentes

Légende :

H<sub>n</sub> : Hypothèse ; E<sub>n</sub> : Elément ou évidence ; p(E<sub>n</sub>) : pondération de l’élément ; LR(H<sub>n</sub>| E<sub>n</sub>) : Likelihood ratio ; p(E<sub>n</sub>)·[LR(H<sub>n</sub>| E<sub>n</sub>)] : Likelihood ratio pondéré ; V(H<sub>n</sub>) : Calcul de la vraisemblance de l’hypothèse (selon le Bayesian updating model développé par MCLAUGHLIN).

Ce modèle est basé sur la construction d’une matrice selon les recommandations de HEUER, puis sur son peuplement par des rapports de vraisemblances, tels qu’utilisés en criminalistique.

L'utilisation de valeurs numériques a l'avantage de pouvoir réellement utiliser la pondération de la qualité de l'élément incertain. Ainsi, un élément qui pourrait avoir un LR élevé pour une des hypothèses, mais une vraisemblance faible, s'en trouvera justement contrebalancé.

La vraisemblance globale d'une hypothèse étant égale au produit des rapports de vraisemblance pondérés.

Un autre avantage de pouvoir disposer d'estimations numériques est qu'il sera plus aisé de commenter l'ensemble des hypothèses, avec leur incertitude propre, comme le recommande HEUER. Selon lui, dans un article récent publié en 2005<sup>393</sup>, c'est bien la non-communication des incertitudes liées à chacune des hypothèses qui est réellement en cause dans l'analyse défailante de la présence d'armes de destruction massives en Irak. Les analyses ont souffert des biais contextuels connus (ancrage et confirmation) amplifiés par la très grande pression institutionnelle. Ainsi, une approche trop intuitive a été privilégiée et les incertitudes des hypothèses n'ont pas été communiquées. Avec une *matrice d'analyse bayésienne d'hypothèses concurrentes*, la vraisemblance de chacune des hypothèses peut être estimée numériquement, puis clairement communiquée.

Afin d'illustrer l'utilisation de cette nouvelle matrice bayésienne, reprenons l'exemple du sadique zoophile déjà évoqué précédemment.

Lorsque le premier cas suspect s'est présenté dans le canton de Neuchâtel le 19 août 2005, l'hypothèse du sadique zoophile était déjà largement privilégiée et médiatisée par la presse écrite radiophonique et télévisée. Un facteur émotionnel important s'était aussi déjà répandu dans l'opinion publique.

Deux autres cas ont encore été recensés dans le canton de Neuchâtel en septembre. Ce n'est qu'à fin septembre que la police neuchâteloise a pu présenter publiquement ses conclusions, alors que près de 50 cas étaient encore attribués à ou aux sadique(s) zoophile(s) dans le Nord-Ouest de la Suisse.

Nous reprenons pour l'exemple les hypothèses qui ont été élaborées durant l'enquête par les policiers neuchâtelois<sup>394</sup>, pour ne pas biaiser cette illustration avec un quelconque *a priori*, ces six hypothèses ont une probabilité initiale de 1/6 :

---

<sup>393</sup> HEUER, *Limits of Intelligence Analysis*, 2005

<sup>394</sup> GUÉNIAT, Chef de la police de sûreté neuchâteloise, communication personnelle

- H<sub>1</sub> : Intervention humaine
- H<sub>2</sub> : Automutilation
- H<sub>3</sub> : Intermutilation
- H<sub>4</sub> : Mutilation accidentelle
- H<sub>5</sub> : Mort naturelle avec passage de carnivores
- H<sub>6</sub> : Fraude à l'assurance & imitation

Afin de tester ces hypothèses, il était nécessaire de récolter des indices. C'est pourquoi, étant donné le contexte de psychose qui régnait dans l'arc jurassien et pour éviter que des actes de justice privée ne se produisent, des moyens importants ont été mis en œuvre, soit<sup>395</sup> :

- E<sub>1</sub> : Recherches sur les lieux (personnes ou véhicules)
- E<sub>2</sub> : Interprétation de l'origine des lésions superficielles (comparaisons)
- E<sub>3</sub> : Causes de la mort (autopsie)
- E<sub>4</sub> : Analyses toxicologiques (recherche de sédatifs)
- E<sub>5</sub> : Analyses ADN
- E<sub>6</sub> : Analyses de poils
- E<sub>7</sub> : Analyses rétroactives (sur 5 ans)

Nous ne détaillerons pas ici les calculs de *Likelihood ratio* qui nous permettront de peupler la matrice bayésienne d'analyse d'hypothèses concurrentes. Ils sont reproduits à l'annexe IV. La figure ci-dessous présente un exemple de l'utilisation de ce type de matrice dans ce cas<sup>396</sup>.

	p(E <sub>n</sub> )	H <sub>1</sub>	H <sub>2</sub>	H <sub>3</sub>	H <sub>4</sub>	H <sub>5</sub>	H <sub>6</sub>
E <sub>1</sub>	0.8	0.5000	0.0001	0.0008	0.0080	0.7920	0.5000
E <sub>2</sub>	0.8	0.4444	0.0001	0.0008	0.0008	79.2000	0.4444
E <sub>3</sub>	0.95	0.0010	0.0001	0.0010	0.0010	950.00	0.0010
E <sub>4</sub>	1	0.2000	100.00	100.00	100.00	100.00	0.2000
E <sub>5</sub>	1	0.0111	0.0111	0.0111	0.0111	1'000.00	0.0111
E <sub>6</sub>	0.9	0.0100	0.0100	0.0100	0.0100	900.00	0.0100
E <sub>7</sub>	0.6	0.3000	0.0060	0.0600	0.1200	0.3000	0.3000
		1.917E <sup>-09</sup>	4.695E <sup>-17</sup>	4.697E <sup>-13</sup>	9.421E <sup>-12</sup>	0.999999985	1.917E <sup>-09</sup>

fig. 185 : Exemple de l'utilisation d'une matrice bayésienne d'analyse d'hypothèses concurrentes

Grâce à cette matrice, on remarque que la différence de vraisemblance entre l'hypothèse H<sub>5</sub> (Mort naturelle avec passage de carnivores) et les autres est frappante. Mais cette différence est surtout

<sup>395</sup> GUÉNIAT, *op. cit.*, communication personnelle

<sup>396</sup> Nous ne nous sommes basés que sur les cas neuchâtelois et une connaissance partielle des dossiers pour estimer la valeur des différents rapports de vraisemblance (LR), qui sont à l'entière responsabilité de l'auteur de cette recherche. La dernière ligne ne reprend pas uniquement les facteurs V(H<sub>i</sub>) tels que décrits dans la figure 184, mais la probabilité a posteriori de H<sub>i</sub>, en fixant une équiprobabilité *a priori* pour chacun des 6 H<sub>i</sub> (1/6). Ici, le but de cette matrice est illustratif et non démonstratif.

due aux éléments probants  $E_2, E_3, E_5$  et  $E_6$ , qui sont des analyses scientifiques des plaies, de la cause de la mort et des microtraces retrouvées sur les cadavres. L'élément  $E_4$ , soit les examens toxicologiques, est également important, mais il est moins probant, puisqu'il ne privilégie pas une seule des hypothèses.

Enfin, les recherches sur les lieux et les examens circonstanciels de cas similaires rencontrés lors des cinq dernières années montrent clairement que ces éléments n'ont un caractère probant que très faible et même s'ils montrent que les hypothèses d'auto-, d'inter- ou de mutilation accidentelle sont moins vraisemblables, les différences entre l'intervention humaine sadique ou cupide et une mort naturelle sont très ténues et les vraisemblances seraient du même ordre.

	$p(E_n)$	$H_1$	$H_2$	$H_3$	$H_4$	$H_5$	$H_6$
$E_1$	0.8	0.5000	0.0001	0.0008	0.0080	0.7920	0.5000
$E_7$	0.6	0.3000	0.0060	0.0600	0.1200	0.3000	0.3000
		<b>0.1662</b>	<b>5.132E<sup>-07</sup></b>	<b>5.1333E<sup>-05</sup></b>	<b>1.029E<sup>-03</sup></b>	<b>0.2691</b>	<b>0.1662</b>

fig. 186 : Exemple d'éléments peu probants

Comme le montre la figure ci-dessus, en s'en tenant à ces simples constatations, les enquêteurs ne pouvaient raisonnablement pas se déterminer sur l'une ou l'autre des hypothèses  $H_1, H_5$  et  $H_6$ . Il était absolument nécessaire de recourir à des examens scientifiques plus poussés pour obtenir des éléments réellement probants. Ces cas pouvaient, au début, sembler bénins et il est compréhensible que des examens lourds n'aient pas été immédiatement entrepris. Ces analyses scientifiques ont nécessité du temps, et c'est durant ce laps de temps que les médias ont pu exploiter l'hypothèse naturellement la plus rentable pour eux et décrier l'apparente inaptitude de la police.

Une fois qu'une hypothèse véhiculant un facteur émotionnel aussi élevé est avancée, un *effet d'ancrage* important apparaît et il faut des preuves suffisamment fortes pour ramener la majorité à la raison.

Nous espérons avoir présenté ici une procédure de production et de test d'hypothèses concurrentes qui limite des jugements trop intuitifs et qui devrait permettre d'éviter ou tout du moins de détecter les pièges cognitifs les plus fréquemment rencontrés.

### 4.3.2 Perspectives de l'automatisation

Le développement informatique actuel et son intégration quasi permanente dans notre vie quotidienne pourrait nous faire penser que l'étape d'analyse peut elle aussi être entièrement automatisée et effectuée par des systèmes informatiques « intelligents ».

Mais, les possibilités de ce qu'on appelle communément l'intelligence artificielle (IA) ont été revues à la baisse après que certains fantasmes de science-fiction se sont envolés avec le passage

dans le nouveau millénaire. La puissance de calcul phénoménale des superordinateurs est principalement utilisée aujourd'hui afin de réaliser des simulations de phénomènes physiques certes excessivement complexes, mais répondant tout de même à des lois. Ces simulations sont utilisées par exemple pour l'étude de l'évolution des phénomènes météorologiques, à court, moyen ou même à long terme, comme le réchauffement climatique. Cette capacité de simulation appliquée au jeu d'échecs<sup>397</sup> a permis à l'intelligence artificielle, dans un contexte médiatique, de dépasser l'intelligence de l'homme. La machine ne fait là également que simuler un nombre phénoménal de possibilités de jeu, celui-ci étant basé sur un nombre restreint de règles, mais dont les combinaisons de jeu sont effectivement très nombreuses.

La révolution de l'information qui a connu un développement aussi rapide qu'inattendu par sa globalisation grâce à Internet et aux télécommunications mobiles a rendu l'information instantanée, globale et digitale, c'est-à-dire à la portée de systèmes « d'interception » et d'analyse.

Ce fut alors dans le milieu du renseignement la grande illusion du SIGINT<sup>398</sup> (*Signal Intelligence*), par opposition à l'HUMINT (*Human Intelligence*). Le premier faisant appel à l'analyse des données issues de l'interception de communications et le second à la récolte de renseignements par le biais d'agents de renseignement. La masse de données issues de l'interception de communications, recoupées avec d'autres bases de données massives, issues des administrations et des sociétés privées, a permis un développement important de techniques de *Data Mining*, qui devaient, espérait-on, permettre de détecter et de prévenir des actes criminels ou terroristes.

Mais les événements ont démontré que des techniques axées et focalisées sur des analyses automatiques n'étaient pas suffisantes et ne remplaçaient en aucun cas l'intelligence humaine.

L'Histoire retiendra sans doute le 11 septembre 2001 comme un exemple particulièrement frappant de cette trop grande confiance accordée à ce type d'intelligence<sup>399</sup>.

Par la suite, les Etats-Unis, notamment, ont placé d'importants espoirs dans la détection des terroristes par l'établissement de leurs « profils » et la recherche de personnes répondant à ces profils types. Tout ceci s'accompagnant de mesures plus dissuasives que réellement efficaces,

---

<sup>397</sup> En 1997, le logiciel *Deep Blue* d'IBM battait le Grand Maître Gary KASPAROV aux échecs.

<sup>398</sup> Il s'agit à la base de notions de la conduite de la guerre électronique. Le SIGINT, qui consistait principalement jusqu'au tournant du millénaire dans les interceptions hertziennes, est divisé en deux sous-catégories qui sont le COMINT pour *Communication Intelligence* et l'ELINT pour *Electronic Intelligence*. Le COMINT est l'interception des communications et l'analyse de leur contenu. L'ELINT est l'analyse du support des télécommunications. [CHARRET, 2006]

<sup>399</sup> À prendre au sens du renseignement. Pour plus de détails, voir le rapport de la commission sur le 11 septembre: THE 9/11 COMMISSION REPORT, Final Report of the National Commission on Terrorist Attacks Upon the United States, U.S. Government Printing Office, ISBN 0-16-072304-3

comme l'enregistrement des empreintes digitales d'un seul doigt ainsi que d'une prise de vue faciale sommaire et de mauvaise qualité lors de tous les passages aux frontières<sup>400</sup>.

L'ouvrage de MENA<sup>401</sup> nous en dit long sur cette doctrine principalement états-unienne ramenée au contexte de la lutte contre la criminalité et de la sécurité intérieure.

Il en ressort toutefois clairement que les techniques découlant directement de l'intelligence artificielle ne sont utilisées majoritairement que dans la détection de crimes. Ces techniques que MENA regroupe dans ce qu'il appelle le *Precrime Data Mining* passent par plusieurs processus tels que : le *Investigative Data Warehousing*, l'utilisation de *Intelligent Agents (Software Detectives)* et des *Neural Networks (Classifying Patterns)*, le *Machine Learning (Developing Profiles)* et finalement les *Criminal Patterns (Detection techniques)*.

C'est donc dans la préparation des structures et des possibilités d'accès aux données qu'apparaît l'intelligence artificielle. Puis, on la retrouve dans la création d'agents intelligents pouvant rechercher, recouper et classer l'information disponible, notamment par des systèmes de réseaux de neurones, dans le but de créer des classifications reconnaissables auxquelles on pourra attribuer un profil de risque, par exemple : légal ou criminel, inoffensif ou dangereux. L'usage ultime étant de rechercher et détecter ces profils criminels dans l'ensemble des données personnelles à disposition.

Le but recherché par les systèmes de détection est d'avoir un pouvoir discriminant maximum en jouant sur les paramètres testés, faute de quoi les réponses positives deviennent trop nombreuses et inutilisables<sup>402</sup>. Les notions de pouvoir discriminant, et faux positif ou négatif, sont bien connues du scientifique qui les utilise dans les processus forensiques de caractérisation et l'individualisation des traces. Mais, rapportées à l'humain, elles peuvent paraître disproportionnées et pas toujours suffisamment fiables, quand il s'agit de lutte contre le crime et surtout de la sécurité de l'Etat.

MENA le montre bien, ces avancées technologiques ne sont d'ailleurs réellement utiles dans le contexte judiciaire que dans la proposition de candidats pouvant présenter un lien avec un crime. Et c'est bien ce que l'enquêteur fait dans la première étape de l'enquête, la recherche du suspect et de son identification, lorsqu'il cherche à réduire la population d'intérêt. Mais, dans la phase suivante de l'enquête dite de confirmation, que constitue l'étape de structuration de la preuve, il est indispensable, selon nous, qu'elle soit aussi discrète et non-intrusive que possible, pour ne pas porter préjudice aux candidats désignés par un système de *Data Mining*. Il faut aussi relever que les

---

<sup>400</sup> Les sociétés aéroportuaires privées étaient responsables de mettre rapidement ces mesures en vigueur. Chacune étant indépendante, ou presque, des systèmes incompatibles et cloisonnés furent mis en place. L'utilité sécuritaire étant proche de zéro, des corrections ont dû être apportées par une démarche régaliennne.

<sup>401</sup> MENA, *Investigative Data Mining for security and Criminal Detection*, 2003

<sup>402</sup> Pour nous, le risque principal est évidemment le faux positif, avec ses conséquences dramatiques, si des actions opérationnelles (que se soit dans le contexte judiciaire ou de protection de l'Etat) découlent directement de ces analyses automatiques.



systèmes de comparaison d'empreintes digitales ou d'ADN poursuivent le même but, mais avec un degré d'individualisation tout différent. Leur recours doit donc être largement privilégié.

On retrouve aussi des systèmes de *Data Mining* dans la lutte contre la fraude. Par exemple, les opérateurs de téléphonie mobile, qui subissent depuis quelques années des attaques importantes de la part d'organisations criminelles, ont dû mettre en place des systèmes de détection des raccordements potentiellement frauduleux<sup>403</sup>. Une grande partie des opérateurs dispose d'un « Fraud Management System » (FMS) ou d'applications semblables. Grâce à un FMS il est possible d'automatiser la détection de la fraude en créant des alertes, qui sont basées sur des règles dynamiques préétablies par les équipes de lutte anti-fraude. Une fois la fraude détectée, les opérateurs vont, suivant son importance, déposer une plainte pénale. Dans le cas d'un dépôt de plainte, le lésé initie une enquête criminelle<sup>404</sup>, où l'investigateur désire aussi bénéficier du potentiel de l'intelligence artificielle qui est capable de détecter des éléments dans des données massives, par exemple en lui appliquant un jeu de filtres prédéfinis. Il faut bien constater que jusqu'à présent, les investigateurs ne sont aidés que par quelques outils de gestion et visualisation d'informations, et qu'ils ne disposent « que » de leur système cognitif pour résoudre ces problèmes.

#### 4.3.2.1 Concurrence ou complémentarité ?

Nous constatons que trop souvent l'intelligence artificielle est placée en concurrence directe avec l'intelligence humaine. Par exemple, dans le contexte même de l'analyse criminelle, depuis de nombreuses années se pose le problème du travail d'intégration des données, jugé toujours trop long et nécessitant trop de ressources pour l'analyste ou l'enquêteur. C'est tout naturellement que sont apparues des tentatives devant permettre à la machine de remplacer l'homme dans cette étape « mécanique » du cycle du renseignement, souvent rébarbative.

De plus en plus de logiciels de reconnaissance sémantique tentent donc de récupérer directement de l'information écrite et de la structurer automatiquement dans des bases de données en vue de leur visualisation. Mais, cette automatisation ne se fait pas sans heurts. Par exemple, LEE<sup>405</sup> conclut que l'identification d'informations par le système d'intelligence artificielle NLU (*Natural Language Understanding*) est possible et efficace, tout comme l'identification des relations entre les entités. Par contre, une limitation qui sera beaucoup plus difficile à résoudre est que ce système ne peut pas décider de lui-même si une entité trouvée dans le texte est bien la même qu'une précédente citation de celle-ci. Il faut alors avoir recours à l'intelligence humaine pour effectuer correctement cette tâche de reconstruction des données en décidant si des éléments sont relatifs à une seule entité.

---

<sup>403</sup> BERGIER & CARTIER, Les fraudes GSM : détection et contre-mesures - Collaboration entre les organisations et les instances de justice et police, 2007

<sup>404</sup> CARTIER & BERGIER, Les fraudes GSM : analyse criminelle et poursuite pénale - Collaboration entre les organisations et les instances de justice et police, 2008

<sup>405</sup> LEE, Automatic information extraction from documents: a tool for intelligence and law enforcement analysts, 1998

L'efficacité d'un système qui sépare complètement le processus d'identification et d'intégration des entités et de leurs liens avec celui de leur individualisation peut légitimement être mis en doute. L'intelligence artificielle et l'intelligence humaine, mises en concurrence au départ, sont ensuite utilisées de façon complémentaire, mais cette réunion semble forcée par les carences de l'intelligence artificielle, plutôt que conceptualisée dès le départ.

Les logiciels standards dédiés à l'analyse criminelle actuels vont également dans le sens de l'analyse sémantique des informations. Par exemple, la société *i2 inc.* a développé un nouveau produit, le *TextChart™*, qui permet de sélectionner manuellement des éléments reconnus sémantiquement dans un texte et de les représenter de manière simplifiée « en deux clics de souris » sur un schéma relationnel. Ici, l'analyse sémantique se borne, en quelque sorte, à reconnaître et à marquer dans le texte les entités et leurs liens, ce qui permet ensuite à l'analyste d'identifier et de représenter « intelligemment » ceux qui apparaissent dans ce texte.

Ces logiciels souffrent toutefois de limites importantes pour deux raisons. Premièrement, dans l'environnement judiciaire qui est le nôtre, nous ne disposons pas ou assez rarement de documents numériques ou numérisés qui permettraient l'usage de tels logiciels en routine. Deuxièmement, et c'est la raison principale, l'usage de logiciels de reconnaissance sémantique, dont on conviendra qu'ils ont malgré tout de la peine à individualiser les entités présentes, provoquent un biais dans le processus de représentation des éléments présents dans le texte. Le travail fourni par l'analyste devient une simple *paraphrase graphique* du texte. Or, ce n'est surtout pas cela que l'on attend d'un analyste.

Prenons l'exemple suivant qui est tiré d'une session de formation continue destinée à des enquêteurs qui ont reçu une formation de base en analyse criminelle au sein de la police de sûreté vaudoise et qui peuvent utiliser leurs connaissances pour réaliser des analyses simples dans le cadre de leurs propres affaires. Lors de ce cours de recyclage, ils ont eu à traiter comme exercice un cas qui avait pour objet une fusillade qui s'était produite entre deux individus inconnus et les forces de l'ordre suite à un simple contrôle d'identité. Le document qui leur était remis était le rapport d'intervention faisant état des circonstances de cet événement. Plus de la moitié du document (qui ne faisait que trois pages) concernait les circonstances qui ont amené la patrouille à effectuer le contrôle inopiné et les circonstances de la fusillade elle-même. En fin de rapport figuraient les éléments intéressants, à savoir les éléments factuels objectifs qui ont pu être retrouvés après la fusillade, lors de la perquisition de la chambre d'hôtel des auteurs, permettant l'identification probable de l'un d'entre eux et donnant des pistes pour retrouver le second (en fuite).

La grande majorité des participants au cours n'a pas pris suffisamment de recul avant de procéder à la représentation du cas. Cette prise de distance, qui constitue la phase « intelligente »

d'appréhension du cas, doit permettre à l'analyste de décider des informations qui sont utiles de celles qui ne le sont pas, par rapport à ce qu'il veut produire comme type de représentation devant faciliter son analyse ultérieure. Cette appréciation rapide et grossière du contenu et de l'utilité d'un document et de ce qu'il faut en retirer est une étape essentielle dans le processus d'analyse. L'intégration automatique d'éléments reconnus par des moyens de sélection ou de peuplement sémantique est inutile si elle n'est pas un gain de temps et si elle ne permet pas une sélection orientée, dans le but d'en retirer uniquement les éléments principaux et utiles.

Dans le cas présenté au cours, l'analyste pouvait simplement résumer les deux tiers du rapport en deux entités représentant l'événement « fusillade » et le lieu de celle-ci. La dernière partie du rapport devait, par contre, être développée dans le détail, puisqu'elle menait à de nouvelles pistes d'enquête. Sans cette phase d'appréhension, une paraphrase graphique pouvait rapidement mener à une représentation trop touffue (donc plus difficile à analyser *a posteriori*) et qui contient beaucoup d'informations superflues comme le nom des policiers, des témoins, ou l'hôpital où les blessés ont été acheminés.

Dans l'exemple qui suit, qui relate la fusillade, l'enquêtrice a su prendre le recul nécessaire face au texte pour ne conserver que les éléments utiles à la suite de l'enquête.

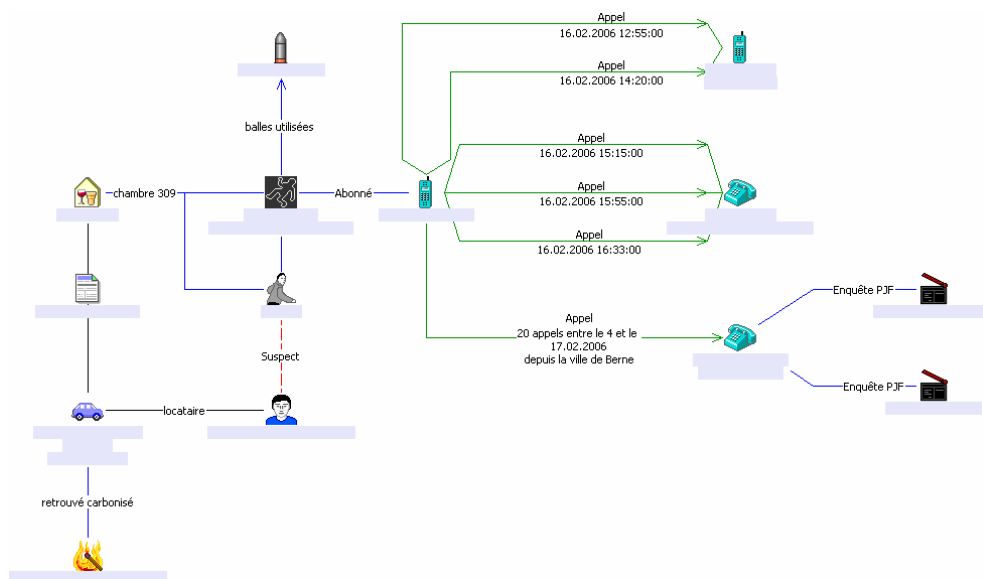


fig. 187 : Exemple de schéma fait sans paraphrase

Dans le schéma suivant, par contre, l'enquêteur a repris des éléments qui ne sont pas forcément nécessaires à la résolution du cas. Il a par ailleurs représenté graphiquement la scène violente par un face à face entre les forces de l'ordre et les auteurs (mis en évidence par l'auteur de cette recherche).

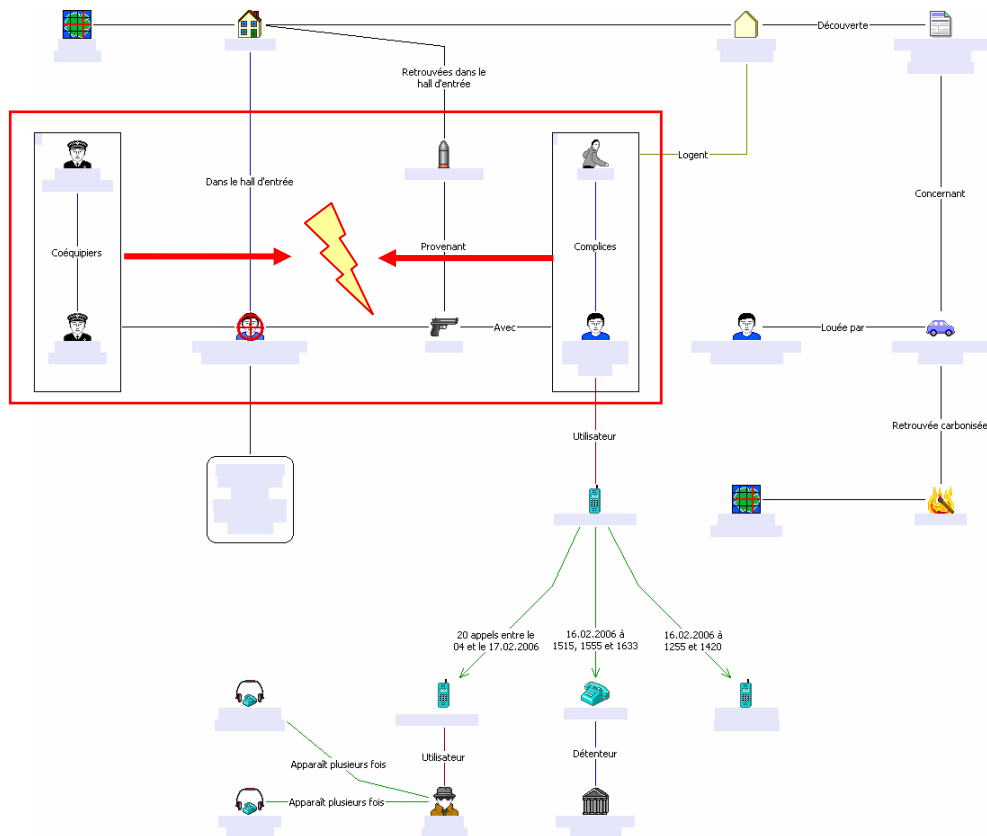


fig. 188 : Exemple de paraphrase graphique d'un texte

Du côté des outils développés pour faciliter le traitement des données, ainsi que leur visualisation, les limites de ce qui est méthodologiquement correct sont désormais peut-être déjà atteintes. Si l'extraction sémantique de données est devenue possible et performante, elle peut amener des biais et des effets secondaires qui peuvent générer des analyses globalement de moins bonne qualité, comme l'a montré l'exemple ci-dessus.

L'automatisation peut toutefois se justifier lorsque la masse d'informations à traiter n'est plus humainement accessible. Mais il ne faut pas oublier que la délégation de certaines tâches à la machine, comme par exemple l'identification d'entités individuelles, est beaucoup plus ardue et pose des problèmes encore importants aux chercheurs.

Ce n'est que grâce à des développements systémiques qui tiennent réellement compte des méthodologies et des meilleures pratiques empiriques, que des outils plus intégrés à chacune des étapes du cycle du renseignement permettront des avancées significatives.

Il faut aussi distinguer d'un côté des outils de soutien à l'analyse qui servent à améliorer la qualité du traitement des éléments factuels (comme ce projet de recherche) de ceux qui se consacrent à remplacer ou accompagner les processus cognitifs de reconnaissance de situations, de génération d'hypothèses ou encore de leur analyse comparative, comme l'analyse d'hypothèses concurrentes (qui a été présenté dans la partie précédente). Il s'agit là, de processus distincts, bien qu'ils se placent en séquence dans le cycle du renseignement, ainsi que dans l'étape d'analyse elle-même.

### 4.3.2.2 Outils informatisés d'analyse d'hypothèse concurrentes

Dans ce cadre aussi, il est primordial de construire ces outils en partant des modèles de raisonnement. CARD<sup>406</sup> l'exprimait ainsi :

« Recommendation: Build upon theoretical foundations of reasoning, sense-making, cognition, and perception to create visually enabled tools to support collaborative analytic reasoning about complex and dynamic problems. » (p. 24)

Parmi les travaux à ce sujet, il me semble intéressant que noter que ceux de HEUER sur l'analyse d'hypothèses concurrentes (*Analysis of Competing Hypotheses* – ACH) décrit précédemment ont été poursuivis avec sa collaboration au sein du Palo Alto Research Center. Ainsi, en 2006, un logiciel libre<sup>407</sup> a été mis à disposition via Internet.

Cet outil permet de créer des matrices d'analyses d'hypothèses concurrentes et de calculer des *scores de contradiction* (*Inconsistency scores*) entre les hypothèses et les éléments permettant de les comparer. Les éléments sont pondérés par deux critères, soit leur crédibilité (*Credibility*) et leur pertinence (*Relevance*).

Cette matrice n'est pas constituée de « + » et de « - », comme dans les matrices originales proposées par HEUER, mais par des listes de choix normalisées. Ainsi, les deux critères de pondération peuvent contenir les valeurs « Low », « Medium » et « High ». Les valeurs à disposition pour déterminer si un élément (*Evidence*) est conforme (*Consistent*) ou contradictoire (*Inconsistent*) avec les hypothèses sont au nombre de six, soit dans un ordre décroissant de conformité :

<b>Evaluation la conformité de l'élément :</b>	<b>Valeur</b>
Très conforme ( <i>Very consistent</i> )	« CC »
Conforme ( <i>Consistent</i> )	« C »
Neutre ( <i>Neutral</i> )	« N »
Contradictoire ( <i>Inconsistent</i> )	« I »
Très contradictoire ( <i>Very inconsistent</i> )	« II »
Ne s'applique pas ( <i>NA</i> )	« NA »

fig. 189 : Table des valeurs d'un élément (logiciel ACH 2.0.3)

La matrice permet ensuite de calculer les *scores de contradiction*, selon un modèle basé sur le modèle de calcul (multiples et puissance de 2) reproduit ci-après :

<sup>406</sup> CARD S. K., *The science of analytical reasoning*, 2005

<sup>407</sup> Le logiciel ACH 2.0.3 a été développé par le Palo Alto Research Center (PARC) en collaboration avec Richards J. HEUER, Jr. Il a été créé pour l'usage de l'U.S. Intelligence Community et ses coûts de développements ont été pris en charge par l'Intelligence Community's Advanced Research and Development Activity (ARDA) et l'Office of Naval Research (ONR). Il est téléchargeable à l'adresse suivante : <http://www2.parc.com/istl/projects/ach/ach.html>

Credibility	Relevance	Inonsistent « I »	Very Inconsistent « II »
High	High	2	4
Medium	High	1.414	2.828
Low	High	1	2
High	Medium	1.414	2.828
Medium	Medium	1	2
Low	Medium	0.707	1.414
High	Low	1	2
Medium	Low	0.707	1.414
Low	Low	0.5	1

fig. 190 : Matrice des scores de contradiction des éléments (logiciel ACH 2.0.3)

La somme de ces *scores de contradiction* détermine la valeur (négative) de la contradiction des éléments par rapport aux hypothèses posées. Il n'est jamais tenu compte des éléments pouvant corroborer une hypothèse dans le calcul, ce qui peut paraître surprenant. HEUER<sup>408</sup> s'en justifie ainsi :

« One purpose of the Inconsistency and Weighted Inconsistency Scores is to keep you focused on the need to refute hypotheses, rather than confirm them, and to help you track your progress in doing that. » (p. 23)

Cette manière radicale de ne calculer que des *scores de contradiction* peut être surprenante, mais s'agit ici d'une démarche découlant ici particulièrement de la théorie poppérienne<sup>409</sup> de la réfutation d'hypothèses.

Afin de pouvoir prendre en compte aussi bien les éléments contradictoires que conformes aux hypothèses, le recours à une *matrice bayésienne d'analyse d'hypothèses concurrentes* qui permet ensuite de calculer la vraisemblance des hypothèses selon le *Bayesian updating model* est, à nos yeux, une solution plus élaborée. En effet, elle tient compte de chaque élément qu'il confirme ou réfute une des hypothèses et qui donne des résultats très similaires, comme on le verra ci-après.

D'ailleurs, HEUER<sup>410</sup> le reconnaît également, mais il nous met en garde devant sa plus grande complexité :

« No Probability Calculation :

It may seem to some users that this ACH software could and should convert the rating of evidence in the matrix into numerical probabilities for each hypothesis rather than a simple Inconsistency or Weighted Inconsistency Score. That could be done, but it is deliberately not done for several reasons.

<sup>408</sup> HEUER, ACH Tutorial, 2006

<sup>409</sup> Voir chapitre 1.4.5.2 – Les raisonnements

<sup>410</sup> HEUER, *op. cit.*, 2006

A much more complex rating system using Bayesian statistical inference would be required to do it accurately, and the conclusions would still be no more accurate than the analyst's subjective judgments that go into rating the evidence. Other versions of ACH with greater mathematical precision have been developed for specialized purposes, but they are less practical for broad use and not easily understood by the average intelligence analyst. » (p. 24)

Pour illustrer cette description du logiciel ACH 2.0.3, nous avons reproduit la matrice de l'exemple du cas du sadique zoophile de l'arc jurassien.

#	Type	Credibility	Relevance	H: 1	H: 2	H: 3	H: 4	H: 5	H: 6
				Intervention humaine	Automutilation	Intermutilation	Mutilation accidentelle	Mort naturelle avec passage de carnivores	Fraude à l'assurance & imitation
	Weighted Inconsistency Score ⇄			-7,414	-12,828	-12,828	-11,414	-0,0	-7,414
E7	Recherches sur les lieux (personnes ou véhicules)	MEDIUM	MEDIUM	N	II	II	II	N	N
E6	Interprétation de l'origine des blessures (comparaisons)	MEDIUM	MEDIUM	N	II	II	II	C	N
E5	Causes de la mort (autopsie)	HIGH	HIGH	II	II	II	II	C C	II
E4	Analyses toxicologiques (recherche de sédatifs)	HIGH	HIGH	N	C	C	C	C	N
E3	Analyses ADN	HIGH	HIGH	I	I	I	I	C C	I
E2	Analyses de poils	MEDIUM	HIGH	I	I	I	I	C C	I
E1	Analyses rétroactives (sur 5 ans)	LOW	MEDIUM	N	II	II	N	N	N

fig. 191 : Exemple d'une matrice d'analyse d'hypothèses concurrente (logiciel ACH 2.0.3)

Il est aussi possible de représenter graphiquement la valeur des scores de contradiction (Inconsistency scores) :

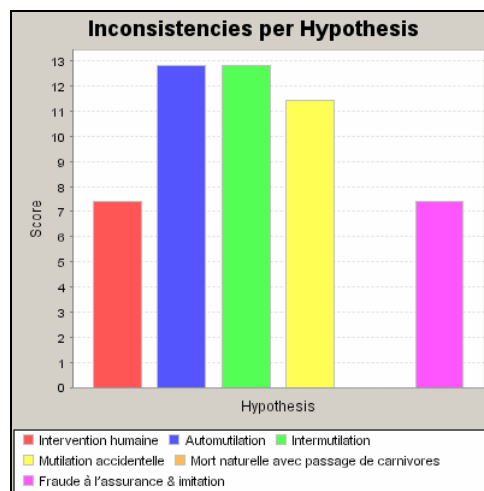


fig. 192 : Exemple d'un graphique des scores de contradiction (logiciel ACH 2.0.3)

La transposition de ces mêmes codes couleurs à la matrice bayésienne telle que présentée à la figure 185 :

	p(E <sub>n</sub> )	H <sub>1</sub>	H <sub>2</sub>	H <sub>3</sub>	H <sub>4</sub>	H <sub>5</sub>	H <sub>6</sub>
E <sub>1</sub>	0.8	0.5000	0.0001	0.0008	0.0080	0.7920	0.5000
E <sub>2</sub>	0.8	0.4444	0.0001	0.0008	0.0008	79.2000	0.4444
E <sub>3</sub>	0.95	0.0010	0.0001	0.0010	0.0010	950.00	0.0010
E <sub>4</sub>	1	0.2000	100.00	100.00	100.00	100.00	0.2000
E <sub>5</sub>	1	0.0111	0.0111	0.0111	0.0111	1'000.00	0.0111
E <sub>6</sub>	0.9	0.0100	0.0100	0.0100	0.0100	900.00	0.0100
E <sub>7</sub>	0.6	0.3000	0.0060	0.0600	0.1200	0.3000	0.3000
		1.917E <sup>-09</sup>	4.695E <sup>-17</sup>	4.697E <sup>-13</sup>	9.421E <sup>-12</sup>	0.999999985	1.917E <sup>-09</sup>

fig. 193 : Exemple de coloration d'une matrice bayésienne d'analyse d'hypothèses concurrentes

Ou représenté de manière graphique :

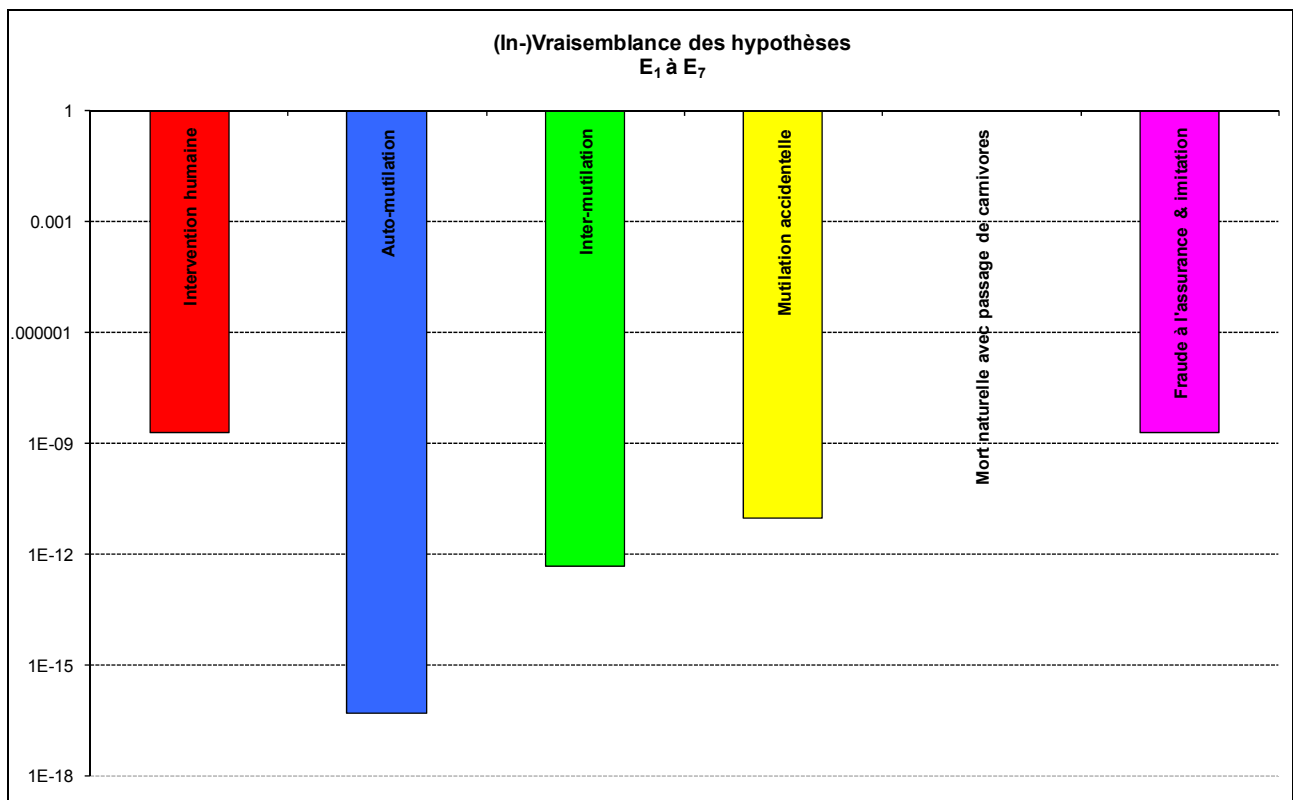


fig. 194 : Exemple d'un graphique d'une matrice bayésienne d'analyse d'hypothèses concurrentes

Les résultats des deux matrices sont comparables, mais l'utilisation d'une *matrice bayésienne d'analyse d'hypothèses concurrentes* apporte malgré tout une qualité d'analyse plus grande que ce qui est proposé par HEUER et le logiciel ACH 2.0.3 développé en collaboration avec le Palo Alto Research Center.



Dans un cas de figure où il est nécessaire de pouvoir analyser plusieurs hypothèses qui sont corroborées par des mêmes éléments, le seul calcul de *scores d'incompatibilité* n'est plus suffisant<sup>411</sup>. L'utilisation d'une matrice bayésienne devient indispensable. Par contre, elle est effectivement, comme le mentionnait HEUER, plus complexe à manipuler, nécessite plus de temps et des connaissances en statistique bayésienne.

#### 4.3.2.3 Synthèse

L'automatisation des processus en jeu dans l'analyse de données, est très utile dans des processus tels que la récolte et le traitement de ces données, d'autant plus si elles sont présentes en masse. Le processus qui mène à leur visualisation doit faire l'objet d'un soin particulier s'il est partiellement ou totalement automatisé. Il faut bien constater que les développements ne se font pas toujours dans un esprit de collaboration entre des praticiens au fait de leurs procédures et méthodes de travail et des techniciens souvent concentrés sur les performances de leurs futurs systèmes et enfermés dans leurs modèles informatiques.

Il doit en être de même avec les développements d'outils d'aide et d'encadrement de l'analyse. S'il est possible d'en automatiser une partie, ce doit être fait pas à pas en respectant les méthodologies et les schémas d'inférences utilisés par les praticiens. C'est là le challenge de la recherche appliquée à l'analyse criminelle, sur un plan pragmatique, comme le conclut CARD<sup>412</sup> dans son ouvrage sur l'analyse visuelle de données :

« Recommandation: Conduct research to address the challenges and seize the opportunities posed by the scale of the analytic problem. The issues of scale are manifested in many ways, including the complexity and urgency of the analytical task, the massive volume of diverse and dynamic data involved in the analysis, and challenges of collaborating among groups of people involved in the analysis, prevention, and response efforts. » (p. 24)

Nous avons donc proposé ici une procédure de génération puis d'analyse d'hypothèses concurrentes basée sur les recommandations d'HEUER<sup>413</sup> qui est complémentaire au système de recherche et de gestion des liens dans l'investigation criminelle liée au cas particulier de la criminalité organisée, qui a été développé dans cette recherche. Nous pensons qu'il faut s'efforcer de travailler avec une *matrice bayésienne d'analyse d'hypothèses concurrentes*, car bien que plus complexe, elle permet une analyse plus élaborée et ne se limite pas à des facteurs d'invraisemblance.

---

<sup>411</sup> Voir Annexe III où le cas du sadique zoophile est illustré plus complètement.

<sup>412</sup> CARD, *op. cit.*, 2005

<sup>413</sup> HEUER, *op. cit.*, 1999



## 5 Conclusion

Une action de sécurité, si elle suit une stratégie de résolution de problèmes se doit d'étudier le problème posé, de se donner les moyens de le comprendre et de l'analyser pour être capable de mener des actions réfléchies et dont on attend un certain résultat, si possible mesurable.

La problématique étudiée par cette recherche porte sur la criminalité organisée. Cette notion étant définie de différentes manières dans la littérature, nous avons considéré ici que la criminalité organisée doit être entendue comme un phénomène criminel formé par l'ensemble des organisations criminelles au sens large, soit comme tout groupement criminel, sans distinction *a priori* de son degré d'organisation, dont le crime organisé ou la *mafia* représente la forme extrême.

Nous pensons qu'un élément décrit dans la première partie de cette recherche, l'état des lieux des thématiques liées à la problématique étudiée et notamment de la criminalité organisée, mérite d'être repris dans cette conclusion. Nous avons en effet constaté que la mise en application en Suisse des nouvelles normes légales spécifiques adoptées dans les années 1990 n'est pas très satisfaisante du point de vue légal, comme l'ont relevé certains juristes. Ceux-ci constatent que les autorités de poursuite pénale sont bien plus souvent confrontées à des groupements criminels formant le tissu de la *criminalité organisée*, qu'à de véritables *organisations criminelles* au sens du code pénal, qui décrit les spécificités du *crime organisé*. Ces auteurs proposent de combler le vide juridique présent en Suisse à l'encontre de ces groupements criminels, en prenant exemple sur *l'association de malfaiteurs*<sup>414</sup>, notion issue du droit pénal français, ou alors de modifier l'art 260<sup>ter</sup> du code pénal en reprenant une vision moins restrictive de la *criminalité organisée*<sup>415</sup>.

Une remise en question de ces normes légales et de la jurisprudence s'y référant doit à nos yeux être entreprise, tant les résultats obtenus lors des jugements pénaux semblent être en rupture avec la perception des autorités de poursuite pénale confrontées aux délinquants agissant de manière organisée.

Cette recherche s'est ensuite naturellement concentrée sur ce qui devait permettre aux policiers de mener leur action sécuritaire face à cette menace (problème), c'est-à-dire comment collecter du renseignement et l'analyser (pilotage) et comment mener des investigations (actions essentiellement répressives).

Là également, nous avons constaté que les enquêtes criminelles qui doivent naturellement se faire dans le respect de la loi et des procédures peuvent souffrir, par exemple, du principe de territorialité

---

<sup>414</sup> DE VRIES REILINGH, La répression des infractions collectives et les problèmes liés à l'application de l'article 260<sup>ter</sup>CP relatif à l'organisation criminelle, notamment du point de vue de la présomption d'innocence, 2002

<sup>415</sup> AUGSBURGER-BUCHELI & PERRIN, Les règles de fond sur la lutte contre le crime organisé, 2006

du droit suisse et international par rapport à la liberté de mouvement dont peuvent bénéficier les criminels et qui en jouent.

Sur un plan pratique également une disparité des moyens peut être parfois perceptible. Les enquêtes qui touchent à la criminalité organisée nécessitent souvent bien plus de moyens et beaucoup plus de temps que le commun des mortels ne peut l'imaginer. Il n'est ainsi plus possible de mener à bien des investigations contre ce type de criminalité sans devoir monter des groupes *ad hoc*, qui rassemblent enquêteurs et spécialistes et qui font appel à pléthore de moyens d'enquête dits spéciaux. Les ressources à disposition des autorités limitent encore souvent le champ de ces investigations. Le nouveau code de procédure pénale suisse unifié va vraisemblablement lui aussi à l'avenir favoriser une conduite des investigations préliminaires orientée par objectifs, tout en conservant une forte réglementation.

CUSSON<sup>416</sup> relève dans son analyse de la diminution de la criminalité en Amérique du Nord dans les années 1990 que la cause, en sus des variables traditionnelles telles que la proportion des hommes de 15-25 ans dans la société, la situation économique et en particulier le taux de chômage, ou encore le nombre de policiers par rapport à la population résidente, semble être plutôt due aux progrès réalisés dans les nouvelles technologies de la sécurité privée et publique. Parmi les avancées technologiques majeures réalisées outre-Atlantique à cette époque en ce qui concerne la sécurité publique, CUSSON relève la création de bases de données centralisées (au plan national aux Etats-Unis et au Canada) regroupant par exemple les antécédents judiciaires des auteurs d'infractions ou les personnes recherchées et les objets volés.

Nous avons également vu dans le premier chapitre qu'afin de lutter plus efficacement contre le trafic de stupéfiants, il existe également en Suisse depuis le milieu des années 1990 une base de données partagée au niveau national (DOSIS). Cette base de données spécifique aux stupéfiants a évolué pour devenir, petit à petit, en suivant le rythme des réorganisations des offices centraux de police criminelle, une véritable base de données sur la criminalité organisée (ISOK), puis JANUS avec l'apparition de la nouvelle police judiciaire fédérale en 2004. Cependant, jusqu'en 2005, JANUS ne permettait pas d'envisager l'exploitation et l'analyse des liens qu'elle contenait, principalement pour des raisons conceptuelles et techniques.

L'analyse criminelle, qui est également apparue en Suisse à la fin des années 1990, peut en partie répondre à cette lacune en s'intégrant au processus d'action sécuritaire. Mais dans notre pays, l'analyse criminelle est en général encore trop souvent perçue uniquement par ses produits visibles, soit les schémas relationnels ou chronologiques et autres visualisations graphiques produits lors des enquêtes, alors que c'est la mise en pratique des méthodes sous-jacentes, et son intégration au

---

<sup>416</sup> CUSSON M., Les nouvelles technologies de la sécurité privée et publique ont-elles contribué à la décroissance de la criminalité ?, présentation faite lors de la journée du centenaire de l'Institut de Police Scientifique (IPS) de l'Université de Lausanne le 24 juin 2009

processus d'action de sécurité qui apportent une réelle plus-value à moyen et à long terme dans les organisations policières et judiciaires, puisqu'elle participe à son pilotage et à la conceptualisation de ses systèmes d'information.

Ainsi, le but de cette recherche était donc de proposer une méthode de travail basée sur un modèle d'organisation du flux de données dans l'enquête judiciaire. L'architecture de ce modèle est fondée sur deux composants interconnectés et informatisés constituant un système d'aide aux investigations criminelles dans le cadre de la lutte contre la criminalité organisée.

Concrètement, deux hypothèses sur la faisabilité et sur l'utilité de ce composant ont été testées.

1. *Il est possible de coupler aux bases de données centralisées un composant d'analyse externe évolutif qui intègre des systèmes de représentation graphique, dans le but d'analyser les relations complexes de la criminalité organisée.*
2. *L'intégration d'un composant d'analyse externe couplé aux bases de données d'enquête centralisées et par conséquent compatible avec la structure des informations qui y sont contenues, est utile à l'investigation dans le cadre de la lutte contre la criminalité organisée.*

La réalisation du projet devait être rendue possible par la mise à jour du système informatique JANUS PV, qui a eu lieu dès 2002, et par la participation de l'auteur de cette recherche au groupe d'utilisateurs de référence, afin de rendre les développeurs attentifs aux besoins des analystes, ces besoins étant souvent antinomiques à ceux des enquêteurs. Le test de ces deux hypothèses a donné les résultats suivants :

- 1.1. La base de données JANUS PV 2.0 a été mise à jour presque dans les délais et la majorité des besoins des analystes ont été entendus. Des défauts conceptuels majeurs, qui rendaient vaine toute tentative d'analyse des données dans l'ancienne architecture, ont été corrigés. On peut citer en exemple, la conservation des entités liées « objets » et leur séparation en deux niveaux de liens, lorsqu'ils sont directement liés à la personne suspecte (les « attributs ») ou indirectement (les « sous-champs ») ; ainsi que leur structuration en des rubriques spécifiques.
- 1.2. La base de données d'analyse (*prototype  $\beta$* ) a été créée selon un modèle générique qui permet de modéliser la réalité selon l'état des connaissances des investigateurs, sa structure devant permettre de traiter le plus grand nombre de situations différentes, tout en restant suffisamment rigide. Ce modèle de base de données est parfaitement compatible avec la structure et l'organisation des données de JANUS PV, permettant ainsi la création d'une interface statique ou dynamique entre les deux composants du système.

- 1.3. Malheureusement, faute de temps et de moyens, et bien que l'aspect légal soit réglé depuis longtemps<sup>417</sup>, les interfaces entre JANUS et la base de données d'analyse (*prototype  $\beta$* ) n'ont pas été réalisées jusqu'à ce jour. Il existe plusieurs raisons à cela, et elles ont été discutées plus avant. Nous espérons toujours que ces blocages techniques, organisationnels ou même budgétaires sauteront ces prochaines années, ce qui permettrait enfin à ce projet d'être entièrement mené à son terme et à la méthode de travail d'être appliquée en routine.

Néanmoins, les premières expériences ont été très positives, que ce soit avec l'un ou l'autre des deux composants, tels que décrits dans le projet de recherche :

- 2.1. JANUS PV 2.0 a obtenu une large adhésion dès sa mise en service. Des problèmes de jeunesse sont apparus, mais ils ont été corrigés. De même, la visualisation des données, telle qu'elle a été initialement implémentée, ne correspondait pas à la réalité des données. Les indications précises transmises aux développeurs, tant par les analystes de la police de sûreté vaudoise que de la police judiciaire fédérale, ont permis d'obtenir des visualisations correctes à la fin de 2009.
- 2.2. Les statistiques d'utilisation 2005-2006 semblent indiquer que le gain d'information au niveau de la base de données JANUS est bien réel et qu'il devrait encore se renforcer avec le temps. Elles expriment également une meilleure adhésion des policiers au système par une augmentation de la qualité de l'information saisie, un meilleur découpage des antécédents et une intégration déjà sensible des notions utiles à l'analyse.
- 2.3. Le *prototype  $\beta$*  a également été utilisé, en tant que modèle de bases de données d'enquête, que ce soit au sein de la police judiciaire ou lors d'exercice de la sécurité militaire, et a donné entière satisfaction. Les avantages d'un système d'analyse décentralisé sont nombreux. Il offre plus de souplesse et permet d'introduire des données non confirmées, mais qui ont leur importance dans le développement d'hypothèses ou dans l'appréciation de la situation. Il permet également de bénéficier de fonctions plus poussées d'analyse, qui ne pourraient que très difficilement être intégrées à un système mono-composant.
- 2.4. Si l'utilisation du système n'apporte aujourd'hui pas encore un gain de temps substantiel, ne diminue pas les doubles saisies ni le reformatage des données, c'est en grande partie à cause de l'inachèvement de la connexion entre les deux composants. Il semble pourtant bien qu'il permette une meilleure analyse des informations d'enquête. La structure des deux composants est plus précise, les données sont mieux décomposées et elles sont

---

<sup>417</sup> Voir l'art. 19 de l'Ordonnance JANUS de 2001

standardisées autant que possible. L'analyste devrait donc à l'avenir avoir plus de temps pour analyser.

- 2.5. Enfin, l'utilisation de tels outils nécessite du personnel spécialisé et des procédures ou directives internes aux fonctionnements des corps de police. Les moyens nécessaires à leur intégration et à leur exploitation n'étant accessibles qu'à de grands cantons disposant des capacités opérationnelles et financières, il pourrait être plus efficient de mettre certaines de ces ressources en commun, par exemple au niveau des concordats régionaux de police. Le concept d'intégration du groupe de travail suisse en analyse criminelle poursuit justement ce but. Une fois cette étape réalisée, on devrait alors pouvoir disposer, en Suisse, des conditions-cadre harmonisées aux niveaux structurels et organisationnels tout à fait favorables à la mise en pratique de telles méthodes de travail.

Ces premiers résultats, bien que largement insuffisants à nos yeux sont encourageants et doivent nous conforter dans la voie que nous avons suivie jusqu'ici. Si nous ne connaissons pas les raisons des blocages qui retardent encore aujourd'hui la réalisation complète des fonctionnalités de JANUS et demandées dès le départ par le groupe d'utilisateurs de référence, nous pouvons légitimement nous poser la question si, finalement, le projet de mise à jour de JANUS n'a été considéré comme de l'« informatique pour l'enquête », alors qu'il aurait dû relever de l'analyse criminelle, discipline systémique qui s'attache aux processus d'enquête et qui revêt le rôle de pilote dans une action sécuritaire orientée vers la résolution de problèmes.

Précisons encore que pour CUSSON<sup>418</sup> les progrès outre-Atlantique dans les années 1990-2000, période qui a vu baisser la criminalité, n'étaient pas que technologiques, mais étaient assortis d'approches stratégiques des organismes policiers basée justement sur la résolution de problèmes, modèle issu de la police communautaire (ou de proximité) et de l'action policière guidée par le renseignement (*Intelligence-Led Policing*).

Force est de constater aujourd'hui que l'influence que l'auteur de cette recherche a tenté d'avoir au sein de l'équipe de développement de JANUS depuis 2002 afin de doter les enquêteurs de moyens leur permettant de mener une action sécuritaire adaptée au problème rencontré, ne semble pas avoir été simultanément une préoccupation stratégique du management policier suisse.

Sans vouloir en trouver la cause, on peut légitimement se demander si la Suisse, pays de petite taille, et son fédéralisme, découpant les juridictions à des niveaux quasi microscopiques à l'échelle mondiale, permettent d'atteindre la taille critique permettant la mise en place de réelles stratégies policières guidées par la résolution de problèmes. Même lorsque la problématique qui nous intéresse, ici la criminalité organisée, est juridiquement dévolue au niveau fédéral, on s'est trouvé,

---

<sup>418</sup> CUSSON, *op. cit.*, 2009

lors de cette recherche, en présence d'une police nouvelle, puis en croissance, et qui ne réunissait sans doute encore pas l'expérience nécessaire à l'intégration de telles stratégies à tous les niveaux de l'organisation.

Nous sommes toutefois confiants dans l'avenir, pour autant que l'action sécuritaire à laquelle nous sommes tenus de participer en tant que policier, analyste, magistrat, expert ou auxiliaire, soit désormais vue comme un processus qu'il est nécessaire de décrire, d'analyser et de définir, non-seulement pour des raisons d'efficience budgétaire mais également d'efficacité sécuritaire.

\* \* \*

Si cette recherche a eu pour but de proposer un système d'aide aux investigations criminelles, elle aborde également quelques difficultés de la phase d'analyse du cycle du renseignement pouvant offrir des perspectives de recherches futures.

On rappellera encore ici que le processus d'analyse en tant que tel est fortement (inter-)subjectif. Les raisonnements récurrents ou non-démonstratifs font systématiquement appel au référentiel de l'analyste. Cela ne changera pas tant que l'homme sera chargé d'analyser des informations ou apprécier une situation. En tout état de cause, la technologie, par l'intelligence artificielle (IA), ne nous permet pas encore de le remplacer, de plus certains des principes de l'IA se basent justement sur des techniques d'apprentissage, qui sont des processus itératifs et de nature inductive.

La subjectivité nécessaire source de créativité<sup>419</sup> lors du développement d'hypothèse, à défaut d'être totalement maîtrisée, peut être guidée et règlementée. Lors de la phase d'analyse à proprement parler, la connaissance des pièges et biais cognitifs tels que les effets de contexte est une condition *sine qua non* à toute analyse sérieuse. De même, l'utilisation de procédures écrites pour la résolution d'analyses complexes est, à nos yeux, nécessaire.

Ainsi, reprenant les travaux de HEUER et l'approche forensique d'interprétation bayésienne de la valeur probante d'un indice matériel, nous avons proposé un système de *matrice bayésienne d'analyse d'hypothèses concurrentes*, qui permet par sa décomposition de suivre le raisonnement (inter-)subjectif de l'analyste, de le corriger le cas échéant et de le commenter dans un rapport d'analyse, en explicitant l'incertitude relative des différentes hypothèses. La poursuite de l'étude des éléments préliminaires décrits dans cette recherche et le développement d'outils informatiques permettant de guider cette étape d'analyse serait une perspective de recherche intéressante à nos yeux.

---

<sup>419</sup> PIERCE parle d'imagination. On retrouve évidemment ce qualificatif pour expliquer le mécanisme de l'abduction, génération subjective mais logique de conditions initiales à partir d'observations et de lois initiales.







## 6 Bibliographie

### 6.1 *Articles et ouvrages*

**AITKEN C. G. G., TARONI F.**, « Statistics and the Evaluation of Evidence for Forensic Scientists », Second Edition. Statistics in Practice. Wiley, 2004, ISBN-10: 0-470-84367-5

**ALBANESE J.S.**, « Organized Crime in America », Anderson, Cincinnati, 1989

**ANDREWS P.P., PETERSON M.B.**, « Criminal Intelligence Analysis », Palmer Press, Loomis, California, 1990, ISBN 0-912479-07-8

**ANTINORI A.**, « L'activité des forces de police dans la lutte contre la criminalité organisée de type mafieux en Italie », *in* Cahiers de la sécurité – Les organisations criminelles, N° 7, INHES, Paris, 2009, pp. 70-78

**AUDA G.**, « Le crime organisé, une perception variable, un concept polémique », *in* Cahiers de la sécurité – Les organisations criminelles, N° 7, INHES, Paris, 2009, pp. 16-24

**AUGSBURGER-BUCHELI I., PERRIN B.**, « Les règles de fond sur la lutte contre le crime organisé », Rapport national suisse présenté au XVIIe Congrès international de droit comparé d'Utrecht, 16-22 juillet 06, Publications de l'Institut suisse de droit comparé, No 54, Schulthess, Juillet 2006

**BACON F.**, « Novum Organum », Book I, point 46, Great book of the western World, Volume 30, originally published in 1620

**BERGIER S., CARTIER J.**, « Les fraudes GSM : détection et contre-mesures - Collaboration entre les organisations et les instances de justice et police », Revue internationale de criminologie et de police technique et scientifique (RICPTS), vol. 4, p. 479-492, 2007

**BERNIER P.**, « La normativité du raisonnement non démonstrative », *in* POLITZER, Le raisonnement humain, Collection Traité des Sciences Cognitives. Paris : Hermès, 2002, ISBN 2-7462-0501-7

**BIEDERMANN A., TARONI F.**, « Bayesian networks and probabilistic reasoning about scientific evidence when is a lack of data », Forensic Science International, N°157, p.163-167, 2006

**BIRRER S., RIBAUX O., CARTIER J. ROSSY Q., CAPT S., ZUFFEREY M.**, « Exploratory study for the detection and analysis of links between prospective advance fee fraud emails in an intelligence perspective », submitted for publication IALEIA Journal, September 2005

**BOUKRIS S.**, « Induction, probabilités et confirmation chez Carnap », *in* Revue de synthèse, Springer, Paris, Volume 127, N°1, 2006, p. 115-139

**BRODEUR J.-P.**, « Tailor Made Policing: a Conceptual Investigation » *in* BRODEUR, How to Recognize Good Policing, Thousand Oaks, Sage, 1998

**BRODEUR J.-P.**, « Le crime organisé », *in* MUCHIELLI L., ROBERT PH., Crimes et sécurité. L'État des savoirs, Paris, 2002

**BRODEUR J.-P.**, « L'enquête criminelle », *in* CUSSON M., DUPONT B., LEMIEUX F., Traité de sécurité intérieure, Presses polytechniques et universitaires romandes, 2008, ISBN 978-2-88074-755-8

**CONSEIL DE L'EUROPE**, « Analyse Criminelle – Crime organisé – Etude des meilleures pratiques no. 4 », PC-S-CO (2002) 2F, Strasbourg, juillet 2002

**CAPT S.**, « L'intégration automatique des données sous forme numérique », mémoire de thèse, IPS, mai 2005.

- CARD S. K.**, « The science of analytical reasoning », UIR-2005-17, Palo Alto Research Center (PARC), 2005.
- CARTIER J., GUENIAT O., COLE M.D.**, « Head-Space analysis of solvents in heroin and cocaine samples », *Science & Justice*, 37(3) : p.175-181, 1997
- CARTIER J.**, « La localisation des téléphones portables », *in* Nouvelles technologies et criminalité : nouvelles criminologie ?, Groupe Suisse de Criminologie, Rüegger Verlag, Zurich, p. 195 ss, 2006, ISBN 3-7253-0840-3
- CARTIER J., BERGIER S.**, « Les fraudes GSM : analyse criminelle et poursuite pénale - Collaboration entre les organisations et les instances de justice et police », *Revue internationale de criminologie et de police technique et scientifique (RICPTS)*, vol. 1, pp. 107-118, Janvier-Mars 2008
- CARTIER-BRESSON J.**, « États, marchés, réseaux et organisations criminelles entrepreneuriales », dans *Criminalité organisée et ordre dans la société*, Colloque du 5,6, 7 juin 1997, Presses Universitaires d'Aix-Marseille, 1997
- CASSANI U.**, « Combattre le crime en confisquant les profits: Nouvelles perspectives d'une justice transnationale », *in* *Criminalité économique*, Groupe Suisse de Criminologie, Rüegger Verlag, Zurich, p. 262 ss, 1999, ISBN 3-7253-0635-4
- CHARRET, A.**, « Ecoutes radioélectriques et renseignement », Collection Culture du renseignement, L'Harmattan, Paris, 2006, ISBN 2-296-00784-8
- CHISUM, J., TURVEY, B.**, « Crime Reconstruction », Academic Press, Burlington, 2007, ISBN: 978-0-12-369375-4
- CHOQUET Ch.**, « Terrorisme et criminalité organisée », L'Harmattan, 2003, ISBN 2-7475-4456-7
- CHOQUET Ch.**, « La Criminalité organisée dans la réflexion géopolitique », *in* *Cahiers de la sécurité – Les organisations criminelles*, N° 7, INHES, Paris, 2009, article disponible sur [www.cahiersdelasecurite.fr](http://www.cahiersdelasecurite.fr)
- CRISPINO F.**, « Le principe de Locard est-il scientifique ? ou analyse de la scientificité des principes fondamentaux de la criminalistique », Thèse de doctorat, Institut de Police Scientifique, Ecole des sciences Criminelles Lausanne, 2006
- CRISPINO F.**, « Nature and place of crime scene management within forensic sciences », *Science&Justice*, Volume 48, 2008, pp. 24-28
- DACG**, « Analyse criminelle et analyse comportementale – Rapport du groupe de travail interministériel » Direction des affaires Criminelles et des Grâces, Bureau des politiques pénales et de la protection des libertés individuelles, Ministère de la Justice, République Française, juin 2003
- DAOUST LCL**, « Le développement de l'analyse criminelle dans la chaîne judiciaire de la Gendarmerie. », *La Tribune du Collège Interarmées de Défense (CID)*, no 25, 2003, Ministère de la Défense, France
- DDPS**, « Les services de renseignement suisses », Secrétariat général du DDPS, 1<sup>ère</sup> édition, 2004, no 92.400 f
- DE VRIES REILINGH J.**, « La répression des infractions collectives et les problèmes liés à l'application de l'article 260terCP relatif à l'organisation criminelle, notamment du point de vue de la présomption d'innocence », *Revue des Juristes Bernois*, Vol. 138, p. 190, 2002.
- DROR I.E., PERON A., HIND S., CHARLTON D.**, « When emotions get the better of us: the effect of contextual top-down processing on matching fingerprints », *Appl. Cogn. Psychol.* 19 (6), pp. 799-809, 2005
- DROR I.E., CHARLTON D., PERON A.**, « Contextual information renders experts vulnerable to making erroneous identifications », *Forensic Science International*, Vol. 156, 2006, pp.74-78
- DUPONT B.**, « Police communautaire ou de résolution de problèmes », *in* CUSSON M., DUPONT B., LEMIEUX F., *Traité de sécurité intérieure*, Presses polytechniques et universitaires romandes, 2008, ISBN 978-2-88074-755-8

- EGGER S.A.**, « Working Definition of Serial Murder and the Reduction of Linkage Blindness », *Journal of Police Science and Administration*, Vol. 12, p.348-357, 1984
- ESSEIVA P., DUJOURDY L., TARONI F., ANGLADA F., GUENIAT O., MARGOT P.**, « Les signatures chimiques à partir des saisies de produits stupéfiants : Utilité et gestion de l'information », *Revue internationale de criminologie et de police technique et scientifique (RICPTS)*, 1 / 02, p.104-111, 2002
- ESSEIVA P.**, « Le profilage de l'héroïne et de la cocaïne – Mise en place d'une systématique permettant une utilisation opérationnelle des liens chimiques », Thèse de doctorat, Institut de Police Scientifique, Ecole des sciences Criminelles Lausanne, 2004
- EU SEMINAR**, « Forensic Intelligence – Intelligence from databases located at forensic science laboratories and its relation to criminal investigations, Gerechtelijk Laboratorium, The Hague, 1997
- FEDPOL.CH**, « Rapport sur la sécurité intérieure de la Suisse 2001 », Office fédéral de la police, DFJP, Berne, 2001
- FEDPOL.CH**, « Rapport sur la sécurité intérieure de la Suisse 2002 », Office fédéral de la police, DFJP, Berne, 2002
- FINKELSTEIN M.O., FAIRLEY W.B.**, « A Bayesian Approach to Identification Evidence », *Harvard Law Review*, Vol. 83, No. 3, pp. 489-517, 1970
- FLÜCKIGER A.**, « La preuve juridique à l'épreuve du principe de précaution », *Revue européenne des sciences sociales*, tome XLI, 2003, n° 128, pp. 107-127
- FOCAS C.**, « L'opérateur Orange perd un million et demi en 36 heures », *Quotidien 24Heures*, 06.04.2007.
- FREEMAN L.**, « Visualizing Social Networks », *Journal of Social Structure*, Carnegie Mellon University, vol. 1, no. 1, 2000
- FROST Ch.C., MORRIS J.**, « Police Intelligence Reports », Palmer Enterprises, Orangevale, California, 1983, ISBN 0-912479-03-5
- GANASCIA J.G.**, « Logique et induction : un vieux débat », in DIDAY E., BRITO P., KODRATOFF Y., MOULET M., « Induction numérique et symbolique à partir de données », Cépaduès, Paris, 2000, ISBN 2-85428-502-6
- GARDARIN G.**, « XML – Des bases de données au service du Web », Dunod, Paris, 2002, ISBN 2-10-006933-0
- GARDARIN G.**, « BASES DE DONNÉES – objet et relationnel », Eyrolles, Paris, 5<sup>e</sup> ed., 2003, ISBN 2-212-112281-5
- GIANNAKOPOULOS N.**, « Criminalité organisée et corruption en Suisse », Haupt Verlag, Berne, 2001, ISBN 3-258-06390-7
- GEORGE Ch.**, « Polymorphisme du raisonnement humain – Une approche de la flexibilité de l'activité inférentielle », Presses Universitaires de France Psychologie et sciences de la pensée, 1997, ISBN 2130480462
- GILL P.**, « Rounding Up the Usual Suspects? – Developments in contemporary law enforcement intelligence », Ashgate Publishing Ltd, Aldershot, 2000, ISBN 1-84014-923-X
- GINOUX J.-M.**, « Histoire des Sciences / Epistémologie », Université du Sud Toulon – Var, 2005
- GISLER F.**, « La coopération policière internationale de la Suisse en matière de lutte contre la criminalité organisée - *Concepts, état des lieux, évaluation et perspectives* », Thèse de doctorat, Université de Fribourg, Schulthess, 2009, ISBN 978-3-7255-5822-3
- GOTTLIEB S., ARENBERG S., SINGH R.**, « Crime Analysis - from first report to final arrest », Alpha Publishing, Montclair, California, 1998, ISBN 0-964773-0-7
- de GROOT A. D.**, « Thought and Choice in Chess », The Hague, Mouton, 1965

- GROSS H.**, « Criminal Investigation. A practical Textbook for Magistrates, Police Officers and Lawyers », fifth ed, trans. ADAM J. and COLLYER A., rev. JACKSON R.L., Sweet & Maxwell, London, 1962
- GUENIAT O.**, « Le profilage de l'héroïne et de la cocaïne – Les méthodes d'analyse, la modélisation du concept de profilage, la gestion et l'exploitation des liens », Thèse de doctorat, Institut de Police Scientifique et de Criminologie, Lausanne, 2001
- GUENIAT O., ESSEIVA P.**, « Le profilage de l'héroïne et de la cocaïne, *une méthodologie moderne de lutte contre le trafic illicite* ». Collection sciences forensiques, Presses polytechniques et universitaires romandes, 2005, ISBN 2-88074-532-2
- GUENIAT O.**, « Le sadique zoophile a surtout sévi dans les journaux ! Autopsie d'une vache. », Conférence donnée lors de AG extraordinaire de l'AAEIPS à Lausanne, le 18 novembre 2006
- HALLIWELL J., KEPPENS J., SHEN Q.**, « Linguistic Bayesian Networks for reasoning with Subjective Probabilities in Forensic Statistics », in: 9<sup>th</sup> International Conference on Artificial Intelligence and Law (ICAIL 2003), pp. 42-50, 2003
- HENRY E.R.**, « Classification and Uses of Finger Prints », Darling and Son Ltd., Londres 1913
- HERNU P.**, « Le Web et les organisations mafieuses : mythes et réalités », in Cahiers de la sécurité – La criminalité numérique, N° 6, INHES, Paris, 2008, pp. 9-18
- HEUER R.J.**, « Psychology of Intelligence Analysis », Center for the Study of Intelligence, Central Intelligence Agency, 1999
- HEUER R.J.**, « Limits of Intelligence Analysis », Orbis, Foreign Policy Research Institute, Winter 2005, pp. 75-94, 2005
- HEUER R.J.**, ACH 2.0.3 software Tutorial, 2006
- HOPKINSON A.**, « Intelligence Models and Best Practices », International Association of Law Enforcement Intelligence Analysts, IALEIA Booklet, 1999
- HOSTETTLER P. et al.**, « Brochure d'analyse opérationnelle », Groupe de travail suisse en analyse criminelle opérationnelle, Office Fédéral de la Police, Berne, 2000
- I2 Ltd**, « i2 Products », Site Internet, [www.i2group.com](http://www.i2group.com), juin 2002
- IACAP**, « Criminal Intelligence Sharing : A National Plan for Intelligence-Led Policing At the Local, State and Federal Levels », International Association of Chiefs of Police Research Division, August 2002
- INTERPOL**, « Guide sur l'analyse criminelle », GTAC, 2<sup>e</sup> édition, Organisation Internationale de Police Criminelle (Interpol), 1997
- KERCHOVE (VAN DE) M.**, « La vérité judiciaire: quelle vérité, rien que la vérité, toute la vérité? », Déviance et société, 2000, n° 1, p. 95ss
- KIND S.S.**, « The Scientific Investigation of Crime », Forensic Science Services Ltd, Harrogate, 1987
- KIND S.S.**, « Crime Investigation and the Criminal Trial: A Three Chapter Paradigm of Evidence », Journal of the Forensic Science Society, Vol. 34, 1994, pp.155-164
- KLERKS, P.**, «The network paradigm applied to criminal organisations», Connections, 24, 3 :53-65, 2001.
- KREBS, V.E.**, «Mapping Networks of Terrorist Cells», Connections, 24, 3 :43-52, 2002

- KREIS G., DELLEY J.-D., KAUFMANN O.**, « La protection de l'Etat en Suisse : l'évolution de 1935-1990 ; étude pluridisciplinaire effectuée et éditée sur mandat du Conseil fédéral », Editions Paul Haupt, Berne, 1993, ISBN 3-258-04831-2
- KUNZMANN P., FRANZ-PETER BURKARD F.-P., WIEDMANN F.**, « Atlas de la philosophie », Livre de Poche, Paris, 1993, ISBN 2-253065-11-0
- LEE R.**, « Automatic information extraction from documents: a tool for intelligence and law enforcement analysts », Proceedings of 1998 AAAI Fall Symposium on Artificial Intelligence and Link Analysis, AAAI Press, Menlo Park, CA, 1998.
- LEMIEUX V.**, « Les réseaux criminels », rapport de la Gendarmerie royale du Canada, Sous-direction Recherche et Evolution, 2003, ISBN 0-662-67645-9
- LEMIEUX F.**, « Normes et pratiques en matière de renseignement criminel – une comparaison internationale », Les Presses de l'Université de Laval, 2006, ISBN 2-7637-8346-5
- LE ROBERT**, « Le Robert pour tous », 1994, Paris
- LEIU**, « Criminal Intelligence File Guidelines, An International Intelligence Network », Law Enforcement Intelligence Unit, Revised March 2002
- LINSAY P.H., NORMANN D.A.**, « Human Information Processing », New York Academic Press, 1977
- LOCARD E.**, « L'enquête criminelle et les méthodes scientifiques », Flammarion, Paris 1933
- LÜTHI R.**, « Enquête administrative au sein du Ministère public de la Confédération », 15 septembre 2006
- MARGOT P.**, « Cours de sciences forensiques », Institut de Police Scientifique et de Criminologie, Lausanne, 1995
- MAROTTA G.**, « Réflexions criminologiques sur le thème de la criminalité organisée », *in* Cahiers de la sécurité – Les organisations criminelles, N° 7, INHES, Paris 2009, pp 237-239
- McLAUGHLIN J.**, « A Bayesian Updating Model for Intelligence Analysis: A Case Study of Iraq's Nuclear Weapons Program », PhD Thesis, Stanford University, 2005
- McGRATH C., KRACKHARDT D. and BLYTHE J.**, « Visualizing Complexity in Networks: Seeing Both the Forest and the Trees. », *Connections*, 25(1): 37-47, 2003
- McGRATH C. and BLYTHE J.**, « Do You See What I Want You to See? The Effects of Motion and Spatial Layout on Viewers' Perceptions of Graphical Structures », *Journal of Social Structure*, Volume 5, Number 2, 2004
- MENA Jesús**, « Investigative Data Mining for security and Criminal Detection », Butterworth Heinemann, Boston, 2003, ISBN 0-7506-7613-2
- MILLER G. A.**, « The Magical Number Seven – Plus or Minus Two: Some Limits on our Capacity for Processing Information. », *The Psychological Review*, Vol. 63, No. 2, 1956
- MORSELLI C., TURCOTTE M., LOUIS G.**, « Le crime organisé et les contre-mesures », *in* CUSSON M., DUPONT B., LEMIEUX F., *Traité de sécurité intérieure*, Presses polytechniques et universitaires romandes, 2008, ISBN 978-2-88074-755-8
- MORRIS J.**, « Crime Analysis Charting », The Palmer Press, Loomis, California, 7<sup>e</sup> edition, 1993, ISBN 0-912479-01-9
- MUTTON P.**, « Inferring and Visualizing Social Networks on Internet Relay Chat », Eighth International Conference on Information Visualisation (IV'04), London, England, IEEE, 14 au 16 juillet 2004

- NASIRE**, « National Information Architecture – Toward National Sharing of Governmental Information – Executive Summary », NASIRE, Lexington, Kentucky, [www.nasire.org](http://www.nasire.org), 2002
- NCIS**, « Interpol & Technology in Partnership, fighting drug trafficking », National Criminal Intelligence Service (NCIS), Kensington Publications Ltd, 1999
- OFF**, « Rapport de situation 2000 », SAP, Office fédéral de la police, 2001
- OFF**, « Rapport sur la sécurité intérieure de la Suisse », Fedpol, Office fédéral de la police, 2002
- OLERON P.**, « Le raisonnement », Collection : Que sais-je?, Presses Universitaires de France (PUF); 4e éd., Paris, 1996, ISBN 2-130470-31-9
- PETERSON M.B. and al.**, « Intelligence 2000 : Revising the Basic Elements », Law Enforcement Intelligence Unit (L.E.I.U.), International Association of Law Enforcement Intelligence Analysts (IALEIA), 2000, ISBN 0-9706887-0-9
- PETERSON M.B. and al.**, « Successful Law Enforcement Using Analytic Methods », International Association of Law Enforcement Intelligence Analysts, IALEIA Booklet, Third Edition, 1998
- PETERSON M.B.**, « Applications in criminal analysis – a Sourcebook », Praeger Publishers, Westport, 1994, ISBN 0-275-96468-X
- PETERSON M.B., FAHLMAN R. C., ROBERTSON S., JACQUES L.**, « Guidelines for Starting an Analytic Unit », International Association of Law Enforcement Intelligence Analysts, IALEIA Booklet, 1997
- PETERSON M.B., SMITH A., FAHLMANN R.C.**, « Intelligence-Led Policing, International Perspectives on Policing in the 21<sup>st</sup> Century », International Association of Law Enforcement Intelligence Analysts, IALEIA Booklet, 1997
- PIERCE C.S.**, « Le raisonnement et la logique des choses », Editions du Cerf, 1995, ISBN 2204051349
- POLITZER G.**, « Le raisonnement humain », Collection Traité des Sciences Cognitives. Paris : Hermès, 2002, ISBN 2-7462-0501-7
- POPPER K.R.**, « La logique de la découverte scientifique », Bibliothèque scientifique Payot, 1973, ISBN 2-228-88010-8.
- POPPER K.R.**, « Conjectures et réfutations - La croissance du savoir scientifique », Payot, 1985, ISBN 2-228-13870-3.
- PRÉVOST L.**, « Enquête criminelle », 2e édition, Mont-Royal, Modulo, 2000, ISBN 2-89113-837-6
- RAUFER X., QUÉRÉ S.**, « Le crime organisé », Que sais-je ?, Presses universitaires de France, 4ème éd., Paris, 2005
- REMY M.**, « Droit des mesures policières. Principes généraux, cadre juridique et coopération policière », Schulthess, Genève/Zurich/Bâle, 2008, ISBN: 978-3-7255-5552-9
- RIBAUX O.**, « La recherche et la gestion des liens dans l'investigation criminelle : le cas particulier du cambriolage », Thèse de doctorat, Institut de Police Scientifique et de Criminologie, Lausanne, 1997
- RIBAUX O., MARGOT P.**, « Inference Structures for Crime Analysis and Intelligence : the example of burglary using Forensic Science Data », Forensic Science International, Vol. 100, 1999, pp.193-210
- RIBAUX O., GITZ Ph., CARTIER J.**, « L'analyse criminelle face à la complexité des données », in BOLL, P.H. & STEFFEN, H., « La criminalité financière », Actes du 60<sup>e</sup> Cours international de criminologie, Collection Neuchâteloise, Helbing & Lichtenhahn, Bâle, 2002



- RIBAUX O.**, « Comprendre l'influence des NTIC sur l'évolution de la criminalité et des moyens de lutte : un champ d'étude pour les sciences criminelles », *La Criminalité économique : ses manifestations, sa prévention et sa répression*, Les Actes de l'ILCE, L'Harmattan, pp. 263-274, juillet 2005
- RIBAUX O., TOURNIE C.**, « Le renseignement et l'analyse criminels – Application à la lutte contre le crime économique et financier », à paraître dans *les meilleures pratiques en analyse financière criminelle*, 2007
- RIBAUX O., MARGOT P.**, « La trace matérielle, vecteur d'information au service du renseignement », in CUSSON M., DUPONT B., LEMIEUX F., *Traité de sécurité intérieure*, Presses polytechniques et universitaires romandes, 2008, ISBN 978-2-88074-755-8
- RODRIGEZ J. A.**, « The March 11<sup>th</sup> Terrorist Network: In its weakness lies its strength », presented at the VIII Congreso Español de Sociología. Alicante, 23-25 of September 2004
- SAKS M.J., RISINGER D.M., ROSENTHAL R., THOMPSON W.C.**, « Context effects in forensic science : A review and application of the science of science to crime laboratory practice in the United States », *Science and Justice*, Vol. 43, N°2, pp. 77-90, 2003
- SCHIFFER B., BIRRER S., CARTIER J., CAPT S., RIBAUX O.**, « Analyse de la forme, du contenu et de la provenance des courriers électroniques de la «Nigerian Connection» », *Revue internationale de criminologie et de police technique et scientifique (RICPTS)*, 2 / 04, p.148-158, 2004
- SCHMIDHUBER J.**, « A Fixed Size Storage  $O(n^3)$  Time Complexity Learning Algorithm for Fully Recurrent Continually Running Networks », *Neural Computation*, Vol. 4, No. 2, p.243-248, 1992
- SPARROW, M. K.**, « The application of network analysis to criminal intelligence. An assessment of the prospects », *Social Networks*, 13 : 251-274, 1991
- TARONI F.**, « La recherche et la gestion des liens dans l'investigation des cambriolages : une étape vers l'exploitation systématique des données de police », Thèse de doctorat, Institut de Police Scientifique et de Criminologie, Lausanne, 1997
- TARONI F., BIEDERMANN A., GARBOLINO P., AITKEN C.G.G.**, « A general approach to Bayesian networks for the interpretation of evidence », *Forensic Science International*, N°139, p.5-16, 2004
- TARONI F., AITKEN C. G. G., GARBOLINO P., BIEDERMANN A.**, « Bayesian Networks and Probabilistic Inference in Forensic Science », John Wiley & Sons, Chichester, UK, 2006, ISBN-10: 0-470-09173-8
- TUFTE E.R.**, « The visual Display of Quantitative Information », Second Edition, Graphic Press, Cheshire, Connecticut, 2001, ISBN 0-9613921-4-2
- USTER H.P.**, « La poursuite pénale au niveau fédéral – analyse de situation et recommandations », Comité de projet « Analyse de situation ProjEff », 31 août 2006
- VAN CAMP R.**, « La lutte contre la criminalité organisée au niveau européen : nouvelles technologies », *Agon* 2001, n°30, 2001, pp. 5-11
- VICK J. and al.**, « Methods of Case Analysis, An International Symposium », *Kriminalistisches Institut, Bundeskriminalamt, Wiesbaden*, vol. 38.2, 1998
- WHEATLEY J.**, « Contre le crime organisé aux Etats-Unis : le RICO », in *Cahiers de la sécurité – Les organisations criminelles*, N° 7, INHES, Paris, 2009, pp.152-162
- XU J. J. and CHEN H.**, « Fighting organized crimes: using shortest-path algorithms to identify associations in criminal networks », *Decision Support Systems*, Volume 38, Issue 3, December 2004, pp. 473-487

**ZINCANI V.**, « Les stratégies d'opposition à la criminalité organisée », *in* Cahiers de la sécurité – Les organisations criminelles, N° 7, INHES, Paris 2009, pp.79-84

**ZLOTNICK J.**, « Bayes' Theorem for Intelligence Analysis », *Studies in Intelligence*, Vol. 16, No. 2, 1972.

## **6.2 Textes légaux**

**FF 1992 VI 150** – Directives de la mise en application de la protection de l'Etat du 9 septembre 1992

**FF 1993 III 269** – Message du 30 juin 1993 concernant la modification du code pénal suisse et du code pénal militaire

**FF 2004 1377** – Système d'interception des communications par satellites du Département fédéral de la défense, de la protection de la population et des sports (projet «Onyx»)

**FF 2006 1057** – Message relatif à l'unification du droit de la procédure pénale

**FF 2008 4767** - Loi fédérale sur les systèmes d'information de police de la Confédération (LSIP)

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

**RS 235.1** – Loi fédérale sur la protection des données (LPD)

**RS 235.11** – Ordonnance relative à la loi fédérale sur la protection des données (OLPD)

**RS 311** – Code pénal suisse (CP)

**RS 312** – Loi fédérale sur la procédure pénale (PPF)

**RS 360** – Loi fédérale sur les Offices centraux de police criminelle de la Confédération (LOC)

**RS 360.1** – Ordonnance concernant l'exécution de tâches de police judiciaire au sein de l'Office fédéral de la police (OCPC)

**RS 360.2** – Ordonnance sur le système informatisé de la Police judiciaire fédérale (Ordonnance JANUS)

**RS 361** – Loi fédérale du 13 juin 2008 sur les systèmes d'information de police de la Confédération (LSIP)

**RS 510.10** – Loi fédérale sur l'armée et l'administration militaire (LAAM)

**RS 780.1** – Loi fédérale du 6 octobre 2000 sur la surveillance de la correspondance par poste et télécommunication (LSCPT)

**RS 780.11** – Ordonnance du 31 octobre 2001 sur la surveillance de la correspondance par poste et télécommunication (OSCPT)

**RS 780.115.1** – Ordonnance du DETEC sur les émoluments et les indemnités en matière de surveillance de la correspondance postale et des télécommunications.

**RS 812.121** – Loi fédérale sur les stupéfiants et les substances psychotropes (LSTUP)

**RS 955** – Loi fédérale concernant la lutte contre le blanchiment d'argent dans le secteur financier (LBA)

**Index des figures :**

fig. 1 :	Rapports qui se nouent entre les quatre fonctions de l'action de sécurité.....	1
fig. 2 :	Continuum criminalité organisée.....	16
fig. 3 :	Continuum des organisations criminelles.....	17
fig. 4 :	Criminalité organisée, crime organisé et organisations criminelles.....	17
fig. 5 :	Modèle universel des trois dimensions d'une enquête.....	37
fig. 6 :	Représentation du déroulement chronologique d'une enquête classique.....	39
fig. 7 :	Représentation du déroulement chronologique d'une enquête d'initiative.....	41
fig. 8 :	Schématisation des trois chapitres de l'enquête selon KIND.....	42
fig. 9 :	Meubles à fiches.....	64
fig. 10 :	Exemple de fiche dactyloscopique avec sa classification.....	65
fig. 11 :	Structure hiérarchique d'une base de données.....	66
fig. 12 :	Structure réseau d'une base de données.....	67
fig. 13 :	Structure relationnelle d'une base de données.....	67
fig. 14 :	Exemple de tables relationnelles.....	70
fig. 15 :	Exemple de tables de relation de cardinalité un à plusieurs.....	70
fig. 16 :	Exemple de tables de relations de cardinalité de plusieurs à plusieurs.....	71
fig. 17 :	Exemple d'un objet d'une base de données orientée objet.....	71
fig. 18 :	Les extensions apportées au relationnel.....	72
fig. 19 :	Cadres des contraintes de l'analyse criminelle.....	87
fig. 20 :	Formes de l'analyse criminelle.....	88
fig. 21 :	Cycle du renseignement.....	90
fig. 22 :	Division traditionnelle des raisonnements.....	91
fig. 23 :	Schématisation des trois raisonnements fondamentaux.....	96
fig. 24 :	Données – Informations - Renseignement.....	97
fig. 25 :	Développement d'hypothèses différentes, voire contradictoires.....	98
fig. 26 :	Division traditionnelle des raisonnements.....	99
fig. 27 :	Processus en jeu dans l'abduction.....	99
fig. 28 :	Squelette d'une matrice relationnelle.....	104
fig. 29 :	Placement des entités dans la matrice relationnelle.....	104
fig. 30 :	Codes de relations des matrices relationnelles.....	105
fig. 31 :	Matrice relationnelle complétée.....	105
fig. 32 :	Comptage des relations dans la matrice relationnelle.....	105
fig. 33 :	Standard de traduction de la matrice relationnelle au schéma relationnel.....	106
fig. 34 :	Exemple de schéma relationnel brut.....	106
fig. 35 :	Exemple de schéma relationnel clarifié.....	106
fig. 36 :	Exemple de schéma relationnel actuel.....	107
fig. 37 :	Exemple de schéma relationnel moderne simplifié.....	107
fig. 38 :	Exemple de schéma relationnel mixte ancien.....	108
fig. 39 :	Exemple de schéma relationnel mixte moderne.....	108
fig. 40 :	Exemple d'une matrice jour/heure d'un contrôle technique.....	110
fig. 41 :	Exemple de représentation des connexions / heures.....	110
fig. 42 :	Exemple de représentation des connexions / jours.....	111
fig. 43 :	Exemple de représentation des connexions / heures selon le jour.....	111
fig. 44 :	Exemple de représentations géographiques rendues possibles par le CTAnalyser 3.0.....	112
fig. 45 :	Exemple de représentation géographique précise.....	112

fig. 46 :	Représentation graphique de contrôles techniques selon d'anciens standards.....	113
fig. 47 :	Représentation graphique de contrôles techniques à l'aide des outils actuels .....	114
fig. 48 :	Exemple de représentation relationnelle d'un contrôle technique .....	115
fig. 49 :	Exemple d'utilisation de plusieurs GSM et de plusieurs cartes SIM.....	124
fig. 50 :	Demande d'un premier contrôle technique.....	124
fig. 51 :	Demande de deux nouveaux contrôles complémentaires .....	124
fig. 52 :	Exemple réel d'échange de cartes SIM dans les téléphones GSM .....	125
fig. 53 :	Squelette d'une étiquette d'un diagramme chronologique.....	126
fig. 54 :	Exemple de l'emplacement des informations dans le squelette des étiquettes .....	127
fig. 55 :	Standard des axes représentation des schémas chronologiques .....	127
fig. 56 :	Standards des symboles de représentation dans les schémas chronologiques .....	128
fig. 57 :	Exemple de représentation chronologique standard .....	128
fig. 58 :	Exemple de schéma chronologique standard clarifié.....	128
fig. 59 :	Exemple de schéma chronologique avec les logiciels modernes.....	129
fig. 60 :	Exemple de schéma chronologique avec les logiciels actuels .....	129
fig. 61 :	Exemple de schéma de flux chronologique standard.....	130
fig. 62 :	Exemple de schéma de flux chronologique de connexions téléphoniques .....	130
fig. 63 :	Exemple de schéma chronologique mixte standard.....	130
fig. 64 :	Exemple de schéma chronologique mixte actuel.....	131
fig. 65 :	Concept du projet de thèse.....	150
fig. 66 :	Suite logicielle de i2 – mars 2008 - source www.i2inc.com.....	153
fig. 67 :	Possibilités de liens définis par « sous-champs » dans le système JANUS PV .....	159
fig. 68 :	Exemple de représentation fautive où tout est lié à tout .....	160
fig. 69 :	Exemple de représentation correcte où les liens sont différenciés.....	161
fig. 70 :	Possibilités de liens définis par dans le système JANUS+ JO (version évaluation) .....	162
fig. 71 :	Structure hiérarchique des personnes et des antécédents de JANUS PV.....	164
fig. 72 :	JANUS PV : Détail des rubriques principales de l'identité et des « sous-champs » .....	165
fig. 73 :	JANUS PV : Détail des champs de l'IDENTITE .....	166
fig. 74 :	JANUS PV : Détail REL> et REL>adr .....	167
fig. 75 :	JANUS PV : Détail SOC> .....	169
fig. 76 :	JANUS PV : Détail ADR> et HOT>.....	169
fig. 77 :	JANUS PV : Détail AUT> et DET>.....	171
fig. 78 :	JANUS PV : Détail CPT> .....	172
fig. 79 :	JANUS PV : Détail TEL> et ABO>.....	173
fig. 80 :	JANUS PV : Détail URL>.....	174
fig. 81 :	JANUS PV : Détail OBJ> .....	175
fig. 82 :	JANUS PV : Détail PAS> .....	175
fig. 83 :	JANUS PV : Détail VER>.....	176
fig. 84 :	JANUS PV : Exemple de l'organisation des données IDENTITE – « sous-champs ».....	179
fig. 85 :	JANUS PV : Correction de l'organisation des données IDENTITE – « sous-champs ».....	180
fig. 86 :	JANUS PV : Mention des contrôles techniques dans des « sous-champs » .....	181
fig. 87 :	JANUS PV : Connexion automatique des « sous-champs ».....	182
fig. 88 :	JANUS PV : Perte du potentiel de liaison des « sous-champs » avec des liens indirects de niv. 2 .....	183
fig. 89 :	JANUS PV : Schéma définitif sur la base du schéma provisoire issu de la base de données.....	184
fig. 90 :	Exemple de la visualisation manuelle d'une « liste de travail » .....	185
fig. 91 :	Exemple de la visualisation manuelle d'une « liste de travail spéciale » .....	186
fig. 92 :	Exemple d'iconographie actuelle.....	202

fig. 93 :	Exemple de chromatographie actuelle.....	206
fig. 94 :	Degré de détail – décomposition de l’information.....	208
fig. 95 :	Degré de détail – décomposition de niveau 2.....	208
fig. 96 :	Matrice relationnelle théorique du modèle générique.....	210
fig. 97 :	Matrice relationnelle pratique du modèle générique.....	211
fig. 98 :	Recherche d’une personne.....	212
fig. 99 :	Analyse du profil téléphonique d’un suspect.....	213
fig. 100 :	Décomposition incomplète des liens indirects.....	213
fig. 101 :	Représentation correcte des relations indirectes.....	214
fig. 102 :	Niveau de détail - Zoom minimum.....	215
fig. 103 :	Niveau de détail - Zoom moyen.....	215
fig. 104 :	Niveau de détail - Zoom maximum.....	216
fig. 105 :	Masque de recherche de base de JANUS PV 2.0.....	220
fig. 106 :	Masque PERSONNE-ANTÉCÉDENT(S) de JANUS PV 2.0.....	222
fig. 107 :	Séparation des niveaux (« sous-champs » et « attributs »).....	223
fig. 108 :	Objets (« sous-champs » et « attributs ») de JANUS PV 2.0.....	225
fig. 109 :	PV2 – « Sous-champ » ADR.....	225
fig. 110 :	PV2 – « Attribut » Adresse.....	226
fig. 111 :	PV2 – « Sous-champ » AUT.....	226
fig. 112 :	PV2 – « Attribut » Véhicule.....	226
fig. 113 :	PV2 – « Sous-champ » VER.....	227
fig. 114 :	PV2 – « Sous-champ » BST.....	227
fig. 115 :	PV2 – « Attribut » Compte.....	227
fig. 116 :	PV2 – « Sous-champ » CPT.....	228
fig. 117 :	PV2 – « Sous-champ » FTA.....	228
fig. 118 :	PV2 – « Sous-champ » HOT.....	229
fig. 119 :	PV2 – « Sous-champ » KOM.....	229
fig. 120 :	PV2 – « Attribut » Communication.....	229
fig. 121 :	PV2 – « Sous-champ » OBJ.....	230
fig. 122 :	PV2 – « Sous-champ » ORG.....	230
fig. 123 :	PV2 – « Sous-champ » PAS.....	230
fig. 124 :	PV2 – « Sous-champ » PRO.....	231
fig. 125 :	PV2 – « Attribut » Relations.....	231
fig. 126 :	PV2 – « Sous-champ » REL.....	232
fig. 127 :	PV2 – « Sous-champ » RTG.....	232
fig. 128 :	PV2 – « Sous-champ » SOC.....	232
fig. 129 :	PV2 – Exemple de fichier d’échange XML.....	234
fig. 130 :	Entités du prototype $\beta$ .....	236
fig. 131 :	Détail de l’entité Antécédent du prototype $\beta$ .....	237
fig. 132 :	Détail de l’entité Argent (biens) du prototype $\beta$ .....	237
fig. 133 :	Détail de l’entité Choses (biens) du prototype $\beta$ .....	238
fig. 134 :	Détail de l’entité Communication du prototype $\beta$ .....	238
fig. 135 :	Détail de l’entité Evénement du prototype $\beta$ .....	239
fig. 136 :	Détail de l’entité Forensique du prototype $\beta$ .....	239
fig. 137 :	Détail de l’entité Lieu du prototype $\beta$ .....	240
fig. 138 :	Détail de l’entité Personne / Société du prototype $\beta$ .....	240

fig. 139 :	Détail de l'entité Transport du prototype $\beta$ .....	241
fig. 140 :	Icônes de l'entité Communication (exemple).....	242
fig. 141 :	Liens du prototype $\beta$ .....	243
fig. 142 :	Détail des liens du prototype $\beta$ (part. 1) .....	244
fig. 143 :	Détail des liens du prototype $\beta$ (part. 2) .....	245
fig. 144 :	Contrôle du type d'entité dans les liens dans iBase™.....	246
fig. 145 :	Recherches visuelles dans iBase™ (Query).....	246
fig. 146 :	Listes de choix du prototype $\beta$ .....	248
fig. 147 :	Listes d'icônes du prototype $\beta$ .....	248
fig. 148 :	Visualisateur interne de iBase™ (iBase Link Chart).....	250
fig. 149 :	Visualisateur interne de iBase™ (filtre sur les liens) .....	250
fig. 150 :	Fonction « explore » dans l'Analyst's Notebook™ .....	251
fig. 151 :	Fonction « expand » dans l'Analyst's Notebook™ .....	252
fig. 152 :	Fonction « Charting settings » dans l'Analyst's Notebook™ .....	252
fig. 153 :	Exemple de représentation relationnelle de données réelles contenues dans le prototype $\beta$ .....	253
fig. 154 :	Représentation chronologique de connexions (liens) contenues dans le prototype $\beta$ .....	254
fig. 155 :	Représentation chronologique d'événements (entités) contenus dans le prototype $\beta$ .....	255
fig. 156 :	Exemple de représentation chronologique de données réelles contenues dans le prototype $\beta$ .....	256
fig. 157 :	Critères de la recherche pondérée d'iBase™.....	257
fig. 158 :	Résultats de la recherche pondérée d'iBase™.....	257
fig. 159 :	Combinaison de sélections dans iBase™ .....	258
fig. 160 :	Analyse de sélections dans iBase™ .....	259
fig. 161 :	Utilisation de l'Analyst's Notebook™ pour la recherche d'éléments communs.....	259
fig. 162 :	Explorateur dans iBase™ .....	260
fig. 163 :	Recherche « texte » dans iBase™ .....	260
fig. 164 :	Masque de saisie Personne / Société du prototype $\beta$ .....	261
fig. 165 :	Transformation et formatage de document XML .....	264
fig. 166 :	Schéma de conversion entre JANUS et le prototype $\beta$ .....	265
fig. 167 :	Principe de représentation des liens de différents niveaux dans JANUS PV 2.0.....	266
fig. 168 :	Modèle de représentation des liens de différents niveaux dans JANUS PV 2.0.....	272
fig. 169 :	Vue de l'assistant d'importation de iBase™ 4, en-tête XML présent et compatible.....	274
fig. 170 :	Schéma du flux d'information au sein d'un EM de conduite incluant un composant d'analyse .....	280
fig. 171 :	Evolution du nombre d'utilisateurs depuis la migration à JANUS PV 2.0.....	292
fig. 172 :	Nombre total d'enregistrements dans JANUS PV en 2006 .....	292
fig. 173 :	Répartition des saisies JANUS PV jusqu'au 31.08.2005.....	293
fig. 174 :	Représentation du nombre des personnes saisies par canton jusqu'au 31.08.2005 .....	294
fig. 175 :	Représentation du nombre des personnes saisies par canton entre le 31.08.2005 et le 30.06.2006.....	294
fig. 176 :	Répartition des saisies JANUS PV entre le 31.08.2005 et le 30.06.2006.....	295
fig. 177 :	Représentation du nombre total des saisies JANUS PV par rapport à la population.....	296
fig. 178 :	Rapport entre les identités et les antécédents dans JANUS PV .....	297
fig. 179 :	Représentation de l'évolution du ratio entre les identités et les antécédents dans JANUS PV.....	298
fig. 180 :	Cycle du renseignement : deux phases nécessaires dans l'étape d'analyse .....	311
fig. 181 :	Effet d'ancrage .....	316
fig. 182 :	Procédure d'analyse d'hypothèses concurrentes .....	319
fig. 183 :	Exemple de matrice d'analyse d'hypothèses concurrentes.....	320

fig. 184 :	Matrice d'analyse bayésienne d'hypothèses concurrentes.....	325
fig. 185 :	Exemple de l'utilisation d'une matrice bayésienne d'analyse d'hypothèses concurrentes.....	327
fig. 186 :	Exemple d'éléments peu probants.....	328
fig. 187 :	Exemple de schéma fait sans paraphrase.....	333
fig. 188 :	Exemple de paraphrase graphique d'un texte.....	334
fig. 189 :	Table des valeurs d'un élément (logiciel ACH 2.0.3).....	335
fig. 190 :	Matrice des scores de contradiction des éléments (logiciel ACH 2.0.3).....	336
fig. 191 :	Exemple d'une matrice d'analyse d'hypothèses concurrente (logiciel ACH 2.0.3).....	337
fig. 192 :	Exemple d'un graphique des scores de contradiction (logiciel ACH 2.0.3).....	337
fig. 193 :	Exemple de coloration d'une matrice bayésienne d'analyse d'hypothèses concurrentes.....	338
fig. 194 :	Exemple d'un graphique d'une matrice bayésienne d'analyse d'hypothèses concurrentes.....	338

## Glossaire :

**Antécédent** : Le sous-système JANUS PV (personne et antécédents) est constitué de fiches personnes et de leurs *antécédents*. Chaque fiche personne pouvant contenir plusieurs antécédents.

**Attribut** : Dans JANUS, un *attribut* est une entité directement liée à la personne faisant l'objet d'un antécédent, par exemple, son numéro de téléphone ou celui qu'elle utilise, son adresse ou son lieu de séjour, son véhicule ou celui qu'elle conduit.

**Entité** : Basée sur la règle informatique du modèle objet<sup>420</sup>. Ainsi, dans notre modèle méthodologique réaliste à la base de notre base de données d'analyse, une *entité* représente un élément du monde réel individualisable.

**Identifiant** : L'*identifiant* est l'élément permettant d'individualiser une entité.

**Identité** : Le sous-système JANUS PV (personne et antécédents) est constitué de fiches personnes, appelées *identités*, et de leurs antécédents. Chaque *identité* pouvant contenir plusieurs antécédents.

**Lien direct** : Les *liens directs* entre personnes sont réservés aux liens familiaux ou relations avérées et non-contestables.

**Lien indirect** : Une entité peut se trouver liée à deux personnes. Elle constitue alors un *lien indirect*. Les attributs et les sous-champs de JANUS constituent des liens indirects.

**Niveau de lien** : On peut définir plusieurs *niveaux de liens* entre des personnes. En sus des liens directs, réservés aux liens familiaux ou relations avérées et non-contestables, une entité peut se trouver liée à deux personnes. Elle constitue alors un lien indirect de niveau 1. Les attributs de JANUS peuvent constituer de tels liens, par exemple, un même raccordement téléphonique ou un même véhicule partagé, une même adresse, ou une même relation. Si une seconde entité ou une troisième entité se trouve intercalée entre les personnes, ils constituent des liens indirects de niveau supérieur : 2 ou 3. Les sous-champs de JANUS sont généralement des liens de niveau supérieur à 1.

**Objet** : Dans JANUS, un *objet* est un élément factuel si possible individualisable en lien direct avec une personne en identité (attribut) ou mentionné dans un antécédent (sous-champ).

**Sous-champ** : Un sous-champ est, dans JANUS, un objet mentionné dans un antécédent. Il permet de faire des liens indirects entre les personnes en identité, par exemple, un ami commun, une même régie immobilière, le même numéro de téléphone de la centrale des taxis.

**Sous-système** : JANUS est constitué de deux *sous-systèmes* : le sous-système PV (personne et antécédents), qui contient les identités des personnes faisant l'objet de mesures d'enquête, et le *sous-système* JO (journaux), qui contient les transcriptions des surveillances téléphoniques, journaux d'enquête ou encore mains courantes.

---

<sup>420</sup> Toute entité du monde réel est un objet, et réciproquement, tout objet représente une identité du monde réel



## 7 Annexes

Annexe I – Figures de grande taille

Annexe II – Liste des icônes du *prototype*  $\beta$

Annexe III – Rapport du design du *prototype*  $\beta$

Annexe IV – Illustration de l'utilisation d'une matrice bayésienne d'analyse d'hypothèses concurrentes



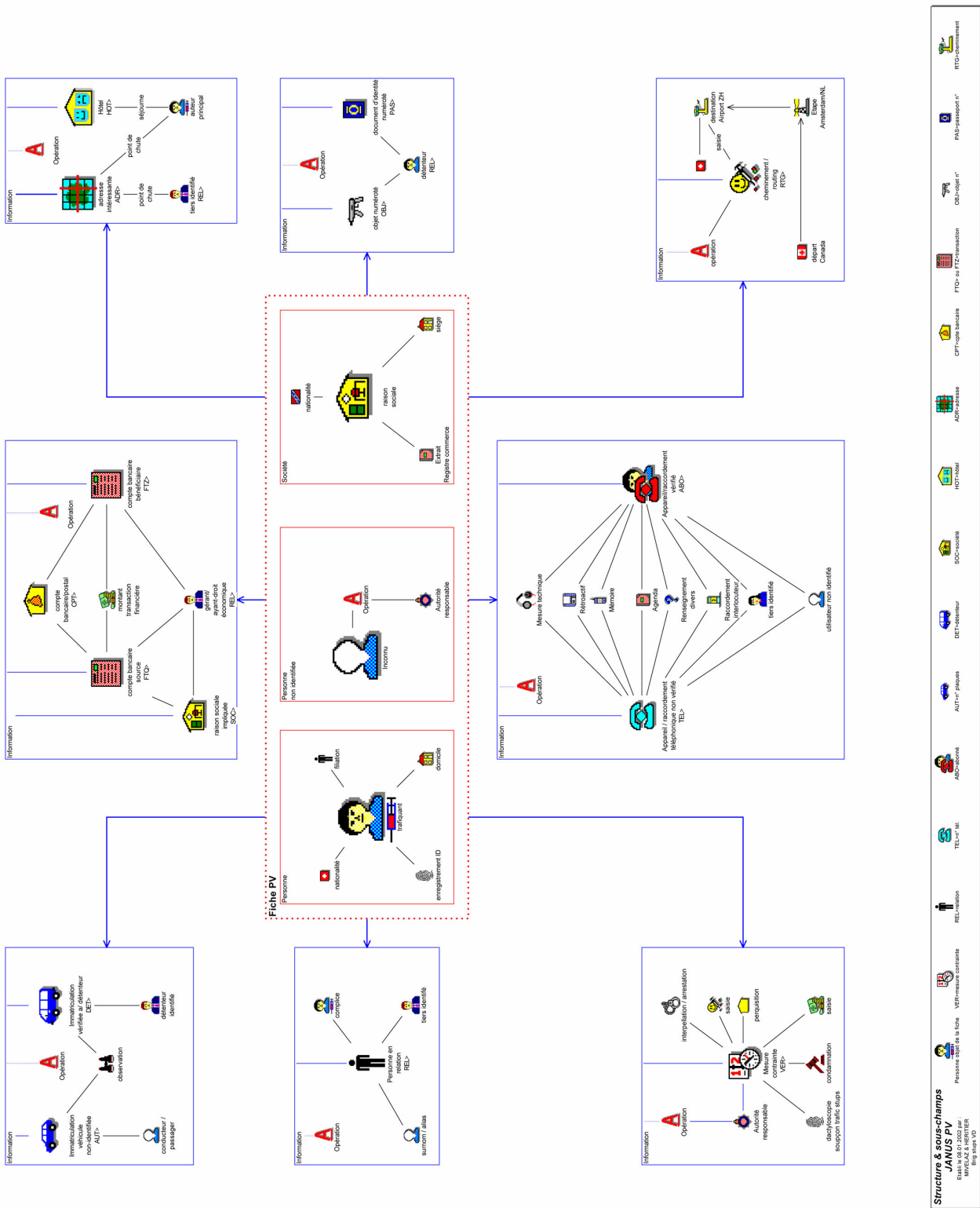


fig 67 : Possibilités de liens définis par « sous-champs » dans le système JANUS PV

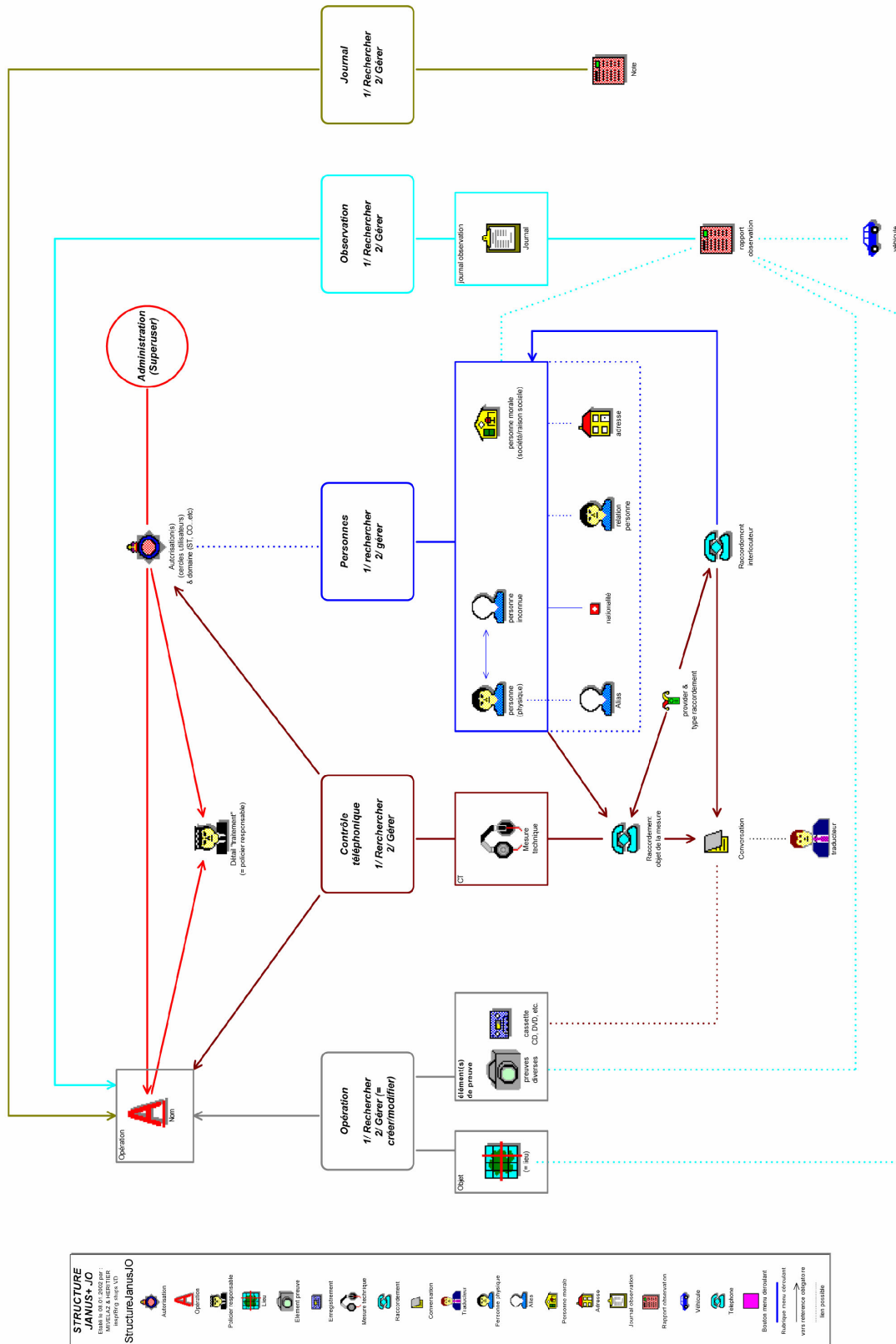


fig 70 : Possibilités de liens définis par dans le système JANUS+ JO (version évaluation)

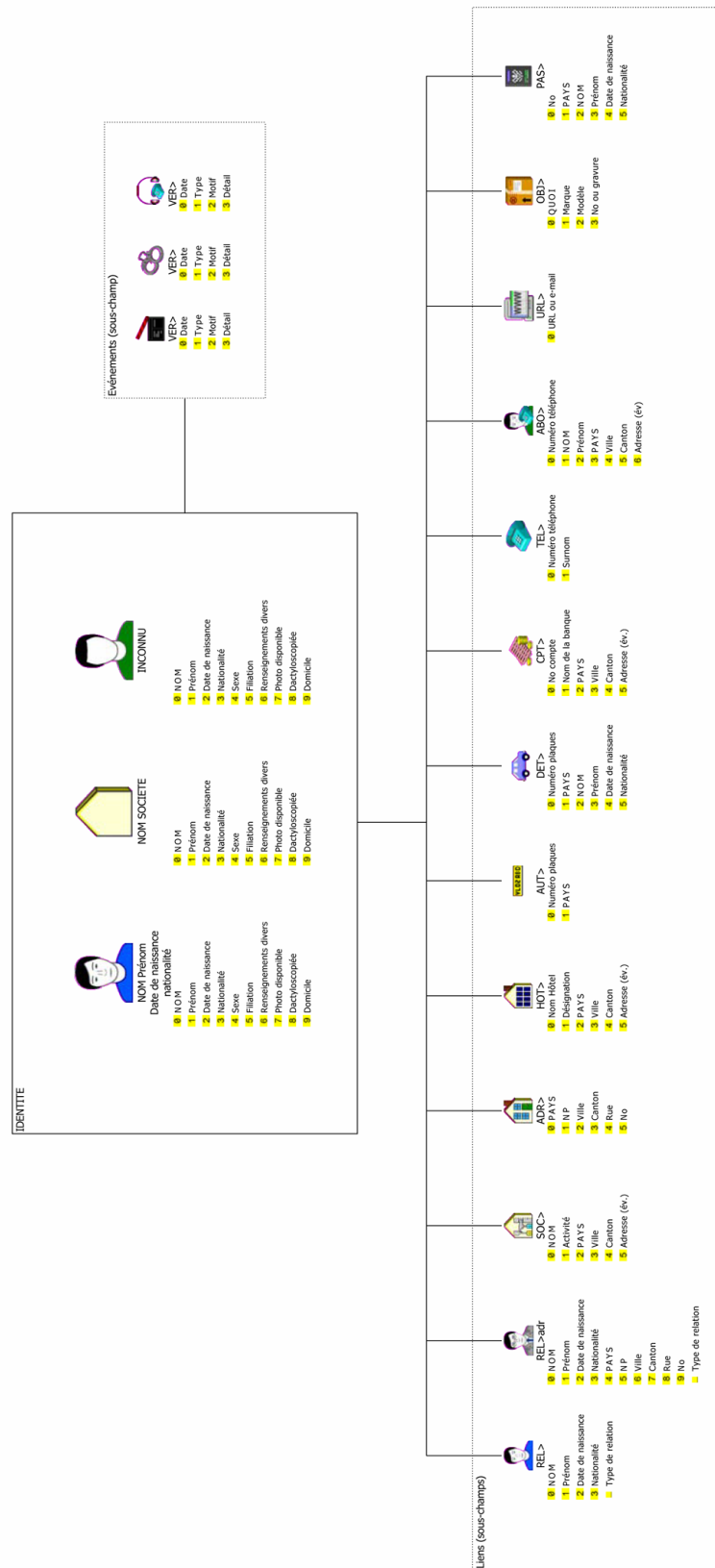


fig. 72 : JANUS PV : Détail des rubriques principales de l'identité et des « sous-champs »

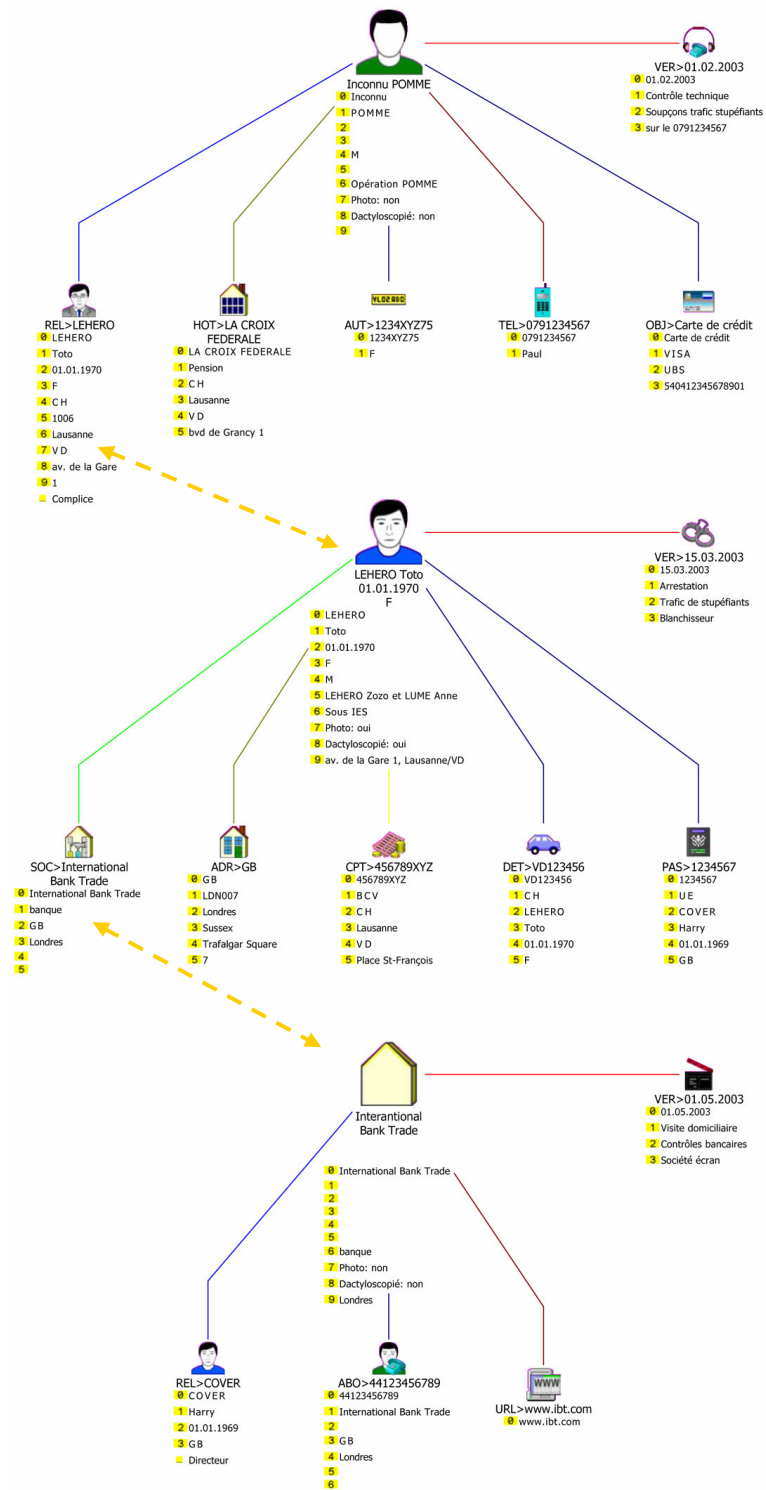


fig 84 : JANUS PV : Exemple de l'organisation des données IDENTITE – « sous-champs »

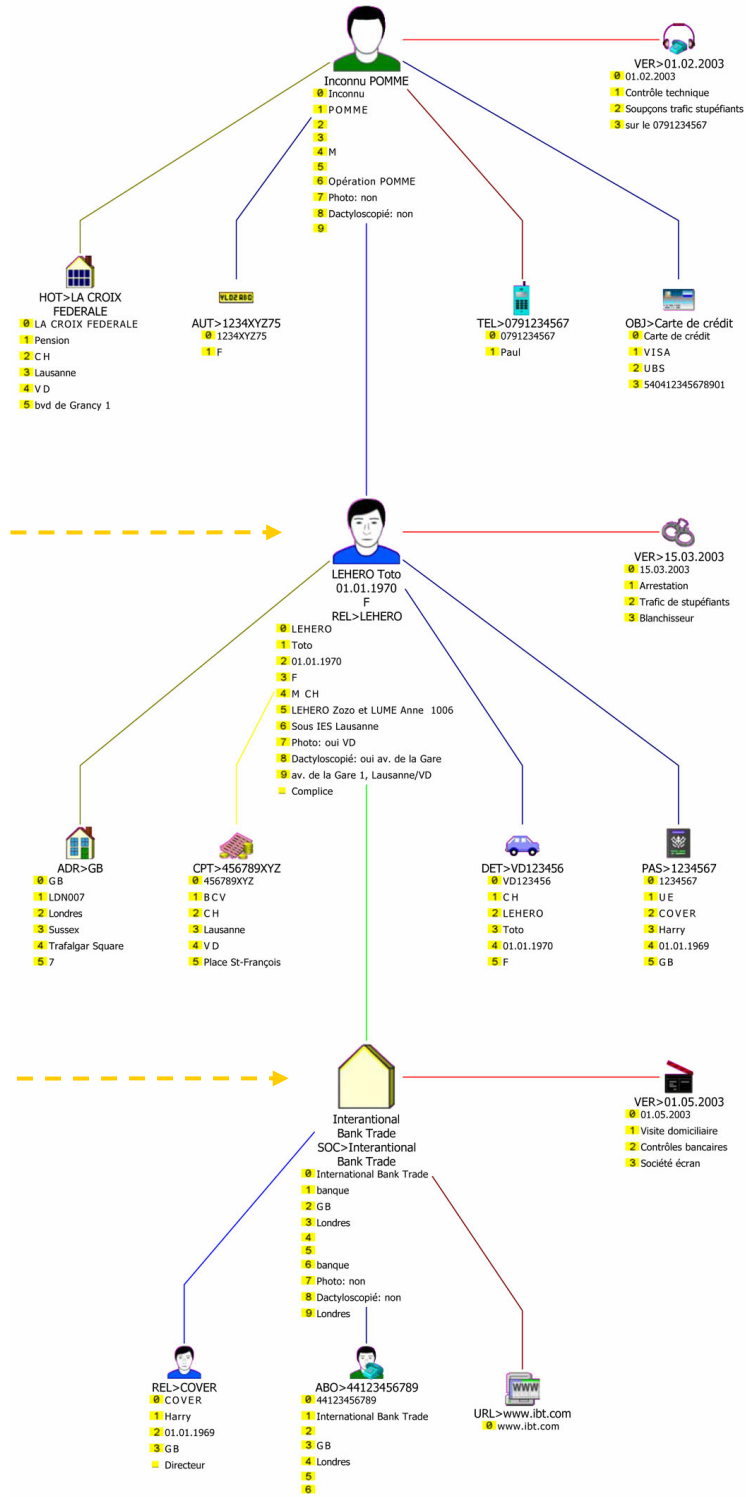


fig. 85 : JANUS PV : Correction de l'organisation des données IDENTITE – « sous-champs »

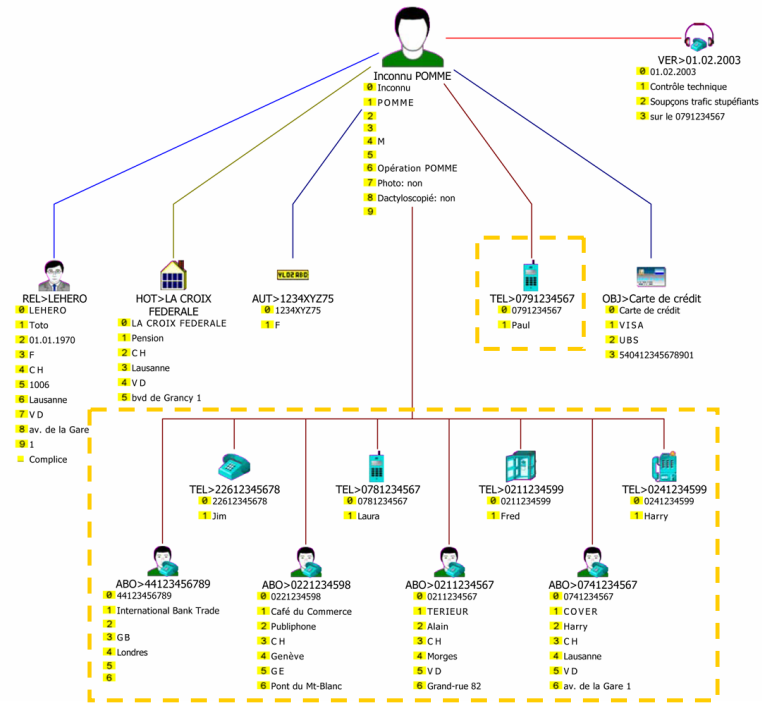


fig. 86 : JANUS PV : Mention des contrôles techniques dans des « sous-champs »

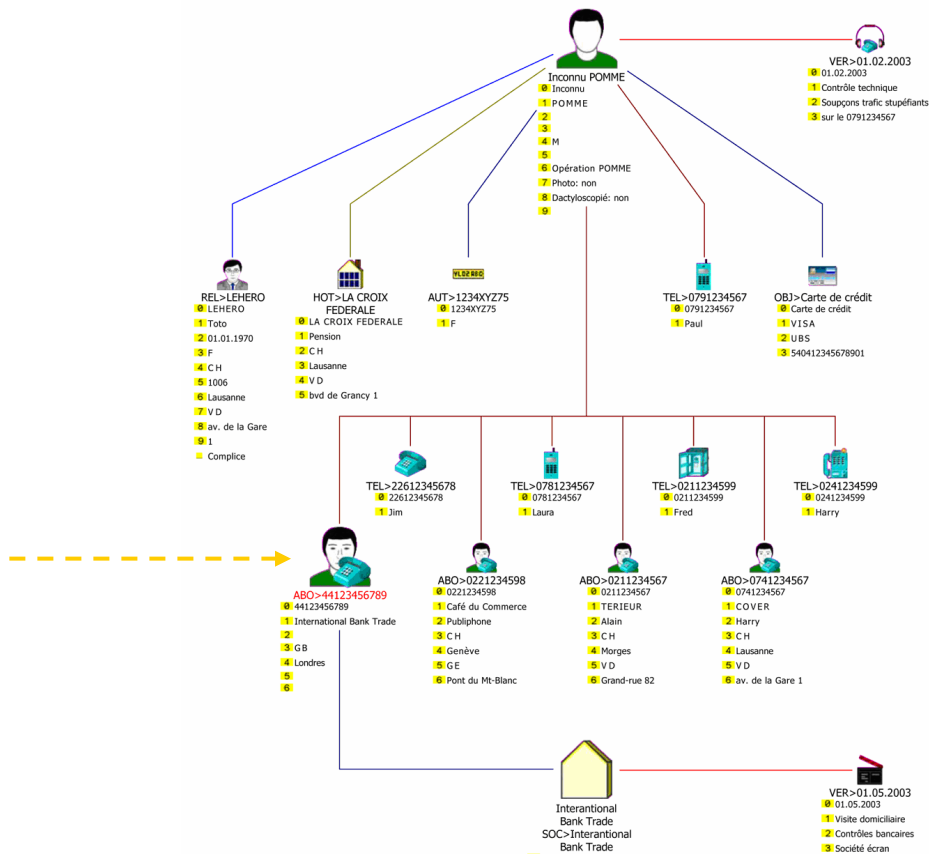


fig. 87 : JANUS PV : Connexion automatique des « sous-champs »



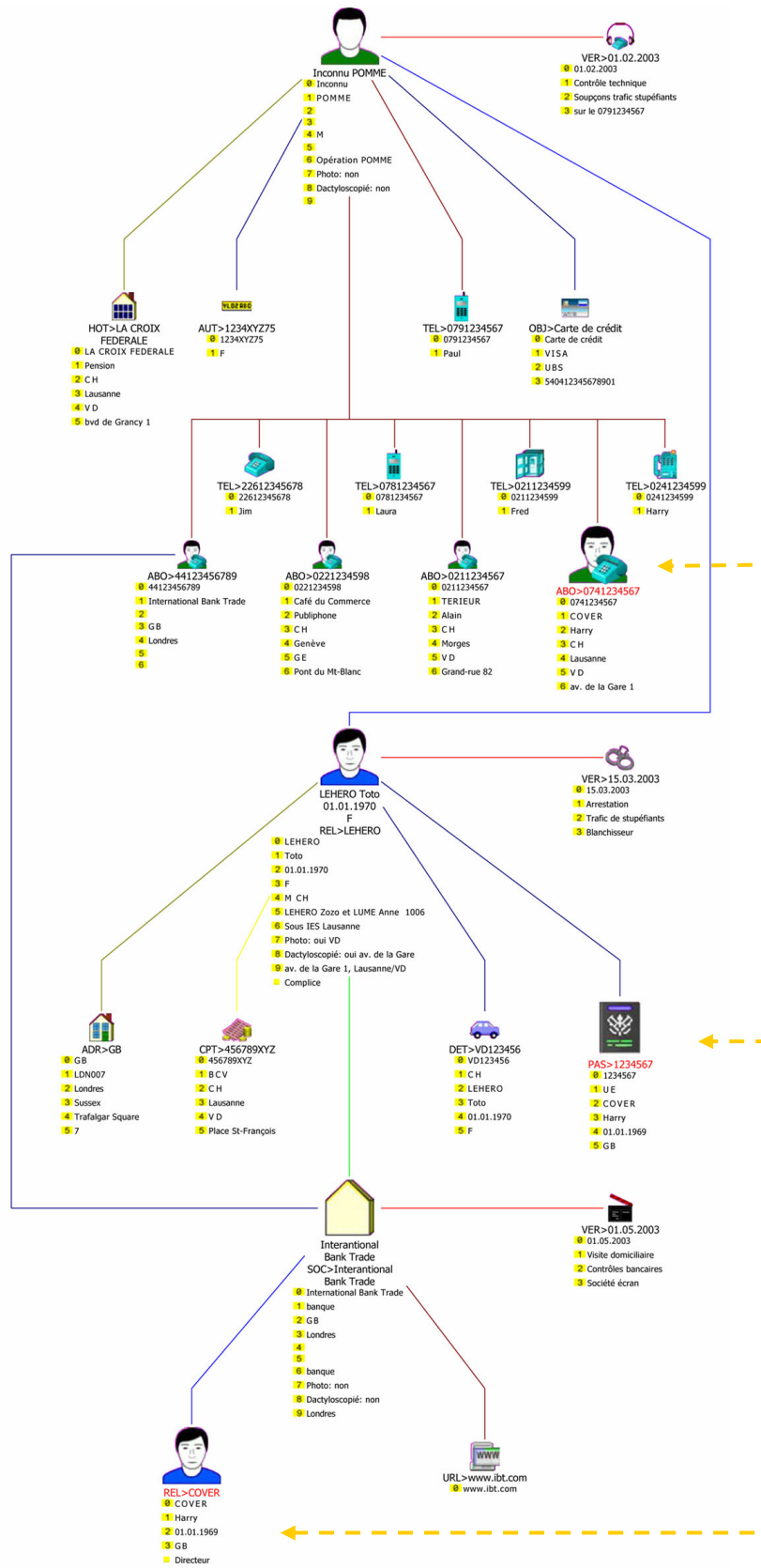


fig. 88 : JANUS PV : Perte du potentiel de liaison des « sous-champs » avec des liens indirects de niv. 2

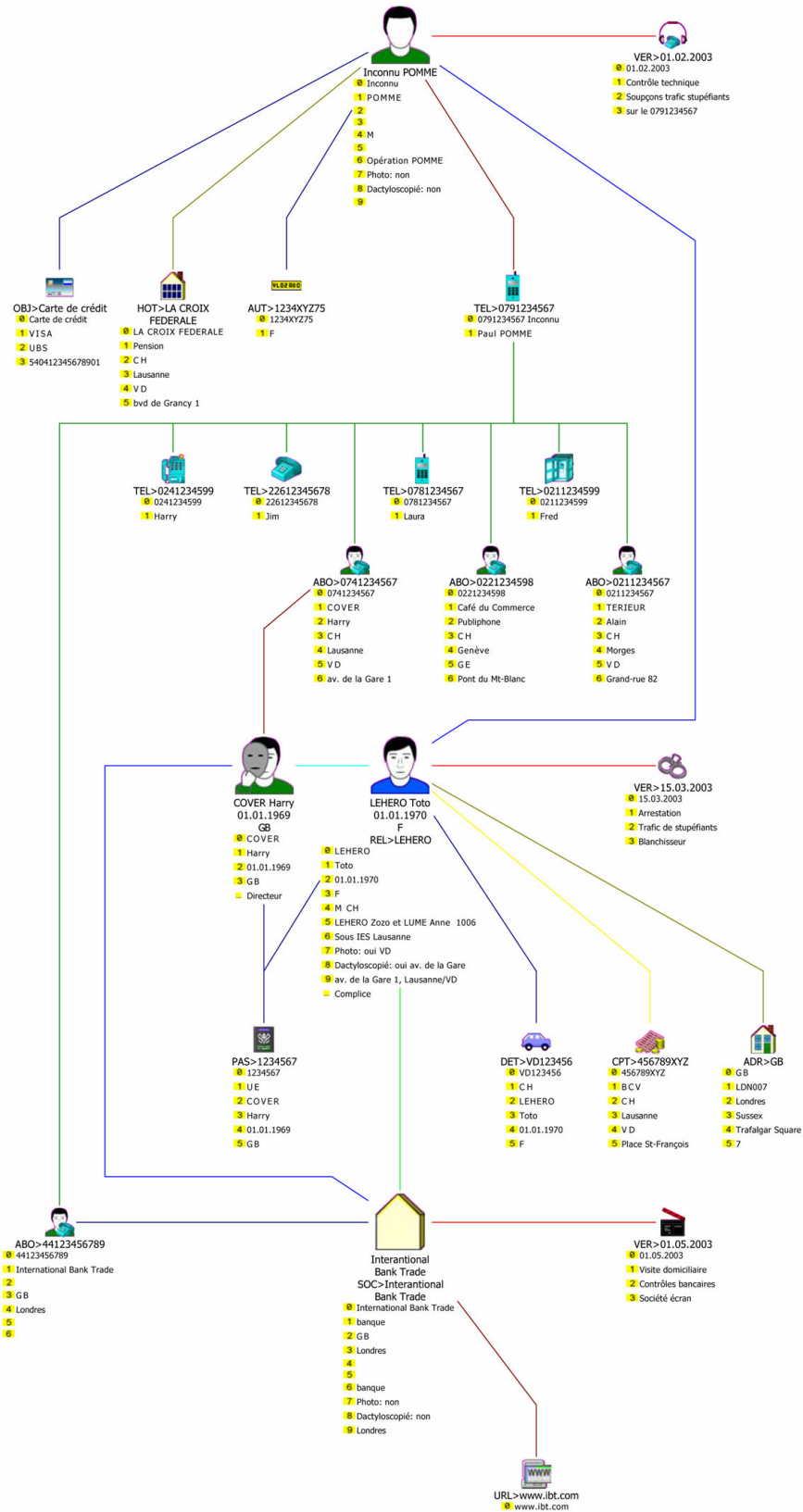


fig. 89 : JANUS PV : Schéma définitif sur la base du schéma provisoire issu de la base de données

## Icône Antécédent :

Action		Arrest	
Binoculars		Cassette	
<u>Filing Cabinet</u>		Headphones	
Incident		Search	
Sentence		Shield US	
Shield UK			









## Icône Argent (biens) :

<u>Account</u>		ATM	
Cash		Chart	
Cheque		Credit	
Claim		Dollar	
Transaction		Wire Transfer	

















## Icône Choses (biens) :

Alcohol		Assault Weapon	
Bomb		Briefcase	
Building		Camera	
Cannabis		Camera Recorder	
Cassette		CD-ROM	
<u>Commodity</u>		Clothing	
Document		Disc	
Drugs		Dog	
Ecstasy		Dustbin	
Industrial Chemicals		I.D.	























Icône Choses (biens) - suite :

Gun		Jiffy Bag	
Jewellery		Kilo of Drugs	
Knife		Machine Gun	
Notebook		Passport	
PC		PDA	
Perfume		Pepper Spray	
Pills		Rope	
RX		Shotgun	
Tobacco		Video Camera	
Video Cassette			
























Icône Communication

Cellphone		CD-ROM	
Envelope		E-mail	
Fax Machine		Fax	
Pager		Letter	
Payphone		Parcel	
PDA		PC	
Phone Box		SIM Card	
<u>Telephone</u>		WWW	



## Icône Evénement

Action		Arrest	
Arson		Assassination	
Body		Binoculars	
Counterfeit		Clock	
Fraud		<u>Event</u>	
Headphones		Hazard	
Incident		Kidnapping	
Magnifying Glass		Meeting	
Query		Search	
Sentence		Shield UK	
Shield US		Software Piracy	

## Icône Forensique (traces) :

Bullet		Bullet Case	
Bullet Cases		Camera	
Cassette		Counterfeit	
Disc		DNA	
Drugs		Evidence Collection	
Fingerprint		<u>Forensic</u>	
Footprint		Nuclear	
Magnifying Glass		Radiation	
PC		Video Cassette	
Tyre Tread			
Airport		Airport Terminal	
Arena		Bank	







Icône Lieu (sans les drapeaux des pays) :

Building		Casino	
Cell		Coach Station	
Court		Church	
Garage		Government	
Factory		House	
Hospital		Hospital bed	
Industrial Plant		Laboratory	
Lake		Letter box	
Mailbox		Medical Lab	
Organisation		Mosque	
<u>Place</u>		Office	
Port		Petrol pump	
Public House		Prison	
Shop		Restaurant	
Supermarket		Theatre	
Train Station		Warehouse	
Workshop		+ Cantons CH (26 x)	

































## Icône Personne :

Adult		Anonymous	
Bank		Boy	
Body		Building	
Casino		Child	
Dealer		Doctor	
Factory		Female	
Female [black]		Female [blue]	
Female [green]		Female [red]	
Fugitive		Garage	
Girl		In-mate	
Government		Lawyer [female]	
Laboratory		<u>Male</u>	
Lawyer [male]		Male [blue]	
Male [black]		Male [red]	
Male [green]		Medical Lab	
Man		Office	
Offender		Organisation	
Officer		Patient	
Other name		Petrol pump	
Person		Prison Officer	
Policeman		Professional [female]	
Prisoner		Public House	
Professional [male]		Shop	
Restaurant		Subscriber	

Icône Personne - suite :

Shell Company		Warehouse	
Spy		Workshop	
Theatre		Woman	

Icône Transport :

Aeroplane		Artic. Cab	
<u>Car</u>		Container Ship	
Coach		Cycle	
Cruiser		Flatbed	
Ferry		Helicopter	
Freighter		HGV Flat	
HGV		Lear Jet	
Hovercraft		Lorry	
License Plate		Motorcycle	
Luton Van		Number Plate	
Minibus		Pickup Van	
Pickup		Police Car US	
Police Car UK		Speedboat	
Ship		Train	
Trailer		Van	
Trawler		Yacht	



## iBase Database Design Report



### Prototype β

**File:** Janus\_pv\_2.idb  
**Description:** Modèle de base compatible avec JANUS PV 2.0  
**Version:** 4.0  
**Audit Level:** 1

## Entity Table Descriptions



### Antécédent

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Antécédent	Icon						
Id JANUS	Text	20	Filing Cabinet	Upper Case	Yes	Yes	Yes
Date Doc	Date		Today	Long Date		Yes	
Dossier	Yes/No		No				
Fiable	Yes/No		No				
Domaine	Suggested: Domaine					Yes	
Lien CO	Yes/No		No				
Procédure	Suggested: Procédure						
Transmission	Yes/No		No				
Resp. de l'enquête	Suggested: Géo_CH_International						
Groupe d'auteurs	Suggested: Géo_CH_International						
Attribution géographique	Suggested: Géo_CH_International						
Source PV	Text	50					
N° d'affaire	Text	50					
Opération	Text	50					
PJF_dossier_1	Text	50					
PJF_dossier_2	Text	50					
PJF_N°_Réf	Text	50					

PJF_N°_procédure	Text	50							
PJF_Projet	Text	50							
Qualification (4x4)	Selected: 4x4								
Source	Suggested: Source				Rens Police			Yes	
Texte	Multi-Line Text								



### Argent (biens)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Argent (biens)	Icon		Account			Yes	
Rôle	Suggested: Rôle Argent						
Numéro de référence	Text	20		Upper Case	Yes	Yes	Yes
Nom de la banque	Multi-Line Text						
Renseignements divers	Multi-Line Text (Append Only)						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	



### Choses (biens)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Choses (biens)	Icon		Commodity			Yes	
Type	Suggested: Type Choses						
Numéro de référence	Text	30		Upper Case	Yes	Yes	Yes
Gravure	Text	50					
Marque / quoi	Text	30				Yes	
Description	Multi-Line Text						
Renseignements divers	Multi-Line Text						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	



## Communication

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Communication	Icon		Telephone			Yes	
Moyen de communication	Suggested: Moyen de communication					Yes	
Numéro / Adresse Fournisseur	Text Suggested: Prestataires de service	30		Upper Case	Yes	Yes	Yes
Sur écoute	Yes/No		No				
Type	Selected: Type de moyen comm					Yes	
IMEI	Text	25		Upper Case			
SIM	Text	25		Upper Case			
Rôle variable du au	Suggested: Rôle moyen comm Date			Medium Date			
Renseignements divers	Multi-Line Text (Append Only)			Medium Date			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	



## Evénement

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Evénement	Icon		Event			Yes	
Date	Date			Short Date	Yes	Yes	Yes
Heure	Time			Short Time			
Type	Suggested: Evénement				Yes	Yes	Yes
Lieu	Text	50			Yes		Yes
Motif	Text	50					
Détail	Multi-Line Text						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	



## Forensique (traces)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Forensic	Icon		Forensic			Yes	
Type de trace	Suggested: Type de traces					Yes	
Code	Text	20		Upper Case	Yes	Yes	Yes
Description	Multi-Line Text						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	



## Lieu

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Lieu	Icon		Place			Yes	
Type d'adresse	Suggested: Type d'adresse						
Variable du au	Date			Short Date			
Code pays	Suggested: Code pays						
Pays	Suggested: Pays	20					
NPA	Text	30				Yes	
Lieu	Text						
Canton	Suggested: Cantons		VD				
Rue	Text	50					
Numéro	Text	10					
c/o	Text	50					
Renseignements divers	Multi-Line Text (Append Only)						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	



## Personne / Société

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Personne / Société	Icon					Yes	
Id JANUS	Text	20			Yes		Yes
NOM	Text	50		Upper Case	Yes	Yes	Yes
Prénom	Text	50		Upper Case	Yes	Yes	Yes
Nom de naissance	Text	50		Upper Case	Yes		
Date de naissance	Date			Short Date	Yes		Yes
Pays de naissance	Suggested: Pays						
Lieu de naissance	Text	50		Upper First			

Annexe III – Rapport du design du prototype β

Nationalité	Suggested: Pays		Suisse			
Lieu d'origine	Text	50			Upper First	
Sexe	Selected: Sexe					
Etat civil	Suggested: Etat civil					
NOM du père	Text	50			Upper Case	
Prénom du père	Text	50			Upper First	
NOM de la mère	Text	50			Upper Case	
Prénom de la mère	Text	50			Upper First	
NOM du conjoint	Text	50			Upper Case	Yes
Prénom du conjoint	Text	50			Upper First	
Moyen de contrôle	Suggested: Moyen de contrôle					
Source du contrôle	Suggested: Source contrôle					
Dactyloscopié	Yes/No		No			
Photo disponible	Yes/No		No			
ADN	Yes/No		No			
Remarques	Multi-Line Text (Append Only)					
Surnom	Multi-Line Text (Append Only)					
Photo	Picture				Upper First	
Qualification (4x4)	Selected: 4x4					
Source	Suggested: Source		Rens Police			Yes



**Transport**

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Icone Transport	Icon		Car			Yes	
Genre vhc	Suggested: Type vhc		Voiture				
Pays	Suggested: Pays		SUISSE (CH)				
Canton	Suggested: Cantons						
N° de plaque	Text	20		Upper Case	Yes	Yes	Yes
Marque / fabricant	Suggested: Marque véhicules				Yes		
Modèle	Text	20					
Couleur	Suggested: Couleurs						
VIN	Text	50					
N° matricule	Text	20		Upper Case			
Renseignements divers	Multi-Line Text			Upper Case			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

## Link Table Descriptions

### ... - ... (Lien générique) (Black)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Text	20				Yes	
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

#### End 1 Types

Antécédent, Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport

#### End 2 Types

Antécédent, Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport

### Abonnement/utilisation (Pers - Comm) (Maroon)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien Abonné					Yes	
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

#### End 1 Types

Personne / Société

#### End 2 Types

Communication

### Adresse (Pers - Lieu) (Olive)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: \$_Lien Adresse					Yes	
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

#### End 1 Types

Personne / Société

#### End 2 Types

Lieu

### Antécédent (Pers - Antécédent) (Red)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Domaine	Suggested: Domaine						
Date	Date			Short Date			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

End 1 Types	End 2 Types
Personne / Société	Antécédent

### Communication (Comm - Comm) (Green)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Selected: Lien Communication					Yes	
Date	Date			Short Date			
Heure	Time			Short Time			
Contenu	Multi-Line Text						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

End 1 Types	End 2 Types
Communication	Communication

### Déplacement (Lieu - ...) (Fuchsia)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien Déplacement		Déplacement			Yes	
Date départ	Date			Short Date			
Date de retour	Date			Short Date			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

End 1 Types	End 2 Types
Lieu	Antécédent, Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport

### Destinataire/Récepteur (Pers - Comm) (Teal)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Date d'envoi/réception	Date			Short Date		Yes	
Heure d'envoi/réception	Time			Short Time			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

End 1 Types	End 2 Types
Personne / Société	Communication

### Événement - ... (Red)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien Événement					Yes	
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

End 1 Types	End 2 Types
Événement	Antécédent, Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport



## Forensique - ... (Silver)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Text	20				Yes	
Qualification (4x4)	Selected: 4x4 Suggested: Source					Yes	
Source			Rens Police				

### End 1 Types

Forensique (traces)

### End 2 Types

Antécédent, Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport

## Propriété/utilisation (Pers - Argent) (Yellow)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: \$_Lien		Titulaire			Yes	
Qualification (4x4)	propriété/utilisation Selected: 4x4 Suggested: Source					Yes	
Source			Rens Police				

### End 1 Types

Personne / Société

### End 2 Types

Argent (biens)

## Propriété/utilisation (Pers - Choses/Transp) (Navy)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: \$_Lien		Propriétaire			Yes	
Qualification (4x4)	propriété/utilisation Selected: 4x4 Suggested: Source					Yes	
Source			Rens Police				

### End 1 Types

Personne / Société

### End 2 Types

Choses (biens), Transport

## Relation (Pers physique - Inconnu) (Aqua)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
------	------	------	---------	--------	---------	-----------	---------------

Légende	Suggested: Lien Personne - Inconnu	Alias	Yes	
Qualification (4x4)	Selected: 4x4			
Source	Suggested: Source	Rens Police	Yes	

<b>End 1 Types</b> Personne / Société	<b>End 2 Types</b> Personne / Société
--	--

## Relation (Pers physique - Pers physique) (Blue)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien Personne - Personne		Connaissance			Yes	
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

<b>End 1 Types</b> Personne / Société	<b>End 2 Types</b> Personne / Société
--	--

## Relation (Pers physique - Société) (Lime)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien Personne - Société Text	50	Employé			Yes	
Description							
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

<b>End 1 Types</b> Personne / Société	<b>End 2 Types</b> Personne / Société
--	--

## Sous-champs (Antécédent - ...) (Grey)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Sous-champs						
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

<b>End 1 Types</b>	<b>End 2 Types</b>
--------------------	--------------------

Antécédent

Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport

## Transaction Argent (biens) (Red)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: \$_Lien transaction (Argent)					Yes	
Montant	Real Number						
Monnaie	Selected: Monnaie		CHF				
Date	Date			Short Date			
Heure	Time			Short Time			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

**End 1 Types**  
Argent (biens)

**End 2 Types**  
Argent (biens), Personne / Société

## Transaction Choses (biens) (Purple)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien transaction (Choses)					Yes	
Date	Date			Short Date			
Heure	Time			Short Time			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

### End 1 Types

Choses (biens)

### End 2 Types

Argent (biens), Choses (biens), Personne / Société

## Emplacement (Lieu - ...) (Black)

Name	Type	Size	Default	Format	Indexed	Mandatory	Discriminator
Légende	Suggested: Lien Emplacement		Emplacement			Yes	
Date	Date			Short Date			
Qualification (4x4)	Selected: 4x4						
Source	Suggested: Source		Rens Police			Yes	

### End 1 Types

Lieu

### End 2 Types

Antécédent, Argent (biens), Choses (biens), Communication, Événement, Forensique (traces), Lieu, Personne / Société, Transport

## Code Lists

### Pick Lists

Pick List Name	Items
\$_Lien Adresse	Adresse officielle, Adresse professionnelle, Bar / Dancing, Dépôt drogue, Dernier domicile connu, Deuxième adresse, Domicile juridique, Feriendomizil, Foyer / Maison, inconnu, Lieu de référence, Lieu de rencontre, Lieu de séjour, Lieu de travail, Motel, Restaurant, Séjour
\$_Lien propriété/utilisation	Bénéficiaire, Conducteur, Dépositaire, inconnu, Locataire, Mandataire, Passager, Prêt, Procuration, Propriétaire, Propriétaire/chauffeur, Signataire, Titulaire, Utilisateur
\$_Lien transaction (Argent) 4x4	Carte de crédit, Changement, Chèque, Inconnue, Liquide, Ordre de paiement, Virement
Cantons	A1, A2, A3, A4, B1, B2, B3, B4, C1, C2, C3, C4, X1, X2, X3, X4 AG+, AI+, AR+, BA+, BE+, BKP, BL+, BS+, FL, FR+, GE+, GL+, GR+, IP, JU+, LU+, NE+, NW+, OW+, SG+, SH+, SO+, SZ+, TG+, TI+, UR+, VD+, VS+, ZH+
Code pays	AD, AE, AF, AG, AI, AL, AM, AN, AO, AQ, AR, AS, AT, AU, AW, AX, AZ, BA, BB, BD, BE, BF, BG, BH, BI, BJ, BM, BN, BO, BR, BS, BT, BV, BW, BY, BZ, CA, CC, CD, CF, CG, CH, CI, CK, CL, CM, CN, CO, CR, CS, CU, CV, CX, CY, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, EH, ER, ES, ET, FI, FJ, FK, FM, FO, FR, GA, GB, GD, GE, GF, GH, GI, GL, GM, GN, GP, GQ, GR, GS, GT, GU, GW, GY, HK, HM, HN, HR, HT, HU, ID, IE, IL, IN, IO, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KI, KM, KN, KP, KR, KY, KZ, LA, LB, LC, LI, LK, LR, LS, LT, LU, LV, LY, MA, MC, MD, MG, MH, MK, ML, MM, MN, MO, MP, MQ, MR, MS, MT, MU, MV, MW, MX, MY, MZ, NA, NC, NE, NF, NG, NI, NL, NO, NP, NR, NU, NZ, OM, PA, PE, PF, PG, PH, PK, PL, PM, PN, PR, PS, PT, PW, PY, QA, RE, RO, RU, RW, SA, SB, SC, SD, SE, SG, SH, SI, SJ, SK, SL, SM, SN, SO, SR, ST, SV, SY, SZ, TC, TD, TF, TG, TH, TJ, TK, TL, TM, TN, TO, TR, TT, TV, TW, TZ, UA, UG, UM, US, UY, UZ, VA, VC, VE, VG, VI, VN, VU, WF, WS, YE, YT, ZA, ZM, ZW
Couleurs	beige, blanc, bleu, brun, gris, inconnu, jaune, noir, rouge, vert
Domaine	BL, CE, CO, CR, FM, PE, PG, ST, TA, TE, TH, VE, VI
Etat civil	célibataire, défunt, divorcé, inconnu, marié, séparé, veuf
Evènement	Arrestation, Condamnation, Crime, Enquête, Fraude, Garantie, Incendie, Inconnu, Interpellation, Meurtre, Mise sous écoute, Observation, Opération police, Recherches préliminaires, Rencontre, Rendez-vous, Rétroactif, Saisie

Annexe III – Rapport du design du prototype β

Géo_CH_International	AD, AE, AF, AG, AG+, AI, AI+, AL, AM, AN, AO, AQ, AR, AR+, AS, AT, AU, AW, AX, AZ, BA, BA+, BB, BD, BE, BE+, BF, BG, BH, BI, BJ, BKP, BL+, BM, BN, BO, BR, BS, BS+, BT, BV, BW, BY, BZ, CA, CC, CD, CF, CG, CH, CI, CK, CL, CM, CN, CO, CR, CS, CU, CV, CX, CY, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, EH, ER, ES, ET, FI, FJ, FK, FL, FM, FO, FR, FR+, GA, GB, GD, GE, GE+, GF, GH, GI, GL, GL+, GM, GN, GP, GQ, GR, GR+, GS, GT, GU, GW, GY, HK, HM, HN, HR, HT, HU, ID, IE, IL, IN, IO, IP, IQ, IR, IS, IT, JM, JO, JP, JU+, KE, KG, KH, KI, KM, KN, KP, KR, KW, KY, KZ, LA, LB, LC, LI, LK, LR, LS, LT, LU, LU+, LV, LY, MA, MC, MD, MG, MH, MK, ML, MM, MN, MO, MP, MQ, MR, MS, MT, MU, MV, MW, MX, MY, MZ, NA, NC, NE, NE+, NF, NG, NI, NL, NO, NP, NR, NU, NW+, NZ, OM, OW+, PA, PE, PF, PG, PH, PK, PL, PM, PN, PR, PS, PT, PW, PY, QA, RE, RO, RU, RW, SA, SB, SC, SD, SE, SG, SG+, SH, SH+, SI, SJ, SK, SL, SM, SN, SO, SO+, SR, ST, SV, SY, SZ, SZ+, TC, TD, TF, TG, TG+, TH, TI+, TJ, TK, TL, TM, TN, TO, TR, TT, TV, TZ, UA, UG, UG, UM, UR+, US, UY, UZ, VA, VC, VD+, VE, VG, VI, VN, VS+, VU, WF, WS, YE, YT, ZA, ZH+, ZM, ZW
Lien Abonné	Abonné, Utilisateur
Lien Communication	Appel vocal, Connexion, Données, E-mail, SMS/MMS
Lien Déplacement	Déplacement, Vacances, Voyage
Lien Destinataire/Récepteur	Expéditeur, Récepteur, Utilisateur, Visiteur
Lien Emplacement	Emplacement, Lieu
Lien Événement	Auteur, Cible, Complice, Confiscation, Présent, Saisie, Séquestre, Sujet, Suspect, Tentative, Victime
Lien Personne - Inconnu	Alias, Connaissance, Employé, Fréquentation
Lien Personne - Personne	Ami, Concubins, Connaissance, Enfant, Frère / Soeur, Mari / Femme, Parent, Relation
Lien Personne - Société	Actionnaire, Associé, Employé, Gérant, Gestionnaire, Patron, Propriétaire
Lien transaction (Choses)	Donation, Echange, Envoi, Réception, Transmission, Vente
Marque véhicules	Abarth, Alfa Romeo, Alpine, Aprilia, Aston Martin, Audi, Autobianchi, Autre, Bentley, BMW, Bugatti, Buick, Cadillac, Cagiva, Chevrolet, Chrysler, Citroën, Daewoo, Daihatsu, Daimler, Datsun, Dodge, Ducati, Ferrari, Fiat, Ford, General Motors, GMC, Harley Davidson, Honda, Hyundai, Innocenti, Isuzu, Iveco, Jaguar, Jeep, Kawasaki, Kia, Lada, Lamborghini, Lancia, Land Rover, Lexus, Lotus, Mack, Man, Maserati, Mazda, MBK, Mercedes Benz, Mercury, MG, Mini, Mitsubishi, Moto Guzzi, Nissan, Noeplan, Oldmobile, Opel, Peugeot, Piaggio, Plymouth, Pontiac, Porsche, Proton, Range Rover, Renault, Rolls Royce, Rover, Saab, Saturn, Saurer, Seat, Skoda, Smart, Ssangyong, Subaru, Suzuki, Talbot, Toyota, Triumph, Volkswagen, Volvo, Yamaha
Monnaie	AED, AFN, ALL, AMD, ANG, AOA, ARS, AUD, AWG, AZM, BAM, BBD, BDT, BGN, BHD, BMD, BND, BOB, BRL, BSD, BTN, BWP, BYR, BZD, CAD, CDF, CHF, CLP, CNY, COP, CRC, CSD, CUP, CVE, CYP, CZK, DJV, DKK, DOP, DZD, ECS, EEK, EGP, ETB, EUR, FJD, FKP, GBP, GEL, GHC, GIP, GMD, GNF, GTQ, GYD, HKD, HNL, HRK, HUF, HTG, IDR, ILS, INR, IQD, IRR, ISK, JMD, JOD, JPY, KES, KGS, KHR, KMF, KPW, KRW, KWD, KYD, KZT, LAK, LBP, LKR, LRD, LSL, LTL, LVL, LYD, MAD, MDL, MGF, MKD, MMK, MNT, MOP, MRO, MTL, MUR, MVR, MWK, MXN, MYR, MZM, NAD, NGN, NIO, NOK, NPR, NZD, OMR, PAB, PEN, PGK, PHP, PKR, PLN, PYG, QAR, ROL, RUB, RWF, SAR, SBD, SCR, SDD, SEK, SGD, SHP, SIT, SKK, SLL, SOS, SRD, STD, SVC, SYP, SZL, THB, TJS, TMM, TND, TOP, TRL, TTD, TWD, TZS, UAH, UGX, USD, UYU, UZS, VEB, VND, VUV, WST, XAF, XCD, XOF, XPF, YER, YTL, ZAR, ZMK, ZWD
Moyen de communication	E-mail, IP/URL, Tel.Nr.
Moyen de contrôle	AFIS, carte d'identité, inconnu, pas vérifié, Passeport, Permis, Pièce d'identité d'étranger, propre indication, Provider, Registre du commerce, vérifié officiellement

Annexe III – Rapport du design du prototype β

<p>Pays</p>	<p>AFGHANISTAN (AF), AFRIQUE DU SUD (ZA), ÅLAND, ÎLES (AX), ALBANIE (AL), ALGÉRIE (DZ), ALLEMAGNE (DE), ANDORRE (AD), ANGOLA (AO), ANGIJILLA (AI), ANTARCTIQUE (AQ), ANTIGUA-ET-BARBUDA (AG), ANTILLES NÉERLANDAISES (AN), ARABIE SAOUDITE (SA), ARGENTINE (AR), ARMÉNIE (AM), ARUBA (AW), AUSTRALIE (AU), AUTRICHE (AT), AZERBAÏDJAN (AZ), BAHAMAS (BS), BAHRÉÏN (BH), BANGLADESH (BD), BARBADE (BB), BÉLARUS (BY), BELGIQUE (BE), BELIZE (BZ), BÉNIN (BJ), BERMUDES (BM), BHOUTAN (BT), BOLIVIE (BO), BOSNIE-HERZÉGOVINE (BA), BOTSWANA (BW), BOUVET, ÎLE (BV), BRÉSIL (BR), BRUNÉI DARUSSALAM (BN), BULGARIE (BG), BURKINA FASO (BF), BURUNDI (BT), CAÏMANES, ÎLES (KY), CAMBODGE (KH), CAMEROUN (CM), CANADA (CA), CAP-VERT (CV), CENTRAFRICAINE, RÉPUBLIQUE (CF), CHILI (CL), CHINE (CN), CHRISTMAS, ÎLE (CX), CHYPRE (CY), COCOS (KEELING), ÎLES (CC), COLOMBIE (CO), COMORES (KM), CONGO (CG), CONGO, LA RÉPUBLIQUE DÉMOCRATIQUE DU (CD), COOK, ÎLES (CK), CORÉE, RÉPUBLIQUE DE (KR), CORÉE, RÉPUBLIQUE POPULAIRE DÉMOCRATIQUE DE (KP), COSTA RICA (CR), CÔTE D'IVOIRE (CI), CROATIE (HR), CUBA (CU), DANEMARK (DK), DJIBOUTI (DJ), DOMINICAINE, RÉPUBLIQUE (DO), DOMINIQUE (DM), ÉGYPTE (EG), EL SALVADOR (SV), ÉMIRATS ARABES UNIS (AE), ÉQUATEUR (EC), ÉRYTHÉE (ER), ESPAGNE (ES), ESTONIE (EE), ÉTATS-UNIS (US), ÉTHIOPIE (ET), FALKLAND, ÎLES (MALVINAS) (FK), FÉROÉ, ÎLES (FO), FIDJI (FJ), FINLANDE (FI), FRANCE (FR), GABON (GA), GAMBIE (GM), GÉORGIE (GE), GÉORGIE DU SUD ET LES ÎLES SANDWICH DU SUD (GS), GHANA (GH), GIBRALTAR (GI), GRÈCE (GR), GRENADE (GD), GROENLAND (GL), GUADELOUPE (GP), GUAM (GU), GUATEMALA (GT), GUINÉE (GN), GUINÉE ÉQUATORIALE (GQ), GUINÉE-BISSAU (GW), GUYANA (GY), GUYANE FRANÇAISE (GF), HAÏTI (HT), HEARD, ÎLE ET MCDONALD, ÎLES (HM), HONDURAS (HN), HONG-KONG (HK), HONGRIE (HU), ÎLES MINEURES ÉLOIGNÉES DES ÉTATS-UNIS (UM), ÎLES VIERGES BRITANNIQUES (VG), ÎLES VIERGES DES ÉTATS-UNIS (VI), INDE (IN), INDONÉSIE (ID), IRAN, RÉPUBLIQUE ISLAMIQUE D' (IR), IRAQ (IQ), IRLANDE (IE), ISLANDE (IS), ISRAËL (IL), ITALIE (IT), JAMAÏQUE (JM), JAPON (JP), JORDANIE (JO), KAZAKHSTAN (KZ), KENYA (KE), KIRGHIZISTAN (KG), KIRIBATI (KI), KOWEÏT (KW), LAO, RÉPUBLIQUE DÉMOCRATIQUE POPULAIRE (LA), LESOTHO (LS), LETTONIE (LV), LIBAN (LB), LIBÉRIA (LR), LIBYENNE, JAMAHIRIYA ARABE (LY), LIECHTENSTEIN (LI), LITUANIE (LT), LUXEMBOURG (LU), MACAO (MO), MACÉDOINE, L'EX-RÉPUBLIQUE YOUGOSLAVE DE (MK), MADAGASCAR (MG), MALAISIE (MY), MALAWI (MW), MALDIVES (MV), MALI (ML), MALTE (MT), MARIANES DU NORD, ÎLES (MP), MAROC (MA), MARSHALL, ÎLES (MH), MARTINIQUE (MQ), MAURIE (MU), MAURITANIE (MR), MAYOTTE (YT), MEXIQUE (MX), MICRONÉSIE, ÉTATS FÉDÉRÉS DE (FM), MOLDOVA, RÉPUBLIQUE DE (MD), MONACO (MC), MONGOLIE (MN), MONTSERRAT (MS), MOZAMBIQUE (MZ), MYANMAR (MM), NAMIBIE (NA), NAURU (NR), NÉPAL (NP), NICARAGUA (NI), NIGER (NE), NIGÉRIA (NG), NIUÉ (NU), NORVÈGE (NO), NOUVELLE-CALÉDONIE (NC), NOUVELLE-ZÉLANDE (NZ), OCÉAN INDIEN, TERRITOIRE BRITANNIQUE DE L' (IO), OMAN (OM), OUGANDA (UG), OUZBÉKISTAN (UZ), PAKISTAN (PK), PALAOS (PW), PALESTINIEN OCCUPÉ, TERRITOIRE (PS), PANAMA (PA), PAPOUASIE-NOUVELLE-GUINÉE (PG), PARAGUAY (PY), PAYS-BAS (NL), PÉROU (PE), PHILIPPINES (PH), PITCAIRN (PN), POLOGNE (PL), POLYNÉSIE FRANÇAISE (PF), PORTO RICO (PR), PORTUGAL (PT), QATAR (QA), RÉUNION (RE), ROUMANIE (RO), ROYAUME-UNI (GB), RUSSIE, FÉDÉRATION DE (RU), RWANDA (RW), SAHARA OCCIDENTAL (EH), SAINTE-HÉLÈNE (SH), SAINTE-LUCIE (LC), SAINT-KITTS-ET-NEVIS (KN), SAINT-MARIN (SM), SAINT-PIERRE-ET-MIQUELON (PM), SAINT-SIÈGE (ÉTAT DE LA CITÉ DU VATICAN) (VA), SAINT-VINCENT-ET-LES GRENADINES (VC), SALOMON, ÎLES (SB), SAMOA AMÉRICAINES (AS), SAO TOMÉ-ET-PRINCIPE (ST), SÉNÉGAL (SN), SERBIE-ET-MONTÉNÉGO (CS), SEYCHELLES (SC), SIERRA LEONE (SL), SINGAPOUR (SG), SLOVAQUIE (SK), SLOVÉNIE (SI), SOMALIE (SO), SOUDAN (SD), SRI LANKA (LK), SUÈDE (SE), SUISSE (CH), SURINAME (SR), SVALBARD ET ÎLE JAN MAYEN (SJ), SWAZILAND (SZ), SYRIENNE, RÉPUBLIQUE ARABE (SY), TADJIKISTAN (TJ), TAÏWAN, PROVINCE DE CHINE (TW), TANZANIE, RÉPUBLIQUE-UNIE DE (TZ), TCHAD (TD), TCHÈQUE, RÉPUBLIQUE (CZ), TERRES AUSTRALES FRANÇAISES (TF), THAÏLANDE (TH), TIMOR-LESTE (TL), TOGO (TG), TOKELAU (TK), TONGA (TO), TRINITÉ-ET-TOBAGO (TT), TUNISIE (TN), TURKMÉNISTAN (TM), TURKS ET CAÏQUES, ÎLES (TC), TURQUIE (TR), TUVALU (TV), UKRAÏNE (UA), URUGUAY (UY), VANUATU (VU), VENEZUELA (VE), VIET NAM (VN), WALLIS ET FUTUNA (WF), YÉMEN (YE), ZAMBIE (ZM), ZIMBABWE (ZW)</p>
<p>Prestataires de service</p>	<p>Abalon, Bluewin, Cablecom, Callino, Direct, EasiLink, Easynet, Economy, EconoPhone, Globalzone, Green.ch, GTN, Interroute, Intertel, Magnet.ch, Multiink, Netstream Voice, One.Tel, Orange, SolNet, Sunrise, Swisscom, Swisscom mobile, swissonline, Tele 2, Telegroup, Téléphonique, Unbekannt, Vartec</p>
<p>Procédure</p>	<p>Non, Oui, Source publique</p>
<p>Rôle Argent</p>	<p>Inconnu, Mandataire, Propriétaire, Signataire</p>
<p>Rôle moyen comm</p>	<p>Abonné, Abonné/utilisateur, Cabine publique, Evaluation de téléphone portable, Inconnue, Utilisateur</p>
<p>Rôle vhc</p>	<p>Conducteur, Inconnu, Propriétaire, Propriétaire/chauffeur</p>
<p>Sexe</p>	<p>F, I, M</p>

Annexe III – Rapport du design du prototype β

Source	Annuaire, Contrôle des habitants, CT / CTR, Document, Informateur, Institution, JANUS, Medias, Mise en cause, Observation, Procès-verbal, Registre du commerce, Rens Police, Service des automobiles, cycles et bateaux, SPOP, Zephir
Source contrôle	AG+ pol. cant., AI+ pol. cant., AR+ pol. cant., BE+ pol. cant., BL+ pol. mun., BS+ pol. cant., FR+ pol. cant., GE+ pol. cant., GL+ pol. cant., GR+ pol. cant., JU+ pol. cant., LU+ pol. cant., NE+ pol. cant., NW+ pol. cant., OW+ pol. cant., PJF, SG+ pol. cant., SH+ pol. cant., SO+ pol. cant., SZ+ pol. cant., TG+ pol. cant., TI+ pol. cant., UR+ pol. cant., VD+ pol. cant., VS+ pol. cant., ZG+ pol. cant., ZH+ pol. cant., ZH+ pol. mun.
Sous-champs	ABO, COM, REL, TEL
Type Choses	Arme longue, Autorisation d'établissement, Autorisation de séjour, carte de crédit, Inconnu, Passeport, Permis, Pièce d'identité, Pièce
Type d'adresse	Adresse officielle, Adresse professionnelle, Dépôt drogue, Dernier domicile connu, Deuxième adresse, Domicile juridique, Foyer / Maison, Inconnu, Lieu de référence, Lieu de rencontre, Lieu de séjour, Lieu de travail, Maison de vacances, Séjour actuel, Séjour hebdomadaire, Succursale, Tierce adresse
Type de moyen comm	Analogique, Câble, inconnu, ISDN, Mobile
Type de traces	ADN, Analyse, Contrefaçon, Cybertraces, ED, Enregistrement, Microtraces, Stupéfiants, Trace de pas, Trace de pneu, Trace d'oreille, Traces d'outils
Type vhc	Autres, Avion, Bateau, Bateau a moteur, Bateau à voiles, Camion, Camion remorque, Camper, Car, Caravane, Fourgonnette, Remorque camion, Remorque voiture, Roller, Tracteur, Tram, Trike, Trolleybus, Vélo, Vélomoteur, Voiture, Voiture commerciale

## Icon Lists

Icon List Name	Items
Icone Antécédent	Action, Arrest, Binoculars, Cassette, Filing Cabinet, Headphones, Incident, Search, Sentence, Shield UK, Shield US
Icone Argent (biens)	Account, ATM, Cash, Chart, Cheque, Claim, Credit, Dollar, Transaction, Wire Transfer
Icone Choses (biens)	Alcohol, Assault Weapon, Bomb, Briefcase, Building, Camcorder, Camera, Cannabis, Cassette, CD-ROM, Clothing, Commodity, Disc, Document, Dog, Drugs, Dustbin, Ecstasy, Gun, I.D., Industrial Chemicals, Jewellery, Jiffy Bag, Kilo of Drugs, Knife, Machine Gun, Notebook, Passport, PC, PDA, Pepper Spray, Perfume, Pills, Rope, RX, Shotgun, Tobacco, Video Camera, Video Cassette
Icone Communication	CD-ROM, Cellphone, E-mail, Envelope, Fax, Fax Machine, Letter, Pager, Parcel, Payphone, PC, PDA, Phone Box, SIM Card, Telephone, WWW
Icone Événement	Action, Arrest, Arson, Assassination, Binoculars, Body, Clock, Counterfeit, Event, Fraud, Hazard, Headphones, Incident, Kidnapping, Magnifying Glass, Meeting, Query, Search, Sentence, Shield UK, Shield US, Software Piracy, Star
Icone Forensique	Bullet, Bullet Case, Bullet Cases, Camera, Cassette, Counterfeit, Disc, DNA, Drugs, Evidence Collection, Fingerprint, Footprint, Forensic, Magnifying Glass, Nuclear, PC, Radiation, Tyre Tread, Video Cassette



Annexe III – Rapport du design du prototype β

<p>Icone Lieu</p>	<p>Afghanistan, Airport, Airport Terminal, Antigua, Appenzell, Appenzell RE, Appenzell RI, Arena, Argentina, Argovie, Armenia, Australia, Austria, Azerbaïdjan, Bahamas, Bâle, Bâle Campagne, Bâle Ville, Bank, Barbados, Belarus, Belgium, Belize, Berne, Bolivia, Brazil, Building, Cambodia, Canada, Casino, Cell, Chile, China, Church, Coach Station, Colombia, Costa Rica, Court, Cuba, Denmark, Dominica, Dominican Rep., EC, Ecuador, Eire, El Salvador, Estonia, Factory, Finland, France, Fribourg, Garage, Genève, Georgia, Germany, Giaris, Government, Greece, Greenland, Grenada, Grisons, Guatemala, Guyanna, Haiti, Honduras, Hong Kong, Hospital, Hospital bed, House, Hungary, Iceland, India, Industrial Plant, Iran, Iraq, Isle of Man, Israel, Jamaica, Japan, Jura, Kazakhstan, Kirghizstan, Korea [North], Korea [South], Laboratory, Lake, Laos, Latvia, Letter box, Libya, Liechtenstein, Lithuania, Lucerne, Luxembourg, Mailbox, Medical Lab., Mexico, Moldova, Mosque, Netherlands, Neuchâtel, New Zealand, Nicaragua, Nidwald, Norway, Obwald, Office, Organisation, Pakistan, Panama, Paraguay, Peru, Petrol pump, Place, Poland, Port, Portugal, Prison, Public House, Puerto Rico, Restaurant, Russia, Saint Kitts and Nevis, Saudi Arabia, Schaffhouse, Schwyz, Shop, Singapore, Soleure, South Africa, Spain, St-Gall, Supermarket, Suriname, Sweden, Switzerland, Tadzchikistan, Tessin, Thailand, Theatre, Thurgovie, Train Station, Trinidad, Turkey, Turkmenistan, UK, Ukraine, Unterwald, Uri, Uruguay, USA, Uzbekistan, Valais, Vaud, Venezuela, Vietnam, Warehouse, Workshop, Zoug, Zurich</p>
<p>Icone Personne</p>	<p>Adult, Anonymous, Bank, Bank\$, Body, Boy, Building, Casino, Child, Dealer, Doctor, Factory, Female, Female [black], Female [blue], Female [green], Female [red], Fugitive, Garage, Girl, Government, In-mate, Laboratory, Lawyer [female], Lawyer [male], Male, Male [black], Male [blue], Male [green], Male [red], Man, Medical Lab., Offender, Office, Officer, Organisation, Other name, Patient, Person, Petrol pump, Policeman, Prison Officer, Prisoner, Professional [female], Professional [male], Public House, Restaurant, Shell Company, Shop, Spy, Subscriber, Theatre, Warehouse, Woman, Workshop</p>
<p>Icone Transport</p>	<p>Aeroplane, Artic. Cab, Car, Coach, Container Ship, Cruiser, Cycle, Ferry, Flatbed, Freighter, Helicopter, HGV, HGV Flat, Hovercraft, Lear Jet, License Plate, Lorry, Luton Van, Minibus, Motorcycle, Number Plate, Pickup, Pickup Van, Police Car UK, Police Car US, Ship, Speedboat, Trailer, Train, Trawler, Van, Yacht</p>

**SCC Lists**

<p><b>SCC List Name</b></p>	<p><b>Items</b></p>
<p>No Code Lists</p>	



Annexe IV – Illustration de l'utilisation d'une matrice bayésienne d'analyse d'hypothèses concurrentes

	p(En)
E1	0.8
E2	0.8
E3	0.95
E4	0.99
E5	0.99
E6	0.9
E7	0.6

E1 : Recherches sur les lieux (personnes ou véhicules)
E2 : Interprétation de l'origine des lésions superficielles (comparaisons)
E3 : Causes de la mort (autopsie)
E4 : Analyses toxicologiques (recherche de sédatifs)
E5 : Analyses ADN
E6 : Analyses de poils
E7 : Analyses rétroactives (sur 5 ans)

	p initiale
H1 : Intervention humaine	0.166666667
H2 : Auto-mutilation	0.166666667
H3 : Inter-mutilation	0.166666667
H4 : Mutilation accidentelle	0.166666667
H5 : Mort naturelle avec passage de carnivores	0.166666667
H6 : Fraude à l'assurance & imitation	0.166666667

p(r En,X)	H1	H2	H3	H4	H5	H6	p(En)
E1	0.4	0.00008	0.0008	0.008	0.792	0.4	0.8
E2	0.4	0.00008	0.0008	0.0008	0.792	0.4	0.8
E3	0.00095	0.000095	0.00095	0.00095	0.95	0.00095	0.95
E4	0.198	0.99	0.99	0.99	0.99	0.198	0.99
E5	0.0099	0.0099	0.0099	0.0099	0.99	0.0099	0.99
E6	0.009	0.009	0.009	0.009	0.9	0.009	0.9
E7	0.3	0.006	0.06	0.12	0.3	0.3	0.6

p(r En,xx)	xH1	xH2	xH3	xH4	xH5	xH6	p(En)
E1	0.64	0.8	0.8	0.8	0.8	0.64	0.8
E2	0.72	0.8	0.8	0.8	0.008	0.72	0.8
E3	0.95	0.95	0.95	0.95	0.00095	0.95	0.95
E4	0.99	0.0099	0.0099	0.0099	0.0099	0.99	0.99
E5	0.891	0.891	0.891	0.891	0.00099	0.891	0.99
E6	0.81	0.81	0.81	0.81	0.0009	0.81	0.9
E7	0.6	0.6	0.6	0.6	0.6	0.6	0.6

LR	xH1	xH2	xH3	xH4	xH5	xH6
E1	0.6250	0.0001	0.0010	0.0100	0.9900	0.6250
E2	0.5556	0.0001	0.0010	0.0010	99.0000	0.5556
E3	0.0010	0.0001	0.0010	0.0010	1'000.0000	0.0010
E4	0.2000	100.0000	100.0000	100.0000	100.0000	0.2000
E5	0.0111	0.0111	0.0111	0.0111	1'000.0000	0.0111
E6	0.0111	0.0111	0.0111	0.0111	1'000.0000	0.0111
E7	0.5000	0.0100	0.1000	0.2000	0.5000	0.5000

p(LR)	xH1	xH2	xH3	xH4	xH5	xH6	Ecart-type
E1	0.5000	0.0001	0.0008	0.0080	0.7920	0.5000	0.3426
E2	0.4444	0.0001	0.0008	0.0008	79.2000	0.4444	32.2613
E3	0.0010	0.0001	0.0010	0.0010	950.0000	0.0010	387.8356
E4	0.1980	99.0000	99.0000	99.0000	99.0000	0.1980	51.0211
E5	0.0110	0.0110	0.0110	0.0110	990.0000	0.0110	404.1613
E6	0.0100	0.0100	0.0100	0.0100	900.0000	0.0100	367.4194
E7	0.3000	0.0060	0.0600	0.1200	0.3000	0.3000	0.1353

	xH1	xH2	xH3	xH4	xH5	xH6
p(LR)	0.166666667	0.166666667	0.166666667	0.166666667	0.166666667	0.166666667
E1	0.111111111	1.99996E-05	0.00019996	0.001996008	0.165275459	0.111111111
E2	0.181377563	5.13213E-09	5.13358E-07	5.14807E-06	0.986468793	0.181377563
E3	0.000155285	3.80375E-13	3.80482E-10	3.81558E-09	0.999632398	0.000155285
E4	3.10625E-05	3.80397E-11	3.80504E-08	3.81579E-07	0.999996893	3.10625E-05
E5	3.45129E-07	4.22638E-13	4.22757E-10	4.23952E-09	0.999999937	3.45129E-07
E6	3.83477E-09	4.69598E-15	4.6973E-12	4.71058E-11	0.999999999	3.83477E-09
E7	1.91739E-09	4.69598E-17	4.6973E-13	9.42115E-12	0.999999985	1.91739E-09
	<b>1.91739E-09</b>	<b>4.69598E-17</b>	<b>4.6973E-13</b>	<b>9.42115E-12</b>	<b>0.999999985</b>	<b>1.91739E-09</b>