16 Cahiers du Centre de Recherches Informatique et Droit

# DROIT DES TECHNOLOGIES DE L'INFORMATION

## REGARDS PROSPECTIFS

Sous la direction de
Étienne Montero

À l'occasion des vingt ans du C.R.I.D.



BRUYLANT
BRUXELLES
1999

# L'ANALYSE CRIMINELLE ET LA PROTECTION DE LA VIE PRIVÉE, OU LES DANGERS DE REMPLACER HERCULE POIROT PAR UN PROCESSEUR

**Béatrice HAVELANGE[*] et Bertrand RENARD[**][1]**

*« Quiconque combat les monstres doit s'assurer qu'il ne devient pas lui-même un monstre. Car, quand tu regardes au fond de l'abysse, l'abysse aussi regarde au fond de toi. »*
F. Nietzsche

## INTRODUCTION

**1.** Depuis toujours, les enquêteurs « font » de l'analyse criminelle : ils recueillent des éléments, les rassemblent, en jaugent la fiabilité, en déduisent des liens avec des affaires précédentes dont ils ont été chargés... Deux facteurs ont toutefois fait évoluer ces méthodes largement empiriques d'une manière spectaculaire. D'une part, le développement des technologies informatiques : l'ordinateur peut traiter autant de données que des équipes entières d'enquêteurs travaillant dans les endroits les plus divers, sur des dossiers en apparence les plus dissemblables. L'ordinateur n'oublie rien, n'a en principe pas *d'a priori* sur les cas qui lui sont soumis, et résiste bien à la pression que connaissent tous les policiers confrontés à une affaire délicate. L'autre élément qui est venu provoquer cette évolution, et sans doute la rendre indispensable, est la complexification des affaires criminelles elles-mêmes, imposant la recherche d'une méthode structurée et plus homogène pour traiter des quantités impressionnantes d'informations de natures diverses : que l'on pense au parcours apparemment erratique de tueurs en série ou aux montages financiers et aux filières de trafic de stupéfiants établies par la criminalité organisée. Plus les stratégies criminelles sont élaborées, plus la réponse de la force publique doit être affinée. C'est donc à la fois par opportunité et par besoin que l'analyse criminelle a pris une place éminente parmi les techniques

---

* Collaboratrice au CRID-FUNDP, Conseiller adjoint à la Commission de la vie privée.

** Juriste au Ministère de la Justice.

1 La présente contribution ne reflète que l'opinion personnelle de ses auteurs.

policières de recherche[2]. L'analyse criminelle n'a, à notre connaissance, pas fait l'objet de débats animés comme ce fut (et c'est toujours) le cas pour la recherche proactive, ou les « techniques particulières de recherche » (utilisation des informateurs, infiltration,...). Elle n'est cependant pas sans risque pour certaines libertés fondamentales, dont la protection de la vie privée.

## DÉFINITIONS

**2.** L'analyse criminelle a pour objectif de tirer le maximum de renseignements utiles d'une masse de données provenant de sources très diverses, en canalisant les opérations de recueil des informations. L'analyste vise à donner une valeur ajoutée aux informations recueillies dans le cadre d'une opération ou d'un projet en les organisant, en les interprétant et en les présentant sous forme claire et simple, de façon à aider les responsables (enquêteurs, magistrats,...) à mieux comprendre les choix possibles et à prendre une meilleure décision.

Concrètement, l'analyse criminelle n'est rien d'autre que l'emploi de méthodes structurées et de techniques normalisées, facilement adaptables aux particularités de la plupart des enquêtes et des projets, qui permet :

- de définir le résultat visé (évaluation de la demande, détermination d'objectifs réalistes) ;
- de déterminer les informations qu'il y a lieu de collecter pour atteindre ce résultat et de planifier leur stockage ;
- d'évaluer les informations collectées (qualité, exactitude des informations, relation entre les sources et les informations, fiabilité,... par l'utilisation d'un système uniforme d'évaluation) ;
- d'organiser le stockage des informations en les structurant (attribution de références croisées permettant de les retrouver rapidement) ;

---

2 Non sans critiques quant à son utilité réelle. Voir à ce sujet par exemple, F. MARTENS, , « The Intelligence Function », in *Major Issues in Organized Crime Control*, H. EDELHERTZ ed., Washington D.C., National Institute of Justice, 1987, p.134: « Intelligence is seldom more than an accumulation of often irrelevant data that serves only marginally useful purposes »... Il semble toutefois généralement accepté que ces critiques sont dépassées à l'heure actuelle.

- d'intégrer les informations stockées en les associant de façon significative (présentation des informations sous une forme qui facilite l'analyse);
- d'interpréter les informations ainsi intégrées pour parvenir enfin à formuler des hypothèses, des prévisions et des estimations.

Les hypothèses que l'analyste formule enfin sur base de cette longue démarche permettront une nouvelle orientation du travail d'enquête, le recentrant sur les informations vraiment pertinentes[3].

**3.** Le concept d'analyse criminelle a été défini de différentes manières ; le travail de définition est cependant toujours problématique car il existe différentes variétés d'analyse. La définition doit être assez large pour correspondre à ces diverses possibilités. Les premières formalisations du concept sont le fruit de réflexions menées outre-Atlantique. Ainsi, en 1976, le National Advisory Committee on Criminal Justice Standards and Goals la définit comme « the product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being or known to be, criminal in nature »[4]. Au niveau européen, un groupe d'experts proposait en 1992 un cadre conceptuel qui fut accepté par la conférence ministérielle Trevi de Lisbonne. La définition suivante fut adoptée : « l'analyse criminelle consiste en la recherche et la mise en évidence méthodiques de relations, d'une part, entre des données de criminalité elles-mêmes et, d'autre part, entre des données de criminalité et d'autres données significatives possibles, à des fins de pratiques judiciaires et policières. »[5] Cette définition est encore largement employée, même si elle est parfois remise en cause[6].

Lorsque l'analyse criminelle vise à l'obtention de résultats directement utilisables dans le cadre des activités de recherche et des poursuites, on parle d'analyse (criminelle) opérationnelle. Il s'agit donc d'un instrument d'aide à l'enquête par lequel des données concrètes du dossier sont utilisées et analysées. Lorsque l'analyse criminelle s'inscrit dans le cadre de la politique à mener, on parle d'analyse (criminelle) stratégique. Ce second type d'analyse est axé principalement sur

---

3 Voir P. GEORGE, Analyse criminelle: recherche d'une logique derrière la criminalité, *Politeia*, Janvier 1996, N°1.

4 Cité in S.R. SCHNEIDER, « The Criminal Intelligence Function : Toward a Comprehensive and Normative Model », The IALEIA Journal, Vol. 9, N°2, disponible sur www.ialeia.org/09021.shtml.

5 Organisation internationale de police criminelle Interpol, *Guide sur l'analyse criminelle («the Criminal Analysis Booklet»)*, Lyon, 1997.

6 P. GEORGE lui reproche son manque de prise en compte de l'aspect inductif de la méthode de travail, in « Operationele misdrijfanalyse. Een instrument voor doeltreffende recherche », Bureau central de recherche, Programme analyse criminelle, 1999, inédit.

l'obtention d'aperçus appuyant la direction tant au niveau de l'élaboration de la politique criminelle que de la stratégie policière[7].

**4.** Comme précisé dans la définition, il existe deux types d'analyse criminelle: l'analyse opérationnelle et l'analyse stratégique. L'une et l'autre peuvent s'exercer au départ de trois éléments : le délit, l'auteur ou la victime d'infraction, les méthodes de contrôle de la criminalité.[8]

Le tableau suivant vise à présenter de manière claire cette typologie[9].

| | **Analyse stratégique** | **Analyse opérationnelle** |
|---|---|---|
| *Délit* | Analyse de phénomène de la criminalité | • Analyse de cas<br>• Analyse comparative de cas |
| *Auteur* | Analyse de profil général | • Analyse de groupe d'auteurs (auteurs connus)<br>• Analyse de profil spécifique (auteur inconnu) |
| *Méthode* | Analyse de méthode générale | Analyse d'enquête |

Les analyses criminelles stratégiques se basent sur des informations générales (données quantitatives ou qualitatives).

- L'analyse stratégique de délit permet une analyse de phénomène de criminalité. Il s'agit d'étudier la nature, l'ampleur et le développement de la criminalité ou de certaines formes de criminalité dans une zone géographique et au cours d'une période données.
- L'analyse stratégique d'auteurs permet une analyse de profil général. Il s'agit d'essayer de déterminer les caractéristiques communes aux individus ayant commis le même type d'infraction.
- L'analyse stratégique de méthode permet une analyse de méthode générale. Il s'agit d'évaluer une méthode de répression appliquée dans plusieurs affaires en vue de définir les meilleures façons de procéder pour les affaires à venir.

---

7 Définitions données par la Commission parlementaire chargée d'enquêter sur la criminalité organisée en Belgique, Documents parlementaires, Sénat, 1998-1999, Rapport final, p. 20.

8 Organisation internationale de police criminelle Interpol, *Guide sur l'analyse criminelle*, *op.cit.*, p. 7.

9 Cité in P. GEORGE, Analyse criminelle: recherche d'une logique derrière la criminalité, *op.cit.*, p. 21.

Les analyses criminelles opérationnelles, par contre, nécessitent le recours à des données personnalisées (données à caractère personnel).

- L'analyse opérationnelle de délit permet de réaliser une analyse de cas ou une analyse comparative de cas.
    - L'analyse de cas consiste à essayer de reconstituer la genèse et le déroulement d'un incident criminel précis afin de déterminer l'enchaînement des événements et les caractéristiques des agissements/activités, en vue d'obtenir des indications sur la direction dans laquelle il conviendrait d'orienter les recherches et de déceler les incohérences parmi les informations provenant de différentes sources.
    - L'analyse comparative de cas vise à comparer les informations relatives à des délits présentant des similitudes, en vue de découvrir si certaines de ces infractions ont pu être commises et/ou organisées par le ou les mêmes individus.
- Une analyse opérationnelle d'auteurs permet soit une analyse de groupe d'auteurs (lorsque ceux-ci sont connus), soit une analyse de profil spécifique (lorsque l'auteur est inconnu).
    - L'analyse de groupe d'auteurs 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.
    - L'analyse de profil spécifique consiste à essayer d'établir le profil (de comportement) du ou des auteurs d'une infraction d'après les caractéristiques de l'affaire et d'autres informations d'ordre général.
- Une analyse opérationnelle de méthode est une analyse d'enquête. Il s'agit d'évaluer les tâches qui sont ou ont été accomplies au cours d'une enquête particulière dans le but de la faire progresser.

Cette typologie de l'analyse criminelle, présentée ici de manière quelque peu aride et synthétique, provient d'une évolution progressive. Approuvée en juin 1992 lors d'une réunion des ministres Trevi (voir *supra*), elle constitue aujourd'hui un cadre de référence non seulement au niveau des pays européens, mais également au sein d'Europol et d'Interpol.

La standardisation des techniques d'analyse permet non seulement d'améliorer la qualité des analyses, mais rend possible également des réalisations d'analyses criminelles à caractère international. L'activité principale d'Europol réside à l'heure actuelle dans des travaux d'analyse impliquant plusieurs ou la totalité des pays membres.

**5.** Il apparaît cependant que les définitions des techniques aujourd'hui uniformes d'analyse criminelle (surtout d'analyse opérationnelle) ne correspondent pas nécessairement aux exigences de la pratique. L'approche inductive des événements analysés est parfois insuffisante. Si les analyses continueront à s'attacher aux aspects relationnels, géographiques et temporels des dossiers abordés, l'approche pourrait prochainement être revue et reformulée comme « analyse d'orientation » et « analyse de description ». L'analyse d'orientation consisterait en un travail poussé d'induction dans les dossiers où, sur la base des rares éléments disponibles, l'analyste parviendrait à orienter l'enquête ou à remplir un vide dans l'enquête. L'analyse descriptive, quant à elle, viserait davantage à apporter, sur base des informations disponibles, une réponse aux interrogations des enquêteurs (policiers et magistrats).

## PROFILING ET VIE PRIVÉE

**6.** Comme nous l'avons déjà mentionné, seules les analyses opérationnelles nécessitent le traitement de données à caractère personnel. Les développements qui suivent se limitent par conséquent exclusivement à ce type d'analyse. Par ailleurs, nous avons choisi de faire porter notre réflexion sur certains programmes d'analyse criminelle, tels Profiler (utilisé aux États-Unis essentiellement), et ViCLAS, au sujet duquel la Commission de la protection de la vie privée a récemment rendu un avis[10].

---

10 Avis 15/99 du 10 mai 1999. ViCLAS (« Violent Crime Linkage Analysis System ») est un programme d'appui à la recherche judiciaire axé sur la détection de crimes graves touchant à l'intégrité physique des personnes et susceptibles d'être commis en série (meurtres, violences sexuelles, rapts non-parentaux). Il s'agit d'une criminalité d'origine « pathologique », par opposition, par exemple, aux meurtres pour faciliter le vol, aux rapts parentaux dans le cadre de divorces conflictuels, etc. Le traitement est alimenté par des informations recueillies au moyen d'un questionnaire ciblé portant sur différents paramètres relatifs aux faits commis, à leurs auteurs et à la victime concernée. Ces informations sont recueillies au cours de l'enquête relative aux infractions prises en compte dans le cadre de ce système. L'objectif du programme est de regrouper et classer les éléments dans une perspective d'analyse. Dans cette optique, tous les

Quoique ces programmes soient généralement considérés comme des programmes de profiling (analyse de profil spécifique), ils reposent toutefois dans une large mesure sur l'analyse comparative de cas, et il est donc difficile de les qualifier exclusivement de l'une ou l'autre manière. Notons que les observations faites ci-dessous ne sont pas nécessairement applicables à toutes les autres méthodes d'analyse criminelle.

Qu'un programme comme ViCLAS puisse présenter un intérêt pour les enquêteurs ne semble pas douteux; mais de toute manière, ce n'est pas ici le lieu de s'interroger sur l'utilité technique d'un tel outil. Nous limiterons notre réflexion à la compatibilité de tels traitements de données avec les principes de protection de la vie privée tels qu'ils ressortent de la Recommandation (87) 15 du Conseil de l'Europe[11] et de la loi belge de protection de la vie privée[12] (ci-après, la loi du 8 décembre 1992). La Recommandation (87) 15 constitue l'instrument international le plus précis faisant autorité en matière de traitement de données policières[13]. On étudie également la nouvelle loi belge de transposition de la directive 95/46/CE, qui vient préciser l'application des concepts généraux établis par le Conseil

---

éléments, toutes les caractéristiques d'un délit ou de son auteur, peuvent être pertinents et mener à l'établissement de liens entre différentes affaires criminelles.

Ce système d'analyse criminelle, développé au Canada, est actuellement utilisé dans plusieurs pays européens : Royaume-Uni, Pays-Bas, Belgique, Autriche, certains länder d'Allemagne. Il devrait être adopté en 1999 en Suède, en Norvège et au Danemark. Il est en outre utilisé dans des pays d'Europe centrale et non-européens.

11 Recommandation N° R (87) 15 du 17 septembre 1987 du Comité des Ministres aux Etats membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, ci-après, la Recommandation (87) 15.

12 Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements automatisés de données à caractère personnel, telle que modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CEE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données. La loi du 11 décembre 1998 n'est pas encore entrée en vigueur au moment de rédiger cet article, mais le délai de transposition de la directive est écoulé, et la Commission recommande de tenir compte d'ores et déjà de la théorie de l'effet direct des directives et dès lors, du nouveau texte belge de transposition.

13 L'application de la directive 95/46 au secteur policier n'étant pas obligatoire. On note que la Convention n° 108 du Conseil de l'Europe est écrite en termes assez larges et ouverts; de plus, elle contient, tout comme la directive précitée une clause d'exemption pour le secteur policier. La Recommandation 87 (15) est venue clarifier ces principes généraux et doit s'appliquer dans son entièreté. Voir à ce sujet W. BRUGGEMAN, « Data protection issues in inter-institutional information exchange : The case of criminal and administrative intelligence », in *The rights of the individual vis-à-vis police information systems*, Actes du Colloque organisé par l'Autorité de contrôle commune de Schengen, Lisbonne, 1999, p.79 : « Since the Recommendation is a clarification, in a specific context of the general derogation clause in the Data Protection Convention, there is no exception clause in the Recommendation itself. In other words, the Recommendation is intended to be applied *in full* to all police activities involving the collection, storage, disclosure and other use of personal data ».

de l'Europe dans ce domaine. Notons enfin que les principes étudiés ici le sont sans prétention à l'exhaustivité et ont été choisis arbitrairement par les auteurs : seuls sont soulignés ceux dont l'application à la technique de profiling nous a paru soulever des questions particulières : il s'agit, au point 7, de principes de qualité des données (adéquation, proportionnalité, exactitude), au point 8, du traitement de données particulières (données sensibles et relatives à la santé). Enfin, au point 9, c'est le rôle de l'autorité de contrôle qui sera étudié.

## 7. Qualité des données

*7.1.* L'article 4 de la loi du 8 décembre 1992 stipule que les données à caractère personnel doivent être (2°) collectées pour des finalités déterminées, explicites et légitimes (...) ; elles doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues (...). Le principe 2 de la Recommandation (87) 15 précise que « la collecte de données à caractère personnel à des fins de police devrait se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'une infraction pénale déterminée. Toute exception à cette disposition devrait faire l'objet d'une législation nationale spécifique. »

Les autorités ne peuvent donc collecter des données hors les cas précis visés ci-dessus. Ne sont pas acceptables les « fishing expeditions » sans objectif précis. En outre, l'admissibilité de la collecte de données en vue de prévenir un danger réel ne doit pas être comprise comme s'étendant à la prévention de la criminalité en général. La collecte de données non directement reliée à la prévention d'un danger réel, et d'une infraction déterminée pose donc problème. Or, dans un traitement d'analyse criminelle tel que ViCLAS, par exemple, le but n'est pas nécessairement la répression d'une infraction déterminée, mais bien l'établissement de liens entre différentes affaires. Ainsi, on gardera des données relatives à l'auteur d'une affaire élucidée, de manière à voir si un lien ne peut pas être établi avec d'autres affaires non résolues. En outre, si l'on considère que la finalité de programmes de profiling est la répression d'une infraction pénale déterminée, la condamnation définitive d'un auteur devrait entraîner l'effacement de toutes les données le concernant, en application de l'article 4, §5 de la loi de 1992. Or, dans le cas ViCLAS, par exemple, les données relatives à des condamnés sont conservées après la décision définitive, pour les cas de récidive.

*7.2.* L'ampleur de la collecte de données nécessaires pour qu'un tel programme puisse fonctionner utilement est impressionnante. Vu la gravité des crimes visés, cela peut se justifier ; la Commission de la protection de la vie privée a suivi ce raisonnement dans son avis 06/98 au sujet des

fichiers d'analyse Europol[14]. Toutefois, des programmes de profiling (et plus généralement les programmes d'analyse criminelle) ne peuvent être utiles qu'à conditions d'être largement alimentés et employés par les services de police compétents. Si ces programmes sont sous-utilisés, l'appréciation de la proportionnalité de la collecte sera différente, comme le rappelle la Commission dans son avis « ViCLAS » : « d'une part, les données recueillies dans ViCLAS pourraient être considérées comme proportionnelles si elles servent à résoudre un nombre significatif d'affaires. Or, les meurtres non expliqués et à caractère « pathologique » représentent un nombre de cas très limité, même si ces affaires sont sans doute plus spectaculaires ou retentissantes que d'autres. Par contre, les violences sexuelles graves sont beaucoup plus nombreuses ; si l'on veut donc que le critère de proportionnalité soit respecté, il faut, paradoxalement, utiliser ViCLAS dans un nombre important de cas. ». Cela conduit donc, de manière assez curieuse, à plaider pour un emploi généralisé de ces programmes dans le cadre de la lutte contre certains types de criminalité.

***7.3.*** Le principe 3.2 de la Recommandation vise une application particulière de l'exigence d'exactitude des données, que l'on retrouve à l'article 4 §4 de la loi belge en des termes plus généraux. La Recommandation (87) 15 exige un « screening » des données en fonction de la fiabilité de leur origine (« Les différentes catégories de données enregistrées devraient être différenciées, dans la mesure du possible, en fonction de leur degré d'exactitude ou de fiabilité, et en particulier les données fondées sur des faits devraient être différenciées de celles fondées sur des opinions et des appréciations personnelles »). En effet, et les traitements d'analyse criminelle sont un terrain choisi pour cela, il existe un risque qu'une information au départ « douce » (non confirmée) ne soit considérée au fil des traitements comme une donnée dure dont l'exactitude ne peut plus être mise en doute... précisément parce qu'on la retrouve dans différents traitements. Ce phénomène, appelé parfois « blanchiment d'information » est très bien décrit par Bruggeman[15] : « This requirement of screening and classification is a crucial requirement in a field in which much of the information is « raw » or « soft » data. Especially if stored (often in summary form) in an automated database, such data have a great tendency to acquire a life of their own, and to be taken for much reliable and « hard » than they often are ». L'inclusion dans une banque de données d'analyse

---

14 Point 11 de l'avis 06/98 : *« het aantal en de soorten gegevens die verwerkt kunnen worden zijn zeer omvangrijk en behelzen bijna de totaliteit van het privé-leven van een persoon. Gezien het over zeer zware misdadigheid gaat kan hiervoor wellicht gepleit worden. Toch blijft het voor de Commissie essentieel dat de omvang van de bevoegdheid strikt gebonden moet zijn aan de finaliteit enerzijds, en aan de pertinentie en proportionaliteit van de gegevens anderzijds. ».*

15 W. BRUGGEMAN, *op.cit.*, p. 82.

peut avoir de lourdes conséquences pour la personne concernée, et l'on plaide donc pour qu'une évaluation systématique de l'information soit effectuée, et que le rating de la donnée concernée « accompagne » cette dernière lors d'éventuelles communications ultérieures. On note que ce système est rendu obligatoire pour les fichiers d'analyse d'Europol.

## 8. Catégories particulières de données

*8.1.* Le Principe 2.4 de la Recommandation pose que les données sensibles ne peuvent être traitées que dans la mesure où elles sont absolument nécessaires à une enquête particulière. On soulignera ci-dessous les problèmes que le droit belge pose en ce domaine, mais relevons déjà que le traitement de données sensibles est un corollaire quasi indispensable de l'analyse criminelle de type profiling. Des caractéristiques telles que celles visées par cet article peuvent en effet se révéler d'une importance cruciale dans l'identification d'un auteur ou en tout cas dans l'établissement d'un profil d'auteur. Ces données seront donc traitées d'office, sans que l'on puisse savoir a priori si elles seront utiles ou non. Ceci résume assez clairement le problème fondamental de l'analyse criminelle de type profiling. Pour établir des liens entre affaires, tous les détails peuvent se révéler importants (ainsi, les caractéristiques physiques de la victime importent-elles autant que son milieu social, son appartenance à des groupes, son activité professionnelle, la façon dont elle était habillée lors du crime,...) mais il ne s'agit que d'une potentialité. Dès lors, la collecte est difficile à limiter a priori à certains types de données ou à ce qui est nécessaire uniquement à la résolution d'une affaire.

En droit belge, le traitement de données sensibles dans le cadre de programmes d'analyse criminelle pose problème également. L'article 6 de la loi prévoit une interdiction de principe pour le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que la vie sexuelle, sauf pour un certain nombre de services, visés à l'article 3, §4, et §6 de la loi[16], et dans certains cas, énumérés aux articles 3 §3a. et 6 §2. Aucune de ces exceptions générales ne s'applique comme telle aux traitements policiers ou judiciaires... Si un certain nombre d'exceptions particulières est prévu à l'article 6 lui-même, on peut toutefois s'interroger sur celle qui permettra aux services de police de traiter des données de ce type. Peut-être faut-il se référer à la dernière exception qui stipule que l'interdiction ne s'applique pas « lorsque le traitement des données à caractère personnel visées au § 1er est permis par une loi, un décret ou une ordonnance pour un autre motif important

16 Il s'agit essentiellement des services de renseignement et du Centre européen pour enfants disparus et sexuellement exploités. Même dans le contexte que l'on connaît, il est étonnant de voir qu'une telle institution se voie reconnaître de larges exemptions d'application de la loi, alors que les service de police eux-mêmes n'en ont pas bénéficié.

d'intérêt public. » Si telle est la volonté du législateur, elle manque singulièrement de clarté. De plus, cette exception fourre-tout n'exige aucune garantie spécifique, et rien n'est précisé quant à la portée à reconnaître au motif d'intérêt public important.[17] A l'égard des services de police en particulier, ce concept devrait être éclairé par le paragraphe 2 de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, qui précise les conditions dans lesquelles une ingérence par l'autorité publique dans la vie privée du citoyen est admissible.

Concrètement, cette exception devrait donc figurer dans un texte législatif concernant les services de police. Or, la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux ne vise pas expressément le traitement de données sensibles, mais se borne à mentionner en son article 191[18] que : « Dans l'exercice des missions qui leur sont confiées, les services de police peuvent recueillir et traiter des données à caractère personnel et des informations relatives notamment à des événements, à des groupements et à des personnes présentant un intérêt concret pour l'exécution de leurs missions de police administrative et pour l'exécution de leurs missions de police judiciaire conformément aux articles 28bis, 28ter, 55 et 56 du Code d'instruction criminelle ».

La Commission de la protection de la vie privée, dans son avis 99/15 précité, est arrivée à la conclusion que cette disposition n'est pas suffisamment précise pour autoriser le traitement de données sensibles par les services de police : il est en effet question d'une autorisation explicite figurant dans une loi. Il faut donc que le législateur comble cette lacune sans quoi le traitement de données sensibles par les services de police (que ce soit dans le cadre de l'analyse criminelle ou non) se voit privé de base légale.

*8.2.* Les données relatives à la santé ne sont pas envisagées comme telles par la Recommandation 87 (15), sans doute parce que l'on imagine peu de contextes où les services de police seraient amenés à traiter des données médicales. Or, dans un programme d'analyse criminelle visant à retrouver des tueurs ou agresseurs en série, des données relatives à l'état de santé des victimes, et à certaines caractéristiques somatiques des auteurs sont traitées. On peut arguer que ces données relatives à la santé ne sont pas traitées en raison des indications qu'elles peuvent donner sur l'état de santé des personnes concernées, mais bien comme caractéristiques pouvant être utiles à l'identification. Il n'en reste pas moins qu'elles correspondent à la

17 Voir à ce sujet les commentaires de Y. POULLET et TH. LEONARD, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, n° 5928, 22 mai 1999, p. 387.

18 Cet article n'est pas encore entré en vigueur, mais il n'apporte pas de changement fondamental du point de vue qui nous occupe.

définition légale des données relatives à la santé et doivent donc répondre aux exigences légales posées par l'article 7 de la loi de 1992. Cet article interdit le traitement de données relatives à la santé sauf (§2.g) *« lorsque le traitement est nécessaire pour la prévention d'un danger concret ou la répression d'une infraction pénale déterminée »*. Or, comme on l'a déjà souligné, dans un traitement d'analyse criminelle, le but n'est pas nécessairement la répression d'une infraction déterminée, mais bien l'établissement de liens entre différentes affaires. Les travaux préparatoires de la loi n'offrent pas à cet égard de possibilité plus large d'interprétation de ce que l'on entend par « répression d'une infraction pénale déterminée ».

L'interdiction de traitement de données relatives à la santé est également levée (§2,e) *« lorsque le traitement est rendu obligatoire par ou en vertu d'une loi, d'un décret ou d'une ordonnance pour des motifs d'intérêt public importants »*. Cette formulation étant moins restrictive que celle de l'article 6 de la loi, relatif aux données sensibles, peut-on considérer que l'article 191 précité de la loi organisant un service de police intégré, structuré à deux niveaux constitue une base légale adéquate ? Le traitement de données relatives à la santé n'est pas rendu « obligatoire » par cette loi, et elle ne peut donc pas, à notre sens, constituer une base suffisante.

Ici aussi, il serait utile que le législateur apporte une base suffisante au traitement de données relatives à la santé.

**9. Rôle de l'autorité de contrôle**

***9.1.*** Le premier principe de la Recommandation (87)15 se rapporte à la question du contrôle et de la notification. Comme recommandé, la Belgique dispose d'une autorité de contrôle indépendante et extérieure aux services de police. Cette autorité est effectivement chargée de veiller au respect des principes de cette Recommandation. Même si la loi belge fait sortir du champ d'application de certains de ses articles les services de police, il n'en demeure pas moins que la Commission dispose de certaines prérogatives pour exercer son contrôle.

- La Commission peut se faire assister d'experts, et procéder sur place à un examen ;
- Ses membres disposent de la qualité d'officier de police judiciaire, auxiliaire du procureur du Roi. Ils peuvent notamment exiger communication de tout document pouvant être utile dans leur enquête, ainsi que pénétrer en tous lieux où ils ont un motif raisonnable de supposer que s'exerce une activité en rapport avec l'application de la loi vie privée ;
- La Commission peut dénoncer au procureur du Roi les infractions dont elle a connaissance ;

- La Commission peut recevoir les plaintes relatives à sa mission de protection de la vie privée à l'égard des traitements de données à caractère personnel ;
- Elle peut émettre, soit d'initiative, soit sur demande des organes parlementaires ou exécutifs du pays de niveaux fédéral, régional ou communautaire, des recommandations sur toute question relative à ses compétences. Ces recommandations sont adressées au responsable du traitement concerné ;
- Elle peut émettre, soit d'initiative, soit sur demande des organes parlementaires ou exécutifs du pays de niveaux fédéral, régional ou communautaire des avis sur toute question relative à ses compétences ;
- En outre, la Commission exerce de manière indirecte pour le citoyen qui en fait la demande le droit d'accès, de rectification, d'opposition, de suppression ou d'interdiction à l'égard des données gérées par les services de police dans le cadre de leurs missions de police judiciaires et administratives...

***9.2.*** En dépit de l'étendue de ces prérogatives, il y a lieu de soulever les interrogations suivantes.

Si la Recommandation (87) 15 ne semble s'appliquer qu'aux « autorités de police », il faut également tenir compte de la notion « d'organe responsable » (responsable du traitement), c'est-à-dire « l'autorité, le service ou tout autre organisme public qui est compétent selon le droit interne pour décider de la finalité d'un fichier automatisé, des catégories de données à caractère personnel qui doivent être enregistrées et des opérations qui leur sont appliquées ». Cela signifie que sont visées, outre les services de police, également les autorités judiciaires. Aucune référence n'est pourtant faite en ce sens dans la loi belge. Alors que, dans toutes les situations où une analyse criminelle est réalisée à la demande spécifique d'un magistrat, au niveau de l'information ou de l'instruction, le traitement mis en œuvre à cette occasion constitue bien un traitement de données à caractère personnel, la question a été soulevée de déterminer si le contrôle de la Commission peut (ou doit) s'exercer envers le pouvoir judiciaire. Selon nous, il convient de répondre par l'affirmative.

En vertu du Principe 1.3. de la Recommandation (87) 15, la mise en œuvre d'un traitement d'analyse de profil spécifique devrait amener l'organe responsable d'un tel traitement à consulter préalablement la Commission de la protection de la vie privée. Dans le cas du programme Viclas, on peut constater que ce fut effectivement la réaction du service policier responsable de sa gestion. Cette demande d'avis à la Commission fut adressée cependant non pas avant la mise en route du traitement, mais à l'occasion de modification envisagée du programme.

La loi belge, conformément à la recommandation, maintient, même à l'égard des services de police, l'obligation de déclarer tout traitement automatisé préalablement à sa mise en œuvre. Tout traitement d'analyse criminel permanent doit par conséquent faire l'objet d'une telle déclaration. Comme le prévoit la loi, la Commission est en mesure de demander d'autres éléments d'information en sus des mentions légalement prévues à l'article 17. Au regard du caractère sensible de tels traitements, la Commission ne devrait pas manquer d'user de cette prérogative, pour autant qu'elle dispose des moyens nécessaires à cette mission, essentiellement en termes de personnel (nombre et qualification).

Le Principe 1.4. de la Recommandation (87) 15 prévoit également en son alinéa 2 que « les fichiers *ad hoc*, constitués à l'occasion d'affaires particulières, devraient également être déclarés à l'autorité de contrôle soit dans des conditions arrêtées avec celle-ci eu égard à leur spécificité, soit conformément à la législation nationale ». Un certain nombre de traitements d'analyse criminelle n'ont pas manqué d'être mis sur pied en Belgique à l'occasion de quelques affaires retentissantes. Au regard de l'ampleur particulière de ces affaires, et des traitements qui ont été développés, on peut penser que la Commission de la protection de la vie privée a dû recevoir des déclarations particulières. À cet égard, une question se pose : les déclarations adressées à la Commission sont versées, conformément à l'article 18 de la loi du 8 décembre 1992, dans un registre des traitements automatisés. Ce registre est accessible au public. Cette dernière précision doit évidemment attirer notre attention à l'égard des déclarations de traitement *ad hoc*, mis spécifiquement en œuvre dans le cadre d'une enquête judiciaire. D'un côté, le caractère sensible de ce type de traitement devrait justifier une déclaration spécifique à la Commission, afin de permettre à celle-ci d'exercer sa mission de contrôle dans les meilleures conditions, d'un autre côté, il serait mal venu d'assurer une publicité à ces déclarations.

Force est de constater que notre loi nationale ne prévoit rien de spécifique à l'égard de ces situations. Et aucun arrêté royal n'a encore été pris pour préciser l'application des articles 17 et 18. Non seulement la question du contrôle de la Commission à l'égard du pouvoir judiciaire est à nouveau soulevée à cette occasion, mais la possibilité de faire sortir les déclarations éventuelles des traitements d'analyse criminelle hors du registre public n'a jamais été davantage abordée. Face à ce constat, il faut souhaiter que la Commission joue son rôle de médiateur, et fasse preuve d'initiative pour inciter les responsables policiers et judiciaires à faire connaître les traitements *ad hoc* particulièrement sensibles sur le plan de la gestion des données à caractère personnel.

## CONCLUSION

**10.** La réflexion menée sur la problématique de l'analyse criminelle au regard de la protection de la vie à l'égard des traitements de données à caractère personnel nous amène à insister sur deux constats.

***10.1.*** L'évolution de la criminalité et la complexification des enquêtes ont poussé les autorités policières à développer des méthodes standardisées d'analyse des informations. Certaines de ces méthodes d'analyse nécessitent le brassage de nombreuses données à caractère personnel, parfois fort sensibles. Si la Recommandation (87)15 du Conseil de l'Europe reste l'instrument international de référence en matière de traitement de données policières, force est de constater aujourd'hui que cet instrument n'est plus tout à fait adapté à la réalité des nouvelles techniques. Des questions nouvelles se posent du fait de l'introduction des méthodes, entre autres, de profiling. En particulier, il faut souligner l'absence d'autorisation de traitement de données sensibles dans ce contexte, ainsi que de celles relatives à la santé.

Si les méthodes d'analyse criminelle ont effectivement été développées par les services de police, c'est bien parce que ce sont eux avant tout qui traitent les informations dans le cadre des missions de police judiciaire. En matière de protection des données, on semble cependant oublier que les missions de police judiciaire sont effectuées sous la direction du pouvoir judiciaire, ce que n'a pas manqué de rappeler le législateur dans la loi du 12 mars 1998 relative à l'amélioration de la procédure pénale au stade de l'information et de l'instruction.[19] C'est pourtant ce même législateur qui, en matière de protection des données, entretient le manque de clarté à l'égard du pouvoir judiciaire, en particulier quant à la position que prend l'autorité de contrôle à son égard. Les techniques de traitement de données comme l'analyse criminelle sont pourtant en plein essor, et de plus en plus, les magistrats sont demandeurs de ce type d'analyse.

Malgré sa récente révision, la loi belge en matière de protection des données démontre à quel point le législateur tient encore peu compte des techniques nouvelles de traitement des données judiciaires et policières. Alors que la loi vie privée présente déjà des lacunes pour donner aux services de police et à la justice un cadre clair sur certaines questions (traitement des données sensibles et médicales, en particulier), l'analyse criminelle est loin de trouver un cadre légal qui donnera non seulement au citoyen, mais aux acteurs judiciaires également, la sécurité juridique qui

19 *M.B.*, 2 avril 1998. Cette loi est issue de ce qu'on appelle communément la réforme Franchimont. Voir par exemple l'article 28*bis* nouveau du Code d'instruction criminelle, qui définit l'information judiciaire placée sous la direction, l'autorité et la responsabilité du procureur du Roi.

s'impose lorsque le respect des droits fondamentaux, comme la protection de la vie privée, est en jeu.