Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie = Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 24 (2006)

Artikel: Les outils informatisés du renseignement criminel

Autor: Ribaux, Olivier

DOI: https://doi.org/10.5169/seals-1051076

Olivier Ribaux

Les outils informatisés du renseignement criminel

Résumé
Le renseignement criminel et le renseignement de sécurité prennent une place toujours plus centrale dans l'organisation des agences de sécurité. L'information est rassemblée, structurée, rapidement mise à disposition et analysée dans le but de saisir en temps réel des problèmes de sécurité et d'en supposer les causes. Des stratégies efficientes sont ensuite élaborées sur la base de ces connaissances dans le but de conserver la maîtrise de ces risques pour la société. Dans ce mouvement, les nouvelles technologies d'information et de communication sont évidemment en question. Leur appréhension est faussée essentiellement par une activité commerciale frénétique qui entretien un flou conceptuel autour de leur rôle et leur potentiel précis dans les processus de renseignement. En proposant de simples visualisations ou la possibilité d'extraire automatiquement des connaissances à partir de grandes quantités d'informations, l'informatique semble passer d'un accessoire qui assiste des analystes à une machine qui se charge elle-même de détecter des menaces pour la sécurité publique.
Il est essentiel de mieux définir ces processus de renseignement et leurs outils informatisés associés afin de déterminer la distribution optimale des tâches entre des analystes et des ordinateurs qui favorise la résolution globale des problèmes. La maîtrise de ces instruments est également indispensable pour protéger des citoyens qui ne sont pas en cause contre des effets de bord indésirables qui mettent en danger leur sphère privée et leur tranquillité. La réalisation de ces objectifs nécessite une activité soutenue de formalisation. Il en résultera des modèles qui intégreront des connaissances provenant de plusieurs disciplines. Ils devront être testés dans des situations pratiques au travers de séries d'expériences afin d'en comprendre les effets possibles et d'indiquer leur efficience potentielle. Un véritable défi pour les sciences criminelles.

Informatik als Werkzeug der Verbrechensbekämpfung
Kriminalitäts- und Sicherheitsinformationen nehmen einen immer zentraleren Platz in der Organisation der Sicherheitsfirmen ein. Die Information wird gesammelt, strukturiert, schnell zur Verfügung gestellt und analysiert mit dem Ziel, die Sicherheitsprobleme und ihre Ursachen in Echtzeit zu erfassen. Auf der Grundlage dieser Erkenntnisse werden dann effiziente Strategien ausgearbeitet in der Absicht, die Kontrolle über die gesellschaftlichen Risiken zu behalten. In diesem Rahmen spielen die neuen Informations- und Kommunikationstechnologien offensichtlich eine zentrale Rolle. Das Verständnis dafür wird stark verfälscht durch frenetische kom-

merzielle Aktivitäten, die eine begriffliche Unschärfe hinsichtlich ihrer Rolle und ihres spezifischen Potentiales im Rahmen der Datenerhebung nährt. Indem einfache Visualisierungen oder Möglichkeiten vorgeschlagen werden, automatisch Erkenntnisse aus grosse Datenmengen zu ziehen, scheint sich die Informatik von einem Werkzeug, das den Analytiker unterstützt zu einer Maschine zu wandeln, die eigenständig Bedrohungen der öffentlichen Sicherheit entdeckt.
Um eine optimale Aufgabenteilung zwischen Analytiker und Computer sicherzustellen, die eine umfassende Problemlösung fördert, erscheint es von zentraler Bedeutung, den Informationsprozess und die Informatikwerkzeuge besser zu definieren. Um zu verhindern, dass als unerwünschter Nebeneffekt unbeteiligte Dritte in ihrer Privatsphäre tangiert werden, ist sodann die genaue Kenntnis dieser Werkzeuge unerlässlich. Die Verwirklichung dieser Ziele bedingt eine zunehmende und andauernde Formalisierung. Daraus werden sich Modelle ergeben, die Erkenntnisse aus verschiedenen Disziplinen integrieren. Sie müssen in der Praxis getestet werden, um die möglichen Folgen zu verstehen und um ihr Potential zu eruieren. Eine wahrhaftige Herausforderung für die Kriminalwissenschaften.

1 Introduction

Un phénomène de cambriolages dans des villas perdure depuis plus de trois ans dans une ville de Suisse. Les vols par effraction ont lieu durant la soirée, d'octobre à décembre, pendant une période et aux heures durant lesquelles il est facile pour les cambrioleurs de détecter des signes de présence (ou d'absence) d'occupants dans les habitations à cause de la nuit qui tombe plus tôt à cette saison. La police utilise tous les moyens à sa disposition pour mettre un terme à ces forfaits, de la surveillance discrète des quartiers touchés aux messages préventifs à la population. Jusqu'au déclic. En visualisant tous ces cas au moyen d'un système d'information géographique (SIG), un analyste découvre qu'un quartier d'habitations n'a jamais été touché durant la période considérée.

Une enquête est enclenchée et conduit rapidement à confondre pour une grande quantité de ces cas un cambrioleur récidiviste qui habitait au milieu de ce quartier. Le système d'information géographique a sans aucun doute joué un rôle important dans ce résultat. Sans ce moyen de visualiser les informations, le quartier d'intérêt

n'aurait certainement pas pu être identifié. Mais il garde un statut d'outil qui se contente de mettre en valeur des jeux de données.

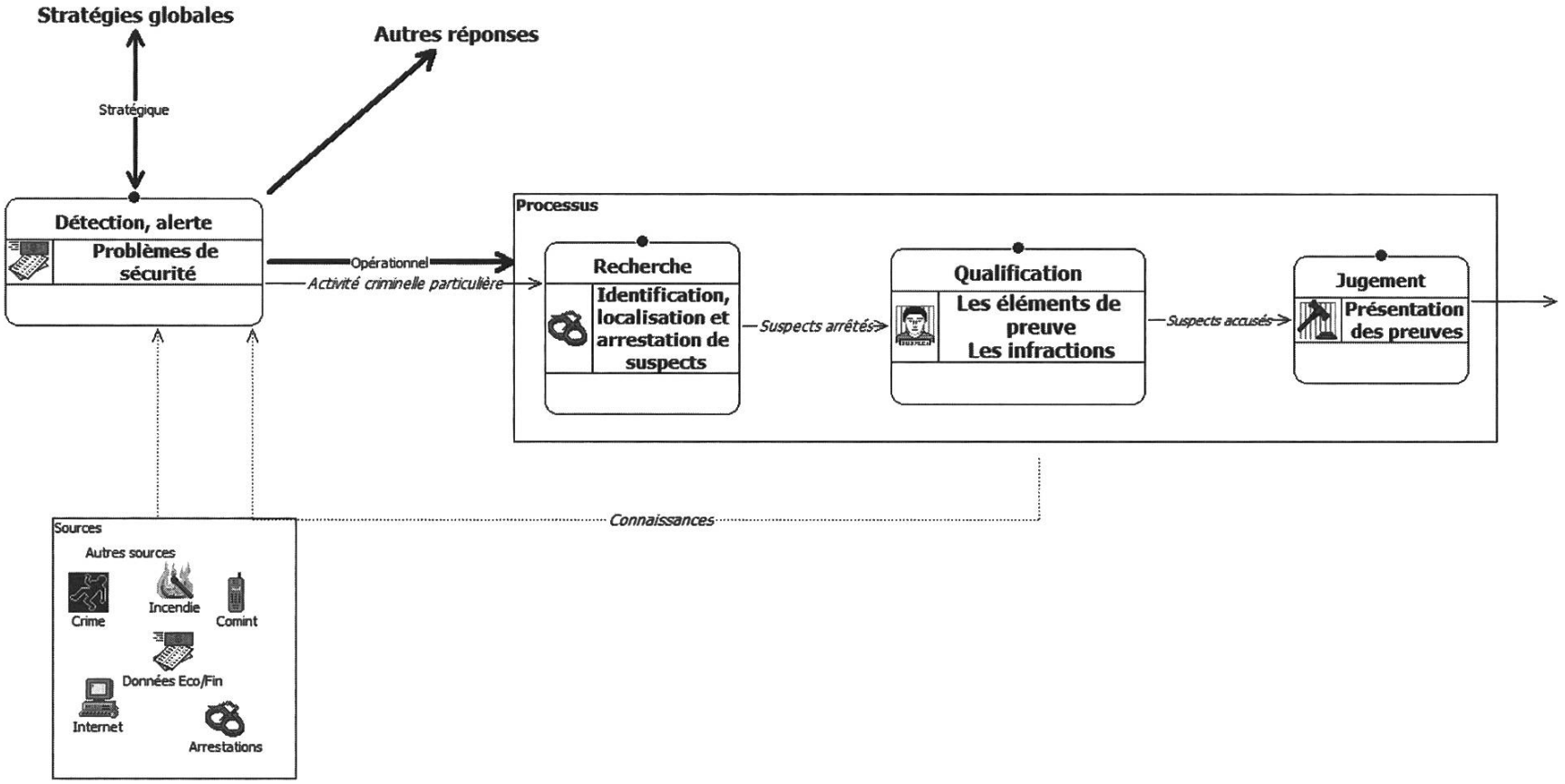
Dans cet exemple, l'analyste a raisonné sur des faits ou informations: une sélection de cambriolages d'habitations extraite des données policières. Sur cette base, il a énoncé une hypothèse qui a indiqué la piste à suivre aux enquêteurs: l'auteur habite éventuellement dans ce quartier. Cette démarche globalement inductive[1] qui va au-delà des faits pour aboutir au renseignement s'appelle l'analyse. Les Services de Renseignement Criminel du Québec insistent sur l'utilisation généralisée de ce mécanisme en en faisant leur slogan: «pour que l'information devienne renseignement».

La communauté européenne incite les Etats membres à renforcer leurs structures de traitement des informations et d'analyse. Ainsi, la recommandation Rec(2001)11 du Comité des Ministres aux Etats membres concernant des principes directeurs pour la lutte contre le crime organisé énonce le principe no 20: «Les Etats membres devraient élaborer de nouvelles méthodes de travail de la police privilégiant l'anticipation par rapport à la réaction et comprenant l'exploitation de renseignements stratégiques et le recours à l'analyse criminelle». Ces idées sont intégrées dans les nouveaux modèles policiers tels que le *National Intelligence Model* de Grande-Bretagne (NCIS 2000; JOHN, MAGUIRE 2003): les décisions stratégiques et opérationnelles doivent systématiquement découler du renseignement, à tous les niveaux.

Dans ce mouvement, le traitement structuré des données au moyen d'outils informatisés est complété d'une capacité d'interpréter les informations en restituant à l'être humain une position centrale de «travailleur du savoir» (knowledge worker).

1 Il est fréquent de parler d'induction en analyse criminelle, par opposition à la déduction, pour exprimer l'idée d'une démarche qui va au-delà des informations accessibles en faisant appel à une variété de formes de connaissances. Il s'agit d'une manière très simplifiée de décrire cette activité inférentielle qui reste encore peu étudiée (RIBAUX, MARGOT 1999; RIBAUX, MARGOT 2003; RIBAUX et al. 2006).

Figure 1 l'analyse criminelle peut poursuivre plusieurs objectifs de nature opérationnelle ou stratégique qui sont résumés dans cette figure.



Cette dualité constitue le thème de cet article. La variété des connaissances produites par des analystes est présentée à un niveau très général pour former un cadre dans lequel les enjeux principaux et les possibilités d'automatisation des processus de détection et d'analyse de problèmes de sécurité sont ensuite envisagés. Finalement, l'exemple d'un système en développement qui porte sur la «fraude à l'avance de frais» (advance fee fraud) illustre une série de difficultés récurrentes et incite à aborder de tels projets au moyen d'une démarche pluridisciplinaire.

Les formes d'analyses

Une profession résulte du développement du renseignement criminel: des «analystes» interviennent partout en Europe depuis quelques années, à différents niveaux, en tant que nouveaux partenaires des policiers ou des magistrats.

Leur analyse criminelle des informations poursuit différents objectifs dans le cadre du processus suivant (figure 1).

Les quatre phases de cette séquence peuvent être illustrées au moyen d'une situation pratique traitée par la structure policière appelée CICOP (Concept Intercantonal de Coordination Opérationnelle et Préventive), qui rassemble et analyse toutes les données sur les délits sériels en Suisse romande.

1. le CICOP assure un suivi systématique du phénomène des vols d'autoradios dans les voitures. Durant une période particulière, il est constaté qu'une grande quantité de cas sont perpétrés dans des quartiers bien délimités de deux villes, à des heures inhabituelles pour ce genre de délits (la journée plutôt que la nuit). En se basant sur l'hypothèse que ces anomalies indiquent une activité particulière d'un nombre restreint de voleurs, ces cas sont extraits de l'ensemble du jeu de données.

Le processus de détection, par un balayage et une classification systématique des vols dans les véhicules, a conduit à détecter une activité particulière dans les informations analysées. A partir de ces constatations, il est décidé d'augmenter la priorité de lutte contre ce phénomène

2. le jeu de données qui couvre le phénomène d'intérêt est ensuite analysé. Il est possible d'en dégager un schéma: les auteurs semblent agir le matin dans une des villes et le même après-midi dans l'autre. Un dispositif opérationnel est organisé par les polices des deux régions. Ces mesures débouchent sur l'arrestation en flagrant délit de deux ressortissants provenant d'un pays de l'est de l'Europe. La finalité de l'analyse est ici clairement de localiser et d'arrêter les suspects. La qualification pénale des délits et la délimitation exacte de la série ne sont pas au centre d'intérêt. L'influence de quelques cas sur l'analyse statistique est négligeable

3. une fois les suspects appréhendés, les éléments de preuve doivent être rassemblés et les infractions qualifiées. La première délimitation des délits effectuée dans la phase antérieure peut servir de base de travail, mais chaque cas est examiné minutieusement en fonction des éléments de preuve accessibles

4. les éléments de preuve sont présentés de manière à favoriser l'appréhension du dossier.

La première phase du processus regroupe toutes les démarches d'identification de problèmes de sécurité au sens large (désordres récurrents, délimitation d'un phénomène criminel ou d'une organisation criminelle, menaces, vulnérabilités, événements particuliers, etc.). Cette étape vise essentiellement l'anticipation et procède par exemple par une variété de formes de surveillances, le balayage systématique des informations accessibles ou des démarches spécifiques de recherche de renseignements. Les possibilités de réponse aux problèmes délimités sont généralement multiples, répressives ou pré-

ventives. En particulier dès qu'une activité criminelle spécifique est découverte, une démarche judiciaire est enclenchée. Elle vise d'abord à délimiter le cercle des suspects, à les identifier, à les localiser, puis à les arrêter. Un travail de qualification des délits est ensuite entamé avant de renvoyer le suspect pour son jugement.

Chaque étape procède par ses mécanismes propres, mais elle sera d'autant facilitée que les données auront été préparées dans les phases antérieures. Par exemple:

- les possibilités de destructions de preuves par le suspect seront envisagées dans la préparation d'une opération d'arrestation
- lorsqu'un cas grave se présente, il s'agit rapidement d'établir la réalité du crime, puis d'identifier, de localiser et d'arrêter les auteurs; les premiers contrôles consistent à évaluer si le crime peut entretenir des relations avec d'autres infractions, ce qui nécessite de se référer à une vue d'ensemble des crimes antérieurs potentiellement liés
- lorsqu'un suspect est arrêté en flagrant délit, les connaissances générales accumulées dans les phases préalables s'avèrent indispensables pour cerner immédiatement l'activité globale du ou des malfaiteur(s).

En résumé, un changement d'attitude s'opère un fois le suspect arrêté. L'enquête consiste alors à traiter les informations pour aboutir à la qualification d'infractions. La démarche d'abord globalement inductive devient essentiellement déductive (KIND 1994). Les façons de traiter les informations sont fortement dépendantes de cette variété des mécanismes de raisonnement qui poursuivent des objectifs différents. Le rôle des différents contributeurs (policiers, magistrats, analystes) peut varier en fonction de l'organisation policière et judiciaire, mais le principe général reste le même.

Le rôle de l'informatique

Ce renversement explique pourquoi les bases de données policières qui supportent l'analyse dans les phases antérieures du processus doivent s'abstraire d'un système de classification basé sur les codes pénaux. Les informations y sont plutôt séparées par un découpage plus pertinent en une variété de «situations criminelles». Par exemple, dans les phases de détection, les lésions corporelles couvrent beaucoup trop de situations différentes; il est préférable de porter l'attention sur les circonstances dans lesquelles l'action s'est déroulée et sa nature (racket, bagarre de rue, hold-up, etc.). Un tel regroupement des événements favorise la détection de crimes en séries car les possibilités de rencontre entre des auteurs motivés et des cibles attrayantes en l'absence de gardiens qui décrivent ces situations sont très spécifiques (FELSON, CLARKE 1998).

L'exploitation des données ainsi colligées consiste essentiellement à développer et gérer des hypothèses, comme dans l'exemple initial des séries de cambriolages: à partir des constatations effectuées sur la représentation spatiale des délits, développer l'hypothèse que l'auteur réside dans le quartier qui n'a jamais été touché. Comment l'informatique peut accompagner ce genre de raisonnement? Pour simplifier, ce support peut prendre trois formes:

1. simple visualisation des informations (par exemple au moyen d'un système d'information géographique)
2. favorise les recherches, la navigation et l'exploration de ces informations
3. propose des hypothèses sur la base de régularités ou de structures automatiquement détectées dans un jeu de données.

Dans les deux premières situations, c'est l'utilisateur du système qui est actif. L'ordinateur se contente de répondre à ses sollicitations dans l'enchaînement de ses raisonnements. Dans la troisième situation, l'ordinateur suggère à l'utilisateur de s'intéresser à un jeu de

données particulier: il a alors un rôle actif de procéder à une sorte de recommandation sur des voies possibles de raisonnements.

Techniques de visualisation

Des formes de visualisation couramment utilisées en analyse criminelle comprennent:

1. les schémas relationnels
   de tels schémas mettent en relation les différentes entités d'une affaire, comme des véhicules, des personnes, des comptes bancaires, etc. Ils offrent ainsi une vue d'ensemble des liens qui sont connus (figure 2).

2. les schémas de flux
   sont particulièrement appropriés lorsque la séquence temporelle de transactions de tous genres est analysée, comme une série de transferts d'argent sur des comptes susceptible d'indiquer une activité de blanchiment (figure 3).

3. les cartes de géographie
   la dimension spatiale est souvent cruciale. L'utilisation de systèmes d'information géographique devient alors indispensable, comme dans l'exemple cité en introduction.

La recherche et la compréhension des relations entre des entités, ainsi que l'analyse des séquences temporelles et de la distribution spatiale d'événements constituent des démarches de base de l'enquête judiciaire. Cette constatation explique le succès que rencontrent certains logiciels qui aident à visualiser les informations selon ces dimensions élémentaires. L'analyste peut aussi imaginer des combinaisons de plusieurs solutions: par exemple, l'affichage de points en séquence sur une carte de géographie souligne des déplacements ou des chronologies d'événements.

Figure 2: Exemple de schéma relationnel, parfois aussi appelé schéma de liaisons. Les entités et relations pertinentes dans le cadre du problème traité sont identifiées et représentées dans un tel schéma.

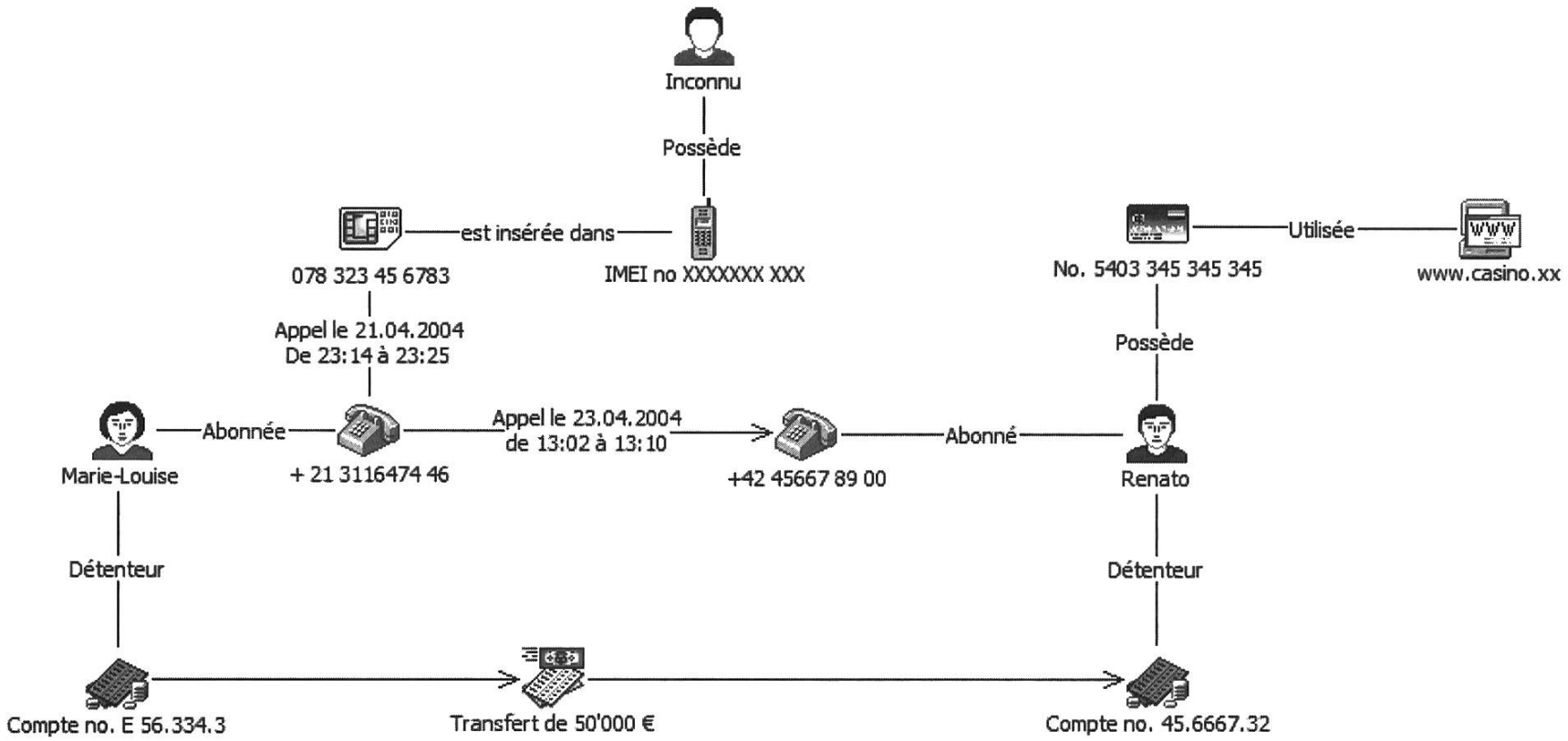
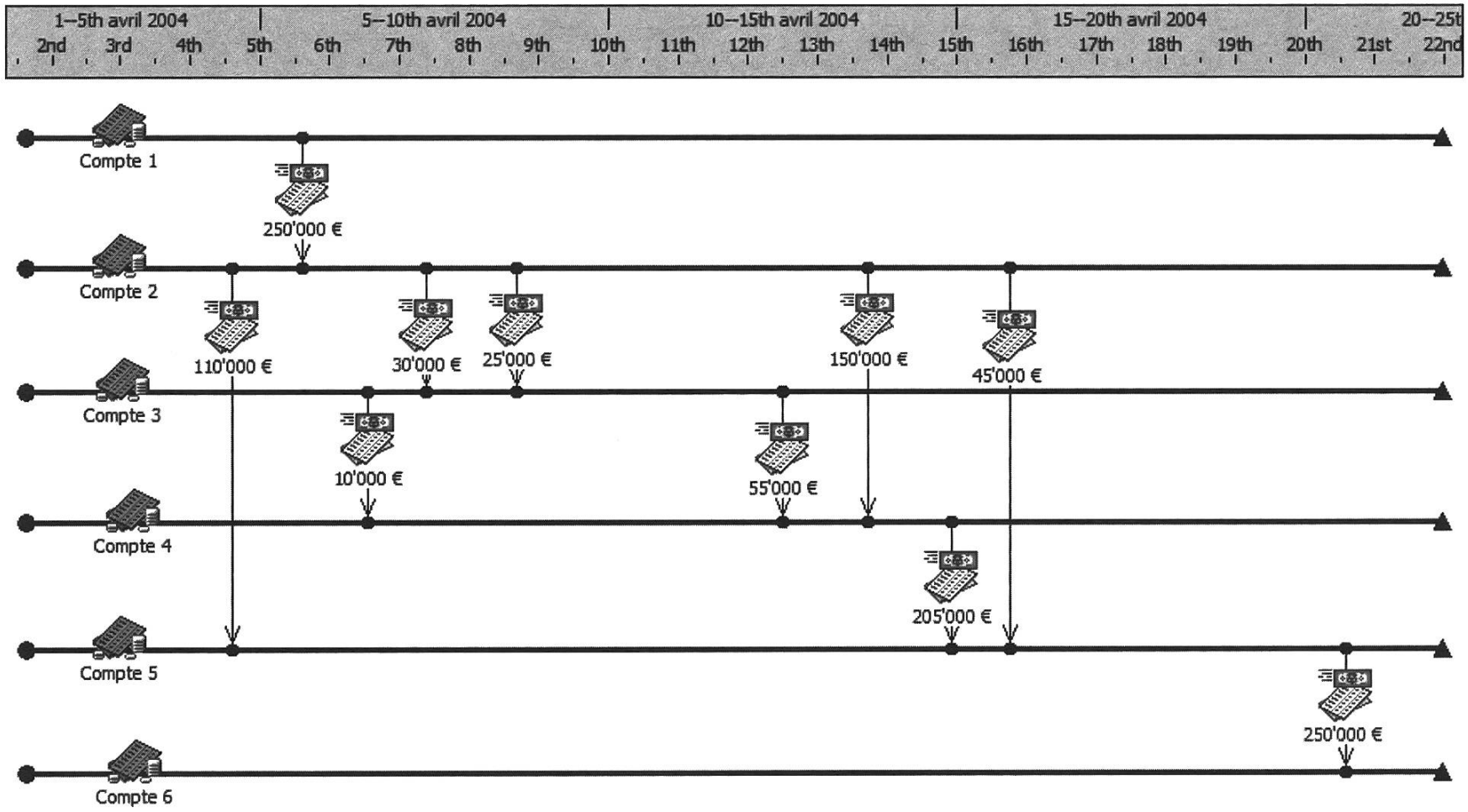


Figure 3: Exemple d'un schéma de flux qui représente des transferts d'argent entre des comptes bancaires. Ce genre de représentation fait apparaître le rythme des transactions et les montants en jeu. Ils sont particulièrement appropriés pour représenter la séquence de toutes formes de transaction.

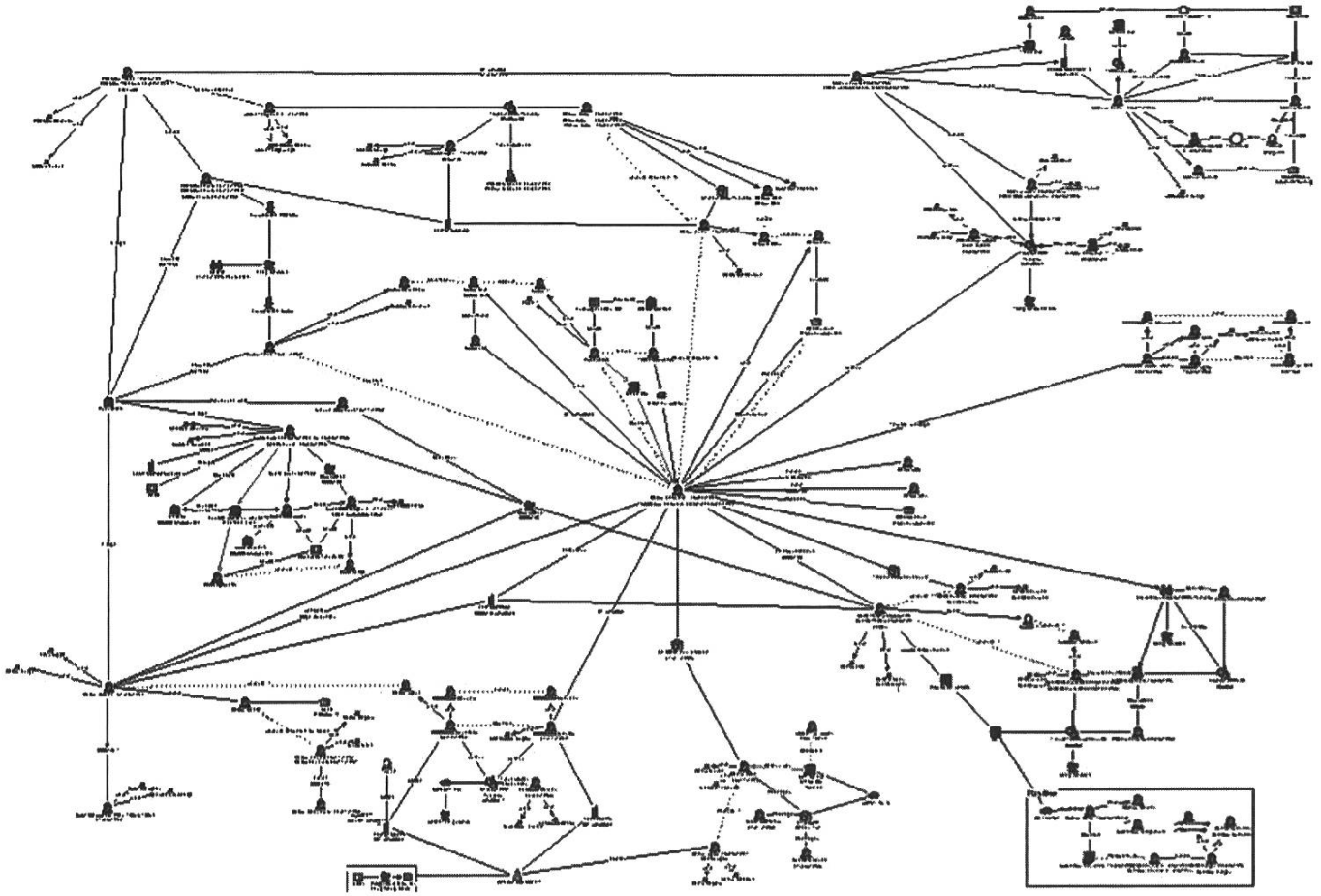


Ces diagrammes renferment parfois des pièges. Une visualisation est par définition une représentation, donc une simplification. Ce schéma médiocre (figure 4) pourrait laisser penser que le personnage central est un protagoniste important de l'affaire. En fait, il désigne surtout un individu sur lequel beaucoup d'information sont disponibles, indépendamment du rôle joué. En fonction de la nature de l'affaire, ce schéma pourrait au contraire suggérer de porter les efforts sur un recueil supplémentaire d'informations qui concerne d'autres individus qui apparaissent plus discrètement en périphérie.

Des systèmes hétérogènes

Les outils informatisés du renseignement criminel sont rarement homogènes. Un système géographique développé par un constructeur ne se connecte pas forcément aisément avec une base de données vendue par un autre fabricant de logiciels. De manière générale, une suite d'opérations compliquées est généralement nécessaire pour basculer des différents outils de visualisation vers la base de données ou vice-versa. Ces difficultés freinent considérablement les analyses. Des connaissances techniques approfondies, souvent très spécifiques, sont indispensables pour utiliser les moyens de transferts que chaque logiciel propose. De même, la base de données devrait être structurée de manière à répondre aux sollicitations de l'analyste lorsqu'il raisonne. Les mécanismes de raisonnement sont malheureusement peu étudiés et mal explicités. En conséquence, les architectures des bases de données n'autorisent pas une navigation naturelle et provoquent ainsi des ruptures dans l'enchaînement des raisonnements. Ces interruptions reportent l'attention sur l'informatique ou la base de données, plutôt que sur l'analyse et le problème traité lui-même.

Figure 4: Ce schéma relationnel d'une affaire complexe de trafic de stupéfiant met en évidence un personnage central. L'allure générale de cette représentation laisse supposer que l'individu en question joue un rôle important. En fait, il s'agit surtout d'un individu sur lequel beaucoup d'informations sont disponibles sans spécification de leur nature. Cet exemple met en évidence les risques liés à l'interprétation mal maîtrisée des schémas communiqués.



Les processus de détection (d'alerte)

Les processus de détection méritent une attention particulière. Ils ont tous le même rôle de balayer systématiquement certains types d'informations, afin de détecter des signes qui peuvent alerter sur l'existence potentielle de problèmes de sécurité de tous genres. Les nouvelles technologies d'information et de communication ont amplifié les possibilités de les mettre en œuvre. Les instruments développés servent par exemple à surveiller des communications sur Internet, écouter des conversations téléphonique, suivre des crimes et délits sériels, lire automatiquement des numéros de plaques minéralogiques et simultanément les confronter avec les bases de données des véhicules signalés ou contrôler l'identité de personnes.

Si ces mécanismes sont connus depuis longtemps, les innovations technologiques ont radicalement transformé l'intensité avec laquelle ils sont appliqués. Par exemple, la rapide installation de systèmes biométriques change radicalement le nombre et la nature des contrôles d'identité des personnes.

La vie privée est menacée par la prolifération de ces nouveaux moyens. En effet, par définition, ce qu'on cherche n'est pas toujours connu *a priori.* Il s'agit de détecter des signes qui indiquent que *quelque chose* met particulièrement en danger la sécurité publique. Le *quelque chose* n'est pas facile à définir et souvent laissé à l'appréciation individuelle comme un certain nombre d'expériences malheureuses l'ont montré. Des données ne relevant pas de la criminalité sont traitées, comme des discussions anodines dans des forums de discussion sur Internet ou des désordres constatés par les forces policières. Le défi consiste donc à formaliser clairement ces processus et procéder aux analyses dans un cadre bien défini, avec une éthique irréprochable, des objectifs clairs et sans priver les agences de sécurité de moyens modernes de détection.

Une description générale de ces processus initialise ces efforts de formalisation (figure 5). Les nouvelles informations recueillies sont accueillies dans un ensemble de renseignements de base déjà organisés. L'analyse de cette mémoire favorise ensuite la détection de problèmes ou d'activités criminelles particulières.

Ce mécanisme de construction par assemblage de petites pièces d'informations apparaît dans le schéma suivant (figure 6). Il synthétise la composition de petits groupes d'auteurs qui opéraient dans le cadre de séries de vols à l'astuce très spécifiques au préjudice de personnes âgées. Le rassemblement patient de ces informations sur une période relativement longue (de l'ordre de 6 mois) montre clairement l'existence d'une bande éventuellement organisée d'auteurs. Cette constatation servira à délimiter l'ampleur du phénomène, à élaborer des mesures préventives ciblées, à procéder à des arrestations et éventuellement à communiquer rapidement à un magistrat la vue d'ensemble de ce phénomène de criminalité susceptible de l'aider à prendre des décisions.

C'est aussi dans le cadre de ces processus que l'intérêt des méthodes d'extraction de connaissances apparaît le plus clairement: un programme informatique fouille les données à la recherche de jeu d'informations présentant des structures (corrélations, régularités, événements types prédéfinis, etc.) qui méritent une attention particulière. Par exemple, un tel système peut alerter l'analyste d'une régularité dans le rythme des transferts de certains montants entre plusieurs comptes bancaires. La caractéristique clé de ces méthodes est la qualité ou l'utilité des hypothèses qu'elles sont capables d'énoncer: les structures trouvées par ces programmes sont souvent détectables facilement par des moyens de navigation ou de visualisation simples et lorsque des résultats sont obtenus, ceux-ci ne désignent pas forcément des activités qui méritent un intérêt particulier. En particulier, la détection de «points chauds» (endroits particulièrement touché par certains types de criminalité durant une période donnée) est difficile à automatiser, mais souvent aisée au moyen d'un système de

Figure 5: Une modélisation des processus de détection qui procède par le recueil de l'information, son intégration dans un ensemble de renseignements de base. L'analyse de cette mémoire, qui est construite de manière itérative, permet de détecter des problèmes de sécurité.

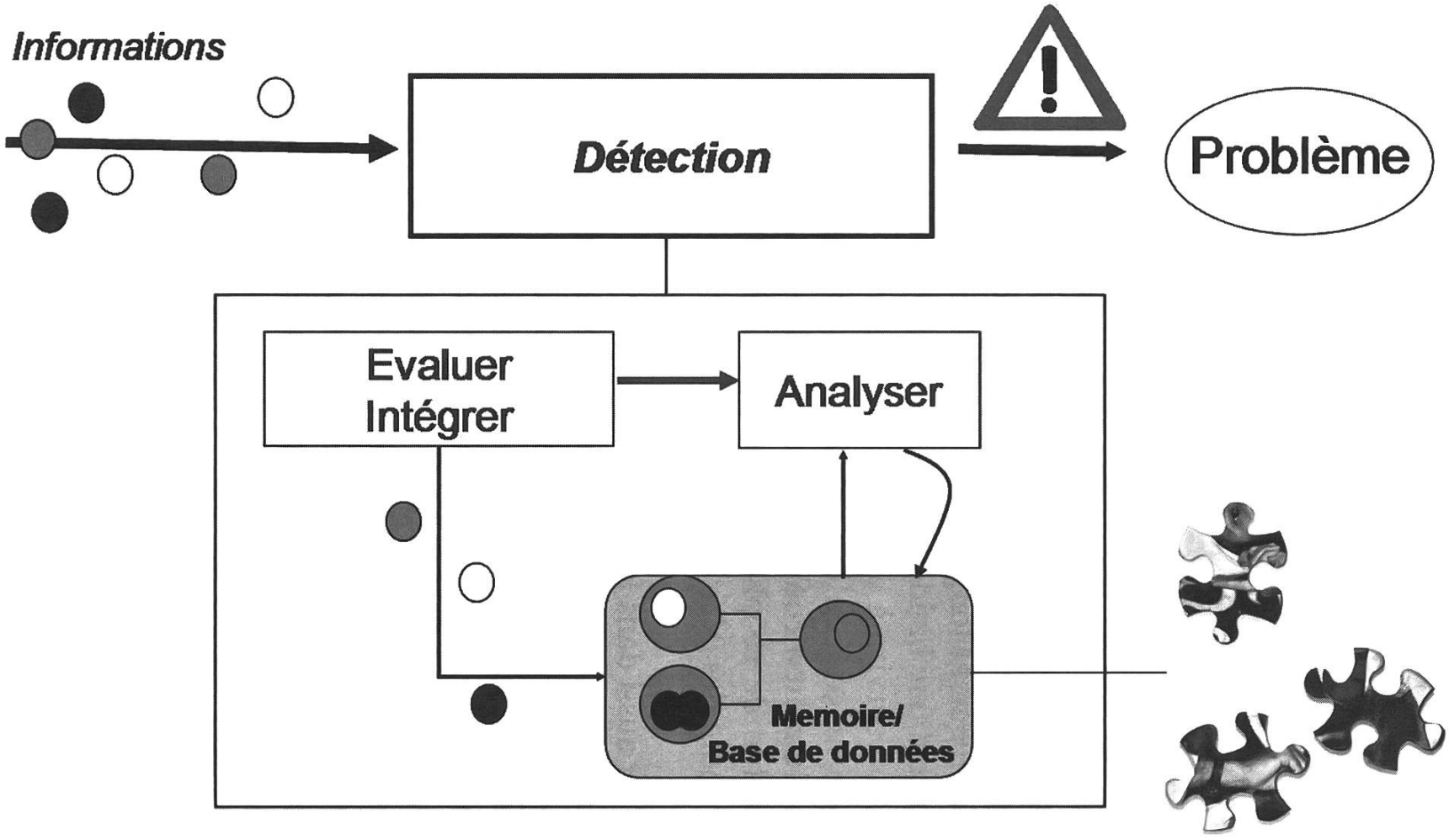
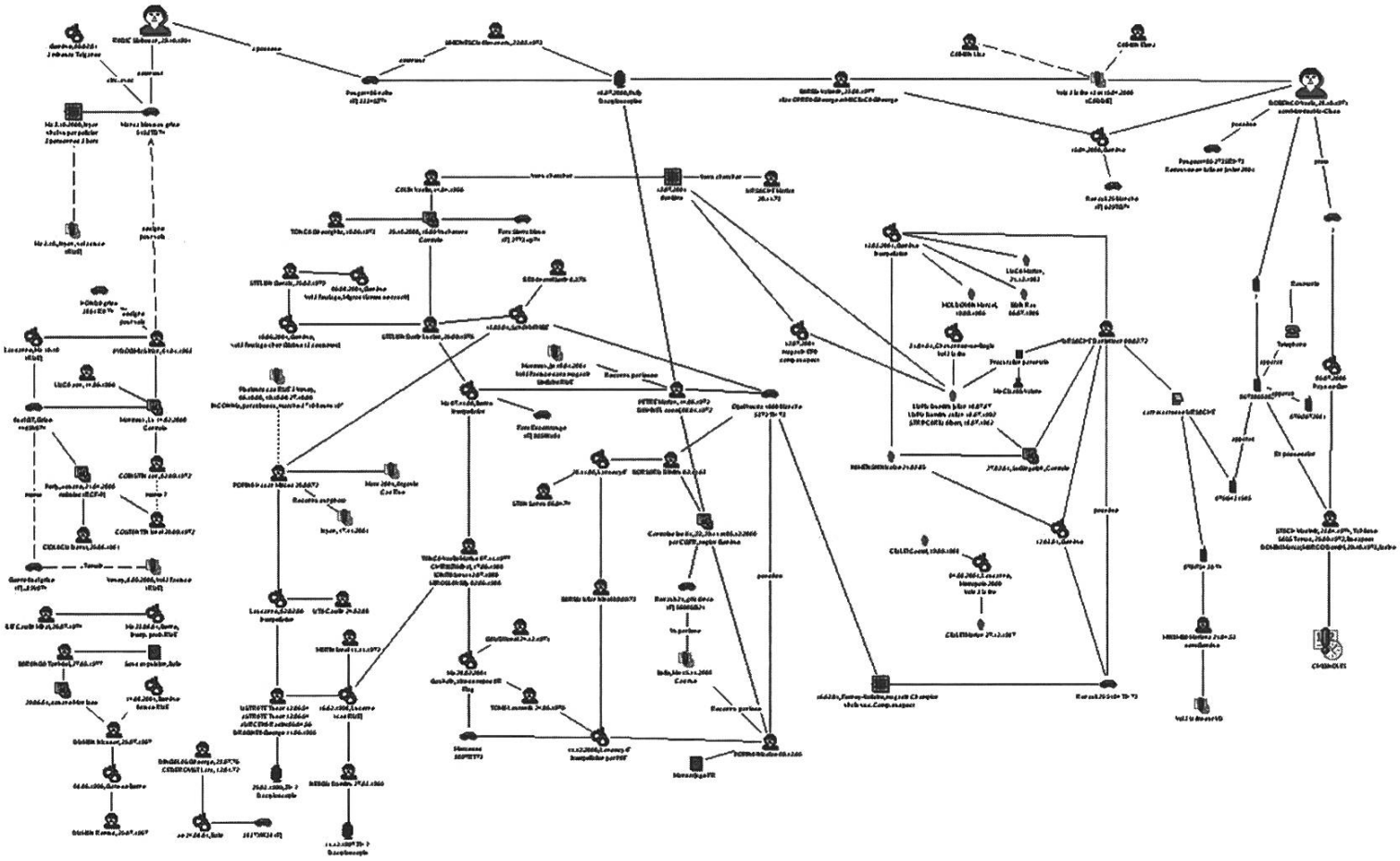


Figure 6: Exemple d'un schéma relationnel constitué de petites pièces d'informations sur de la délinquance dont le traitement n'est souvent pas jugé prioritaire (vols à la tire). L'association d'auteurs qui présentent le même profil et qui commettent des délits dans des situations semblables très spécifiques laisse supposer une activité en bande de ces auteurs. De telles analyses par assemblages sont primordiales pour détecter des phénomènes de criminalité présentant des formes d'organisation.



navigation performant. Cela explique certainement le contraste entre la prolifération de la littérature académique sur le sujet et l'utilisation encore très rare de ces méthodes dans la pratique policière.

Le potentiel de ces techniques, bien qu'incontestable, n'est donc pas encore bien cerné. Afin de mieux le délimiter, une série de projets très spécifiques et plus réalistes sont en cours de réalisation.[2] Ils se concentrent sur la détection automatisée de tendances (augmentations et diminutions au cours du temps), ainsi que des regroupements spatiaux extraordinaires de certaines formes de criminalité. Effectués sur toutes les dimensions connues des événements (traces physiques recueillies, modes opératoires, situations criminelles), de tels automatismes pourraient ainsi attirer l'attention des analystes sur des jeux de données limités qui reflètent des séries d'événements liés. Vu le nombre de dimensions analysées et la spécificité des situations criminelles, il serait alors bien difficile aux malfaiteurs de dissimuler leurs activités, sans laisser paraître de régularité dans les données.

L'escroquerie à l'avance de frais

Le projet d'un processus de détection complet a été proposé par un analyste[3] et est actuellement en développement.[4] Il porte sur les courriels qui polluent les boîtes aux lettres électroniques par des messages qui promettent des gains exceptionnels en échange d'une aide pour procéder à des opérations financières. Cette astuce permet aux escrocs d'établir un contact avec une victime potentielle. Leur stratégie consiste ensuite, sous différents prétextes, à faire payer des avances de frais dérisoires en regard du profit escompté.

2 Recherche soutenue par le *Fonds National Suisse de la Recherche Scientifique* No. 105211-107862, «Recognition of Patterns in Forensic Case Data: the Use of Chemical/Physical Signature of Illicit Drug Seizures in an Intelligence Perspective».

3 JULIEN CARTIER, Police cantonale vaudoise.

4 Collaboration entre la Police cantonale vaudoise, l'Ecole des Sciences Criminelles de l'Université de Lausanne et la Haute Ecole d'Ingénierie et de Gestion du Canton de Vaud.

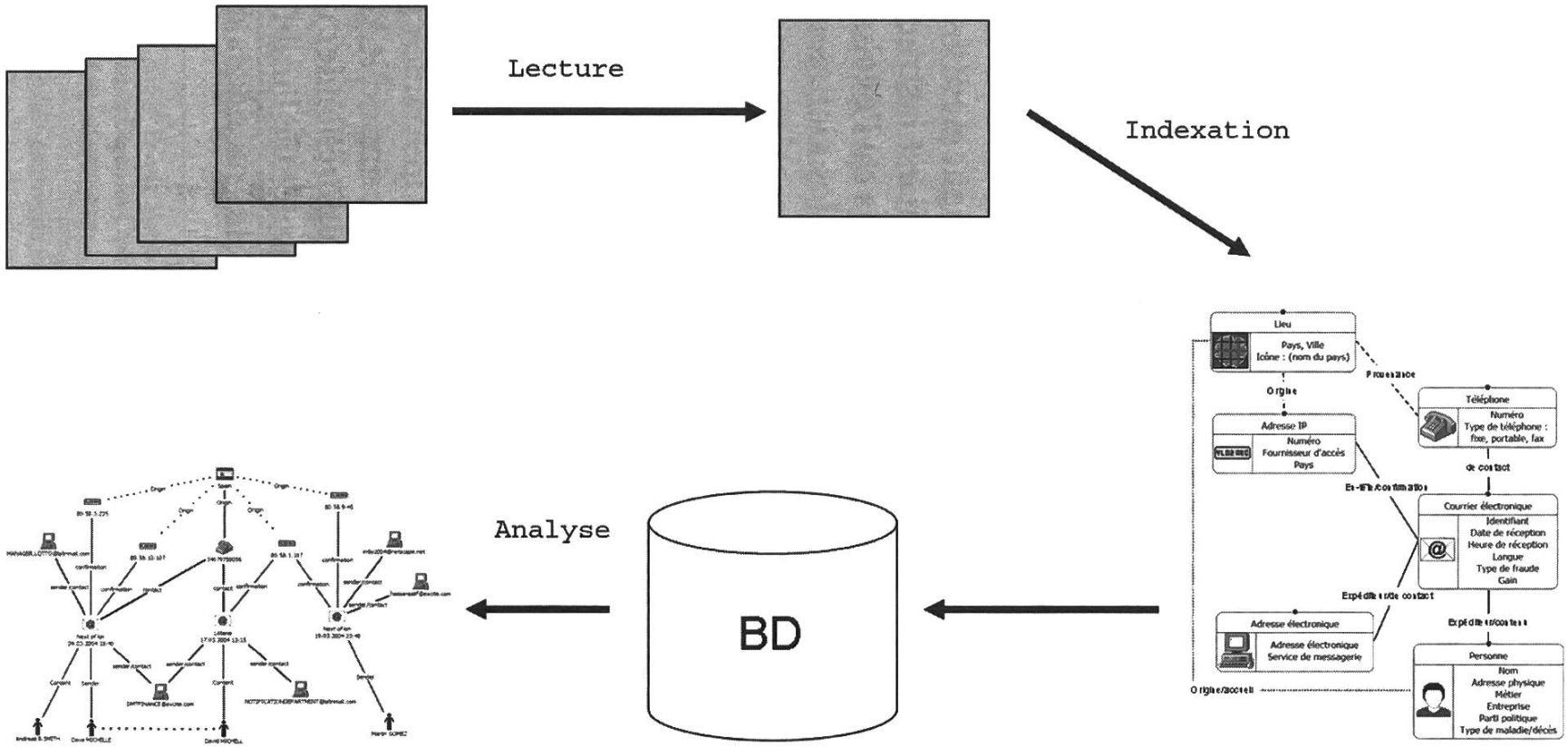
Afin de déterminer l'efficience potentielle d'un observatoire qui analyserait systématiquement ce genre de messages électroniques, deux échantillons de 200 de ces courriels ont été étudiés dans une étude préliminaire (SCHIFFER et al. 2004). Des premiers résultats prometteurs et quelques tentatives d'automatisation réussies encouragent à poursuivre ce développement.

Un tel processus (figure 7) commence par une étape d'acquisition: comment recevoir les courriels et filtrer ceux qui sont pertinents pour l'étude? Il s'agit ensuite d'indexer les messages en fonction de leur contenu: numéros de téléphones, numéros IP, adresses e-mails, etc. Une fois les données organisées et stockées dans la base, l'analyse consiste à extraire autant de renseignements stratégiques et opérationnels que possible. Par exemple, il est instructif de déterminer l'origine géographique de ces messages ou l'évolution des scénarios utilisés par les escrocs pour appâter les victimes (stratégique), ainsi que de détecter des signes qui indiqueraient une activité particulière d'une bande de malfaiteurs (opérationnel).

Ce projet est très ambitieux puisqu'il nécessite la définition d'une architecture logicielle extrêmement souple, apte à accepter les évolutions de ces formes de criminalités et des technologies utilisées. Le «phishing» est un exemple d'un phénomène criminel apparenté que le système doit être capable de traiter.

Une approche pluridisciplinaire (analyse criminelle, droit, informatique, criminologie, etc.) s'impose pour appréhender de tels processus. Elle cherchera notamment l'équilibre entre l'utilité du dispositif mis en place, son coût, sa souplesse et les menaces qu'il constitue pour la vie privée.

Figure 7: Etapes du processus de traitement des e-mails portant sur la fraude à l'avance de frais.



Contrairement à une conception répandue, le développement de tels systèmes ne constitue pas qu'un détail technique. La transcription automatique du contenu des communications par le téléphone, la traduction instantanée de conversations, la reconnaissance de personnes dans une foule, de même que la détection dans de gigantesques quantités de transactions de tout ordre de séquences d'«événements types» forcément pertinentes ne sont pas pour demain. Y croire, c'est oublier que dans les années 50, quelques chercheurs avaient prédit que, rapidement, les ordinateurs apprendraient, raisonneraient et créeraient en simulant l'esprit humain dans une gamme très large de problèmes. Les succès de l'intelligence artificielle sont finalement restés limités en fonction de ces promesses et des investissements consentis (NEWQUIST 1994; CREVIER 1997).

Conclusion

Les moyens informatisés ont amplifié les possibilités des agences de sécurité de détecter des activités qui mettent en danger la sécurité publique et de traiter les informations au profit du système judiciaire. Toutefois, il reste encore à mieux cerner la place de ces outils dans l'ensemble des organisations et de leur système d'information. Des études pluridisciplinaires sont indispensables pour délimiter le réel potentiel de ces instruments et mettre en œuvre des méthodes bien intégrées à la pratique. Ces dernières devront prouver leur efficience, mais simultanément éviter d'entraîner la société dans un système de surveillance exagéré. La démarche fondamentale de formalisation proposée fixera également de manière claire les objectifs des processus de détection et les conditions d'exploitation des données sur les personnes. Ces précautions devraient préserver les agences de sécurité d'un excès inverse qui consisterait à les priver d'instruments performants.

Références

CREVIER, D. (1997). *A la recherche de l'intelligence artificielle.* Traduction française, Flammarion, France.

FELSON, M., CLARKE, R.V. (1998). *Opportunity Makes the Thief: Practical theory for crime prevention.* Police Research Series. Research, Development and Statistics Directorate, Policing and Reducing Crime Unit, Home Office, London (98).

JOHN, T., MAGUIRE, M. (2003). *Rolling out the National Intelligence Model: Key Challenges. Crime Reduction and Problem Oriented Policing.* K. Bullock and N. Tilley. Willian, Portland: 38–68.

KIND, S. (1994). Crime investigation and the criminal trial: a three chapter paradigm of evidence. *Journal of the Forensic Science Society* 34(3): 155–164.

NCIS (2000). *The National Intelligence Model.* National Crime Intelligence Service.

NEWQUIST, H. P. (1994). *The Brain Makers: Genius, Ego and Greed in the Quest for Machines that Think.* Sams, Indianapolis.

RIBAUX, O., MARGOT, P. (1999). Inference Structures for Crime Analysis and Intelligence Using Forensic Science Data: the Example of Burglary. *Forensic Sci. Int.* 100: 193–210.

RIBAUX, O., MARGOT, P. (2003). Case-Based Reasoning in Criminal Intelligence using Forensic Case Data. *Science & Justice* 43(3): 135–143.

RIBAUX, O., S. J. WALSH, MARGOT, P. (2006). The contribution of forensic science to crime analysis and investigation: Forensic Intelligence. *Forensic Sci. Int.* 156: 171–181.

SCHIFFER, B., BIRRER, S., CARTIER, J., CAPT, S., RIBAUX O. (2004). 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* (2): 148–158.