

LES CAHIERS  
DE LA SÉCURITÉ INTÉRIEURE

*Risque et information*

### **Conditions de publication**

*Les Cahiers de la sécurité intérieure* publient des articles, des débats et des notices bibliographiques relatifs aux différents aspects nationaux et comparés de la sécurité intérieure et de ses acteurs.

Les propositions d'articles doivent être adressées à la rédaction pour évaluation. Les manuscrits soumis ne sont pas retournés à leurs auteurs.

Toute correspondance est à adresser à la rédaction de la revue :

19 rue Pécelet, 75015 Paris. Tél. : 01 53 68 20 48/49

Fax : 01 45 30 50 71 - [cassis@cedocar.fr](mailto:cassis@cedocar.fr)

© Paris, 1998

ISSN : 1150-1634

N° de commission paritaire : 2 325 AD

Les articles publiés dans *les Cahiers de la sécurité intérieure* ne représentent pas une opinion de l'IHESI et n'engagent que la responsabilité de leurs auteurs.

# *Risque et information*

## *Polices et nouvelles technologies*

### *Les enjeux de la transparence*

Avant-propos .....	5-6
--------------------	-----

#### **Dossier**

Point de vue : Le principe de proportionnalité ■ Louise CADOUX .....	7-12
---	------

#### **De la protection à la sécurité des réseaux**

Nouvelles technologies, nouveaux délits ■ Peter GRABOSKY, Russell G. SMITH, Paul WRIGHT .....	13-29
--	-------

Tiers de confiance ou de défiance ?

La sécurité collective face à la cryptographie asymétrique ■ Gaël BOISSEAU .....	31-55
---	-------

Internet et le droit à la sécurité

■ Isabelle FALQUE-PIERROTIN (Conseil d'Etat) et Commission européenne .....	57-67
--	-------

#### **Vers la police de l'information**

Police et innovations technologiques

■ Nicole SOULLIÈRE .....	69-90
--------------------------	-------

Du renseignement au partage des informations :  
l'intelligence protéiforme

■ Nicholas DORN .....	91-108
-----------------------	--------

Table ronde : information et sécurité : les institutions françaises

■ Alain BELVEAU, Richard BROUSSE, Jean-Pascal CODINE, Yves GUILLOT, Jean GUISNEL, Colonel HERNANDEZ, Jean-Claude KARSENTY, Paul LAGIER .....	109-124
--	---------

L'information liberticide ? Le bogue de l'an 2000 :  
un révélateur de la vulnérabilité de nos libertés

■ Daniel NAULLEAU .....	125-134
-------------------------	---------

Interconnexions et fichiers policiers : deux débats de notre temps

■ Joël BOYER .....	135-147
--------------------	---------

La surveillance électronique à domicile :

Une nouvelle économie du pouvoir de punir ?

■ Jean-Charles FROMENT .....	149-168
------------------------------	---------

## Repères

### LES FONDAMENTAUX DE LA SÉCURITÉ

#### La police dans la société du risque et de l'information

■ *Un texte de Richard V. ERICSON et Kevin D. HAGERTY*

*Présenté par Nicolas DUPEYRON* ..... 169-202

### NOTES ET ÉTUDES

#### La « tolérance zéro » est-elle applicable en France ?

■ *Sebastian ROCHÉ* ..... 203-232

#### La mosaïque de l'expertise judiciaire : entre public et privé, monopole et concurrence

■ *Laurence DUMOULIN* ..... 233-251

## Actualités

### NOTES BIBLIOGRAPHIQUES

■ *Julien DAMON, Jean-Louis LOUBET DEL BAYLE,*

*Frédéric OCQUETEAU, Christilla ROEDERER* ..... 253-266

### COLLOQUES ET RENCONTRES

■ *Pierre VARLY* ..... 267

ABSTRACTS ..... 269

ONT CONTRIBUÉ ..... 273

INDEX DES AUTEURS ..... 277

INDEX DES NOTES BIBLIOGRAPHIQUES ..... 283

## AVANT - P R O P O S

Qu'on le veuille ou non, en retard ou en avance, la France fait actuellement son entrée dans la société de l'information. Seize mois après le discours d'Hourtin, le dernier Comité interministériel pour la société de l'information (CISI) a confirmé la réussite du Programme d'action gouvernemental pour la société de l'information (PAGSI). De même, du côté de Bercy, on attribue les bons résultats économiques de 1998, en majeure partie aux richesses et emplois créés par les nouvelles technologies de l'information et de la communication (NTIC). Le débat reste ouvert : les NTIC ne sont-elles qu'un prolongement technologique de plus, ou l'élément central du procès de production de la richesse dans le cadre d'un nouvel ordre économique et socio-politique ?

Concernant la sécurité et plus précisément la police, on retrouve cette opposition. Les technologies nous entourent, c'est indéniable. Elles redéfinissent le paysage de nos pratiques quotidiennes et ce dossier des *Cahiers* a pour but d'explorer plus en avant cette mutation : l'information deviendrait-elle une ressource centrale ?

Le premier thème abordé est celui de la sécurité des réseaux. Les machines ne sont pas omnipotentes et dans l'interface, la sécurité est d'abord une affaire d'hommes. Pour échapper au fort potentiel criminel induit par

l'informatique, les Australiens Graboski, Smith et Wright, soulignent que la protection la plus efficace dans un contexte libéralisé relève de l'ordre de la régulation et essentiellement de l'autodiscipline. Daniel Naulleau prend l'exemple du bogu de l'an 2000 pour mettre en évidence le risque auto-généré par les technologies, à moins d'une veille de tous les moments coûteuse en temps et en moyens. Enfin est posée la question de la redéfinition des limites entre espaces public et privé à la faveur de la communication électronique, de sa transparence et de sa « traçabilité ». Gaël Boisseau décrit bien les affres du débat versatile sur la cryptologie, marqué par des virages à 180 degrés.

Quelles sont les conséquences pour la police, et plus largement pour l'activité policière ? Tout d'abord, il faut observer que les NTIC, malgré leur apparence d'uniformité, relient les univers distincts de l'information, du renseignement, de la communication. En tant que matière numérisée, reproductible à l'infini, instantanément triée et communicable, l'information semble acquérir un pouvoir considérable qui vient remodeler puissamment le métier policier, l'intensifier dans ses moyens et ses contraintes. Une nouvelle économie du pouvoir de coercition et du monopole légitime de la violence semble émerger, qui relie systématisation

du renseignement, ciblage, observation et surveillance directe, à côté du modèle classique de contrôle social fondé sur le couple dissuasion-répression. Ce pouvoir de la surveillance et de la simulation peut aussi s'exercer potentiellement en direction des agents des forces de l'ordre, tel que le signale Nicole Soullière. La mutation doit cependant être analysée et comprise dans l'ordre d'une pensée raisonnée. La recherche de Richard Ericson et Kevin Haggerty, par sa finesse sociologique et par l'introduction de la notion de risque qui fait pendant à celle d'information, y contribue. Pour ces auteurs, la police deviendrait avant tout une police de communication et de gestion des risques. La «proximité» dont on parle tant consisterait avant tout en la connaissance intime des individus et de leurs pratiques, par le ciblage *via* la combinaison de l'information et des modes de calcul du risque. Entre éclatement du local et mondialisation, l'information permettrait alors de redonner consistance au réel. Cette recherche montre aussi que le risque et l'information impliquent la mise en relation et en réseaux des acteurs du contrôle social, l'émergence de nouvelles formes de travail telles que le partenariat, qui transforme la police en intermédiaire informationnel.

Nicholas Dorn qualifie ce changement au niveau de la construction policière et judiciaire européenne. Du renseignement confidentiel, secret, on est passé au partage des informations entre les différentes instances nationales de contrôle et de régulation. Pour lui, cette circulation des informations contribue pour une part non négligeable à l'émergence de la notion de crime organisé.

Mais où en est-on de ce processus en France? La table ronde qui réunit plusieurs des artisans de l'informatisation de nos administrations de contrôle fournit une bonne indication.

En bref, les nouvelles technologies fabriquent de la complexité, en même temps qu'elles sont censées la gérer. Et si le monde anglo-saxon reste un laboratoire nous permettant d'analyser cette complexité, les conditions de reproduction de l'expérience Outre-Atlantique, le plus souvent, ne sont pas réunies. Dans ce contexte de globalisation, la comparaison nous renseigne mais ne saurait nous tracer complètement la voie. Il faut s'atteler à notre spécificité, *via* l'échelle européenne qui permet de revendiquer une éthique et une déontologie propres, ménageant insertion des technologies dans le quotidien et respect de la vie privée, articulant principes de proportionnalité, de finalité et droit à l'oubli (Louise Cadoux). Malgré les efforts nationaux, tels que ceux décrits par Joël Boyer pour la CNIL, quel terrain d'entente trouver pour la transposition de la directive européenne sur les données personnelles et la mise en capacité de l'autorité européenne de régulation des télécommunications (ART)? Les débuts promoteurs du commerce électronique, ou du moins l'ébauche de régulation consensuelle (Isabelle Falque-Pierrotin, Conseil d'État, et Commission européenne) sont un bon indicateur du potentiel européen.

■ Philippe MELCHIOR

## LE PRINCIPE DE PROPORTIONNALITÉ

par Louise CADOUX

Le principe de proportionnalité, applicable par le juge même sans texte, énonce que toute limite, justifiée par un motif d'intérêt public, à l'exercice par les citoyens des libertés publiques doit être strictement proportionnelle à l'objectif à atteindre. Étendu aux applications de l'informatique, ce principe est mis en œuvre par des dispositifs législatifs particuliers se rattachant, à l'intérieur des textes sur les droits de l'Homme, à ceux de la filiation Informatique et Libertés.

Par un jugement en date du 21 juin 1990, non frappé d'appel, le Tribunal administratif de Marseille a annulé la délibération du 12 décembre 1988 du conseil municipal d'Avignon projetant d'installer sur le territoire de la ville quatre-vingt-dix-huit caméras de vidéo-surveillance et un poste central «*permettant la visualisation en permanence de l'ensemble du territoire de la commune et, le cas échéant, l'enregistrement des images*». Pour ce faire, le juge faisait application du principe de proportionnalité, relevant que, malgré la précaution prise par la ville de confier le contrôle du système à la police nationale, «*l'installation généralisée et le fonctionnement permanent de caméras portaient une atteinte excessive aux libertés et notamment au droit à la vie privée et à l'image, qui n'est justifiée ni par une habilitation judiciaire ni par les nécessités de l'ordre public ou la constatation ponctuelle d'infractions au code de la route ou d'atteintes aux biens ou aux personnes*». La délibération était annulée «*comme*

*prise en violation des principes fondamentaux régissant l'exercice des libertés publiques et individuelles».*

Les justifications apportées par la puissance publique pour restreindre les libertés au profit d'une action de police sont-elles suffisantes ? C'est ce que regarde le juge, c'est aussi ce sur quoi devrait s'interroger toute autorité publique avant de décider de recourir à un système informatique, créer un fichier, automatiser un service. Conciliation, équilibre, ajustement, balance des intérêts, place du curseur entre le trop et le pas assez, l'arbitrage n'est pas facile. Et si le principe de proportionnalité est applicable même sans texte, comme l'a dans l'espèce rappelé le Tribunal administratif de Marseille, il n'est pas interdit pour autant de fixer dans des dispositions écrites les outils dont pourra s'aider tout acteur de la sphère publique lorsqu'il aura à examiner si le recours aux nouvelles technologies de l'information et de la communication (NTIC) ne porte pas une atteinte excessive aux libertés, et singulièrement à la vie privée.

#### DE L'EXISTENCE DE DISPOSITIONS ÉCRITES OU D'UNE REDÉCOUVERTE DES TEXTES

Ces dispositions écrites existent. Remontons aux sources, et citons le texte qui donne un fondement juridique explicite au principe de proportionnalité. Tout d'abord l'article 8 de la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales qui dispose : *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale publiques ou à la protection des droits et libertés d'autrui ».*

Une exégèse sans prétention de cet article met en évidence quatre exigences : seule une loi peut border le dis-



positif ; le champ des intérêts protégés est délimité : il s'agit de la vie privée de la personne qui s'étend à celle de sa famille, de son domicile et de sa correspondance ; les intérêts susceptibles de justifier une action publique, - les logiques collectives, diront certains - sont énumérés et bien que nombreux, ils ne sont pas imprécis ; l'ingérence doit être impérativement limitée : il ne peut s'agir que d'« *une mesure, dans une société démocratique, ... nécessaire à la sécurité nationale ...* ». À vrai dire, c'est dans ce quatrième point qu'est plus particulièrement logé le principe de proportionnalité.

La directive européenne du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dont on attend la transposition en droit interne français<sup>1</sup>, tire ses lettres de noblesse de l'article 8 de la convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales qu'elle mentionne dans son considérant 10, notamment pour adjurer les États membres de ne pas utiliser le prétexte de la transposition et le rapprochement des législations de l'Union européenne, pour affaiblir la protection qu'ils assurent déjà.

La France, quant à elle, dispose depuis plus de vingt ans d'un corpus de règles applicables au traitement automatique des informations directement ou indirectement nominatives, corpus constitué par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ainsi que par la convention 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, en vigueur depuis le 1<sup>er</sup> octobre 1985.

Deux points méritent ici d'être soulignés avant d'explorer en quoi ce dispositif concourt à la mise en œuvre du principe de proportionnalité. D'une part, depuis les années 1993-95, le Conseil constitutionnel a accueilli la loi de 1978 dans le socle des lois de libertés publiques auxquelles la Constitution apporte, selon lui, sa garantie, la vie privée étant visée par le Conseil comme une composante de la liberté individuelle. D'autre part, la loi de 1978 dite Informatique et Libertés est d'application générale ; elle

••••(1) BRAIBANT, 1998, rapport au premier ministre, *Données personnelles et société de l'information*, transposition en droit français de la directive du n°95-46, Documentation française.

peut être écartée par le législateur au profit de régimes juridiques autonomes qu'il plaît au Parlement d'établir, sous le contrôle du Conseil constitutionnel. Cependant la dérogation doit être expresse, comme ce fut le cas pour la loi du 21 janvier 1995 qui a encadré le recours aux systèmes de vidéo-surveillance dans les lieux publics et les lieux privés ouverts au public. En revanche, faute d'avoir spécifié clairement que la loi de 1978 était mise à l'écart, le système de placement sous surveillance électronique des condamnés introduit dans l'article 723-7 du code de procédure pénale par la loi du 19 décembre 1997, même s'il précise avec soin les conditions de son application aux détenus, même s'il ne renvoie pas à un avis de la CNIL, ne devrait pas échapper à l'examen de cette autorité pour ce qui n'est pas déjà décidé par la loi, et qui n'est pas négligeable (système informatique mis en place, centralisé ou décentralisé, fiabilité du capteur, conservation des transactions, personnes habilitées à avoir accès aux données collectées, destinataires de ces données, règles de confidentialité, etc.).

#### DU CONTENU DES DISPOSITIONS ÉCRITES : CINQ GRANDS PRINCIPES À APPLIQUER

En quoi la loi du 6 janvier 1978 et la convention 108 qui la complète donnent-elles un contenu au principe de proportionnalité ? C'est ce qu'il faut tenter d'explorer maintenant.

Des droits nouveaux particulièrement adaptés aux risques de l'informatique y sont imaginés. On pourrait souhaiter ne pas les passer en revue et soutenir que c'est l'ensemble des dispositions de ces textes qui met en œuvre le principe de proportionnalité. Pourtant certaines des règles qui y sont prévues participent plus directement à la mise en œuvre du principe. Cinq d'entre elles seront privilégiées.

Au sommet de la pyramide des principes de protection des données est inscrit le principe de finalité. Un traitement, un fichier, doit avoir une finalité précise et déclarée par son responsable, et c'est par rapport à ce principe cardinal de finalité, à cette référence, que les autres principes - qu'il est possible de qualifier de corollaires - peuvent être à leur tour spécifiés et évalués.

Ces principes corollaires concernent ensuite la nature et la masse des données à saisir et traiter, la durée de conservation des données, les destinataires de ces données et l'usage à faire du résultat final du traitement effectué.

Les données personnelles à saisir et traiter doivent être « adéquates, pertinentes et non excessives » par rapport à la finalité annoncée du traitement ; expression pour une première condition légale qui comporte une indication qualitative (adéquates, pertinentes) et quantitative (non excessives).

À l'intérieur de l'enveloppe de ces données, certaines jouissent d'un statut spécial : ainsi les données dites sensibles, relatives aux opinions politiques, philosophiques et religieuses, aux appartenances ethnique et syndicales, à la santé, aux mœurs, à la vie sexuelle, qui, sauf dérogation pour motif d'intérêt public, ne peuvent faire l'objet d'un traitement automatique qu'après consentement exprès de la personne ; ainsi du NIR (numéro d'inscription au répertoire national des personnes physiques), dont l'utilisation ne peut être autorisée que par décret en Conseil d'État, pris après avis de la CNIL ; ainsi des infractions, condamnations et mesures de sûreté qui ne peuvent être traitées que dans le fichier d'un service relevant du ministère de la justice (le casier judiciaire).

Certains traitements, parce qu'ils doivent mettre en regard finalité et données, contraignent à une attention très particulière dans la rédaction de l'acte créant le traitement. De ce point de vue, l'article 3 du décret du 14 octobre 1991 sur le fichier des renseignements généraux qui ne parvient pas, peut-être injustement, à rallier tous les sceptiques ni à réduire les rumeurs au silence, mérite cependant l'estime : après les avatars dont avait été victime un texte précédent en 1990, la nouvelle mouture de 1991 est beaucoup plus resserrée. On invite le lecteur à se reporter au texte, à l'intégralité de celui-ci d'ailleurs.

La durée de conservation des données et des résultats des traitements doit, elle aussi, être limitée par rapport à la finalité de l'application. Il est rare que l'on puisse obtenir des responsables de fichiers que des faits ayant donné lieu à des condamnations légères de personnes encore dans l'adolescence, soient effacés des données stockées ou que

des purges soient systématiquement entreprises. L'émotion de l'opinion dont la presse s'est fait l'écho, au moment de l'examen récent du Système de traitement de l'information criminelle par la CNIL, pointait souvent sur des délais de conservation hors de proportion avec les faits reprochés.

La dissémination des informations personnelles, de certaines d'entre elles du moins, si facile pour une application informatique de consultation à distance, doit être évitée ; c'est dire que la liste des destinataires des données ou des personnes ayant accès aux données doit être arrêtée avec soin et limitée. De ce point de vue, on ne peut que soutenir le ministre de la défense qui, dans sa réponse à un député le 10 février 1997, précisait que la gendarmerie nationale était habilitée, dans ses tâches de recherche et d'enquête, à accéder au fichier des déclarations préalables à l'embauche, à celui des permis de conduire, et au fichier national des automobiles. En revanche, disait-il, les finalités déclarées du fichier de la sécurité sociale ou du fichier des impôts ne justifiaient pas de rendre la gendarmerie directement destinataire des informations y figurant, en dehors d'une commission rogatoire du juge.

Enfin, le résultat du traitement informatique ne doit pas être appliqué mécaniquement ; une appréciation humaine est indispensable pour prendre une décision à l'encontre de quelqu'un. Le principe de la non automaticité des décisions est donc prévu par la loi de 1978 qui ne conçoit pas que l'être humain puisse être traité à l'égal d'un objet. Particulièrement vigilante sur ce point pour les arrêts de la justice, la loi de 1978 pourchasse également les décisions administratives prises sur la base de profils de personnalité. Cette assurance contribue à limiter les excès et dérives de l'informatique que se propose de contenir le principe de proportionnalité.

Tout ce qui vient d'être dit concerne l'établissement de la règle. Il reste à vérifier que celle-ci est respectée. Mais ceci est un autre sujet, celui de l'« enforcement », selon le terme impossible à traduire, de nos partenaires anglo-saxons, qui impose la mise en place de véritables mécanismes de surveillance.

■ **Louise CADOUX**

*Conseiller d'État honoraire, membre de la commission nationale Informatique et libertés (1980-1998)*

# NOUVELLES TECHNOLOGIES, NOUVEAUX DÉLITS<sup>1</sup>

— par Peter GRABOSKY, Russell G. SMITH, Paul WRIGHT

Les nouvelles technologies ouvrent la voie à des potentialités criminelles sans précédent, qu'on trouvera ici recensées dans leur globalité. Face à la mondialisation, et dans l'attente d'une régulation internationale hypothétique, la meilleure solution reste encore, selon les auteurs, l'auto-protection et la discipline individuelle.

•••(1) Cet article a fait l'objet d'une première publication en 1996, sous le titre « Crime and telecommunications », *Trends and Issues in Crime and Criminal Justice*, n° 59, Australian Institute of Criminology. La recherche a été financée pour partie par une bourse du *Telstra Fund for Social and Policy Research in Telecommunications*. Les opinions exprimées ici n'engagent que leurs auteurs et pas nécessairement le gouvernement australien.

Les nouvelles technologies de l'information et de la communication (NTIC) fournissent l'occasion d'activités criminelles d'une étendue et d'une dimension sans précédent. La révolution dans les technologies de l'information que nous connaissons actuellement est sans doute le développement le plus significatif de notre époque. Les changements récents et à venir en matière de télécommunications, notamment en termes de possibilités de connexion et d'informatique, ont de quoi couper le souffle et ont d'ores et déjà eu un impact significatif sur de nombreux aspects de nos vies. Le secteur bancaire, la bourse, le contrôle aérien, le téléphone, l'énergie électrique et tout un ensemble d'institutions dans le domaine de la santé, du social et de l'éducation sont largement dépendants des NTIC pour leur bonne marche. Leurs capacités ont également gagné en efficacité. Pourtant, cette efficacité accrue s'accompagne aussi d'une plus grande vulnérabilité. Dans cet article, on s'attache à résumer une recherche récemment

achevée sur les risques liés aux usages criminels des télécommunications, que celles-ci soient utilisées comme moyen ou prises pour cible. La recherche a été conduite à l'Institut australien de criminologie<sup>1</sup>. Outre l'identification des formes courantes ou émergentes de criminalité impliquant les systèmes de télécommunications comme instruments et/ou comme cibles de l'activité criminelle, l'objectif global de cette recherche était de définir les défauts organisationnels ou de régulation qui facilitent cette activité criminelle, les difficultés existantes dans la détection, l'investigation et la poursuite de ces activités illégales, les problèmes légaux nouveaux posés par ces activités, les mesures qui permettront de minimiser les risques dans le futur pour ces formes d'illégalité, sans provoquer d'effets pervers collatéraux. Notre travail se termine par une discussion des dispositions les plus adéquates pour lutter contre les différentes formes de criminalité dans les télécommunications. Les configurations idéales permettant de lutter contre cette forme de crime ont certes toutes les chances de varier en fonction de l'activité en question mais dans tous les cas, on y retrouvera un mixte de contrôles fondé sur l'application de la loi, sur la régulation et sur le marché. Notre projet s'intéresse aussi aux questions soulevées par la globalisation due à l'extension des systèmes de communication. Pour l'écrire de manière figurée, les systèmes de télécommunications ont fait du monde un espace rétréci, et peu d'entre nous peuvent ignorer dorénavant que les décisions financières prises à Londres ou à Tokyo se répercutent rapidement dans le monde entier, avec leurs conséquences au niveau local. Les photos de célébrités prises à Hollywood deviennent les nouvelles icônes de la Russie ; les images pornographiques prises au Danemark sont accessibles aux jeunes de quinze ans en Australie. Cette réalité nouvelle pose un formidable défi en matière de poursuite judiciaire, qui nécessite une mobilisation par-delà les frontières et les juridictions.

••••(1) GRABOSKY (P.), SMITH (R. G.), WRIGHT (P.), 1998.

## TYPOLOGIE DES DÉLITS

La variété des activités criminelles potentielles est étonnamment étendue. Certaines ne sont pas substantiellement

nouvelles ; seul le moyen est nouveau. D'autres constituent en revanche de nouvelles formes de délinquance. Toutes ces formes de criminalité font l'objet de notre recherche. Elles ne sont pas forcément mutuellement exclusives et la liste n'en est évidemment pas exhaustive. Elles représentent cependant les domaines qui posent actuellement le plus de problèmes aux pouvoirs publics.

#### *Vol de services de télécommunication*

Depuis les premiers pilleurs d'il y a un quart de siècle, les services de télécommunications ont toujours été l'objet de vols, tant de la part de simples plaisantins que de la part de personnes ayant fait de ce type de crime un véritable style de vie et une activité criminelle majeure. Dans tous les cas, ceux qui volent des services posent de sérieux problèmes aux producteurs et aux prestataires de services et au public en général qui, bien souvent, supporte les coûts financiers de la fraude.

Le marché des services de télécommunications volés est fort large. On recense d'abord ceux qui évitent de payer le téléphone ou cherchent à le payer moins cher. D'autres, comme les migrants illégaux, utilisent ce type de services car ils ne peuvent pas avoir accès à des moyens légaux de communication sans révéler leur identité et leur statut ; d'autres encore l'utilisent pour mener à bien des activités illégales, évitant ainsi d'être détectés. À travers le monde, d'immenses sommes d'argent sont ainsi perdues par les victimes de ces formes de délinquance. Des sommes substantielles sont également investies pour prévenir, détecter, et poursuivre de tels délits.

#### *Conspiration criminelle*

Le fait essentiel de la conspiration criminelle consiste en ce que plusieurs individus s'entendent pour commettre une activité criminelle. Les moyens modernes de télécommunications favorisent grandement ce type de collusion d'intérêts. L'émergence de réseaux inaccessibles aux institutions du contrôle social, au moyen de clés d'accès privées, de

cryptages et de technologies de transfert *ultra* rapides de données peut fortement accroître la capacité des organisations criminelles sophistiquées dans l'organisation du trafic de drogues, le jeu, la prostitution, le blanchiment d'argent, la pornographie enfantine et le commerce d'armes (là où bien sûr de telles activités sont illégales).

#### *Vol de la propriété intellectuelle*

Des milliards de dollars sont perdus chaque année en *royalties* et en droits divers du fait du non respect des *copyrights*. La qualité des copies et la vitesse à laquelle il est possible de les réaliser maintenant ont été considérablement accrues par des technologies comme les réseaux d'information en ligne. Le non respect du *copyright* est devenu à la fois facile et rapide, pouvant être réalisé par n'importe qui maîtrisant un tant soi peu l'Internet. Le développement récent et rapide des technologies multimédia crée de nouvelles opportunités pour les pirates de la propriété intellectuelle.

16

#### *Diffusion d'informations attentatoires*

On trouve dans le cyberspace de nombreux contenus qui, aux yeux de certains, devraient être prohibés. Parmi ceux-là, tout ce qui est sexuellement explicite, la propagande raciste et les modes d'emploi permettant de fabriquer des engins explosifs et incendiaires. Les systèmes de télécommunications peuvent également être utilisés à des fins de harcèlement, de menace et d'intrusion, depuis le traditionnel coup de téléphone anonyme obscène à ses formes contemporaines de manifestation dans le cyberspace, lorsqu'un message est envoyé de manière persistante à une personne ne désirant pas le recevoir.

#### *Blanchiment d'argent électronique*

Depuis maintenant un certain temps, les transferts de fonds ont aidé à dissimuler et à déplacer la criminalité. Les technologies émergentes peuvent grandement aider à la



••••(1) WAHLERT (G.), 1996.

dissimulation des gains illicites<sup>1</sup>. Les grandes institutions financières ne seront plus longtemps les seules à pouvoir réaliser des transferts de fonds électroniques passant par-dessus plusieurs juridictions à la vitesse de la lumière. Le développement d'institutions bancaires informelles et de systèmes bancaires parallèles devrait permettre d'échapper à tout contrôle central et faciliter par la même occasion le fait de ne pas remplir l'obligation, qu'exigent certains pays, de déclarer les transactions en *cash*. Les banques clandestines traditionnelles, qui ont fleuri dans les pays asiatiques pendant des siècles, vont pouvoir connaître un nouveau développement grâce aux systèmes de communication. Avec l'émergence et la prolifération de technologies de commerce électronique variées, les mesures traditionnelles de lutte contre le blanchiment de l'argent seront d'ici peu complètement dépassées.

*Vandalisme électronique*

••••(2) HUNDLEY (R.), ANDERSON (R.), 1995.

Plus que jamais, la société industrielle-type des pays occidentaux est dépendante de systèmes de télécommunications et de production de données complexes. Le fait de porter atteinte à ces systèmes ou d'interférer avec eux peut avoir des conséquences catastrophiques<sup>2</sup>.

••••(3) United States, General Accounting Office, 1996.

En novembre 1988, un programme informatique fut introduit sur le Net qui, très rapidement, parvint à bloquer le fonctionnement de quelque six mille ordinateurs sur tout le territoire des États-Unis. Les coûts estimés pour les diagnostics de panne et de maintenance des systèmes s'élevèrent à plusieurs millions de dollars. Les installations de défense américaines ont constitué des cibles privilégiées<sup>3</sup>. Les responsables de la défense, partout dans le monde, investissent énormément dans le domaine de la guerre de l'information et dans les moyens de détruire les infrastructures technologiques des systèmes de communication dans le domaine de la défense.<sup>4</sup>

••••(4) STIX (G.), 1995.

Les systèmes informatiques des universités ont été également visés, étant donné leur accessibilité à de nombreux jeunes gens curieux et fort compétents techniquement. Dans un cas au moins, une attaque dirigée contre un sys-

tème de prévision météorologique conduisit à la perte d'un navire en mer.<sup>1</sup>

••••(1) CHESWICK (W. R.), BELLOVIN (S.M.), 1994.

### *Fraude par télémarketing*

L'usage du téléphone pour des ventes frauduleuses, les sollicitations téléphoniques pour des œuvres de charité et les fausses propositions d'investissements représentent un marché d'environ un milliard de dollars aux États-Unis. L'intensification de l'activité commerciale combinée à l'émergence des NTIC ne peut qu'accroître les risques de ventes frauduleuses. On trouve déjà des ventes frauduleuses et des propositions d'investissement fictif sur Internet. Les développements du *marketing* électronique fourniront de nouvelles opportunités aux personnes peu scrupuleuses et de nouveaux risques pour ceux qui demeureront inattentifs.

### *Interceptions illégales*

Le développement des télécommunications fournit de nouvelles opportunités pour la surveillance électronique des conversations. Depuis des activités aussi traditionnelles que la surveillance des époux infidèles aux nouvelles formes d'espionnage industriel et politique, l'interception des télécommunications a des implications croissantes. Là encore, les développements technologiques créent de nouvelles vulnérabilités. Aidé d'un simple scanner, un individu peut s'asseoir tranquillement chez lui et se connecter sur les téléphones sans fil. De la même façon, les signaux électromagnétiques émis par un ordinateur peuvent être interceptés, la loi existante n'interdisant pas le contrôle à distance du rayonnement des ordinateurs.

### *Transfert électronique de fonds*

La prolifération des transferts électroniques de fonds va augmenter le risque que de telles transactions soient interceptées et détournées. Les systèmes existants tels que les guichets automatiques et les points de ventes automatiques

permettant de réaliser des transferts ont déjà été la cible d'activités frauduleuses, et le développement des cartes à puce de toutes sortes et des cartes à mémoire optique vont sans aucun doute inviter certains à appliquer leurs talents à la contrefaçon de ces moyens de paiement et aux moyens de forcer les systèmes de sécurité protégeant les accès. De la même façon qu'une simple carte de téléphone, les cartes à mémoire peuvent être reprogrammées. Le transfert de fonds, depuis chez soi, de compte à compte ou pour payer des transactions créera inmanquablement des formes de vulnérabilité en termes de vols et de fraudes et le développement à large échelle de la monnaie électronique utilisée sur internet fournira aussi de nombreuses opportunités pour les activités criminelles.

**LE DÉFI DU CONTRÔLE COERCITIF**

Malheureusement, la criminalité liée aux télécommunications, contrairement au pillage de banques ou aux accidents de voiture mortels, n'est pas facilement quantifiable. Certains des délits perpétrés contre les systèmes de télécommunications, lorsqu'ils sont adroitement menés, ne sont jamais détectés, pas même par leurs victimes ; parmi ceux qui le sont, certains sont dissimulés aux autorités car leur révélation pourrait se révéler embarrassante ou pénalisante d'un point de vue commercial.

La quantification peut également se révéler trompeuse. Ce qui apparaît comme quelque chose de trivial peut n'être en fait que la pointe émergée d'un immense iceberg. On trouve une illustration classique de cela chez Stoll<sup>1</sup> qui, en cherchant à comprendre une erreur de compte de 0,75 dollar américain dans un système informatique, en vint à mettre la main sur un réseau international d'espionnage.

Même les descriptions de type qualitatif peuvent être illusoire. De nombreuses personnes, quelles qu'elles soient, ont tendance à accentuer la portée de ce qu'elles font. Les criminels spécialisés dans les télécommunications ne font pas exception à cette règle. Alors que certains font tout pour préserver leur anonymat, d'autres recherchent la notoriété. Bien souvent, ceux-là enjolivent

•••(1) STOLL (C.), 1991.

leurs méfaits. Il existe un décalage significatif entre ce qu'ils font, ce qu'ils disent faire et ce qu'ils croient faire. Les agences de contrôle, quant à elles, sont connues de longue date pour avoir tendance à amplifier les problèmes qu'elles ont à gérer afin de justifier le maintien ou l'accroissement de leurs ressources. D'autres acteurs encore ont bien évidemment un intérêt commercial à accentuer la gravité du problème, l'industrie de la sécurité et les médias.

Au-delà de la réticence mentionnée *supra* des victimes à déclarer les méfaits, les technologies du secret et de l'anonymat, comme par exemple le codage des données, rendent la détection des contrevenants extrêmement difficile. Ceux qui cherchent à masquer leur identité peuvent souvent le faire, en surfant sur de multiples sites dans plusieurs pays. Les redistributeurs de messages électroniques et les procédures de codage peuvent dissimuler quelqu'un aux yeux de tous, à l'exception de quelques agences particulièrement déterminées et disposant de moyens technologiques sophistiqués. Certains crimes ne se traduisent pas immédiatement par une détection ni même par la moindre perte, et d'autres peuvent ne jamais être découverts. Un temps considérable peut s'écouler avant l'activation d'un virus ou bien entre le moment d'une insertion d'une bombe logique et celui de son explosion.

#### PROBLÈMES D'EXTERRITORIALITÉ

L'un des aspects les plus significatifs de la criminalité dans le domaine des NTIC tient à son étendue spatiale. Si la criminalité internationale n'a pas attendu notre époque pour exister, la globalisation des télécommunications augmente considérablement la vulnérabilité aux crimes commis depuis l'étranger. C'est désormais devenu un lieu commun d'avancer que nous vivons dans un monde sans frontières. Cela est sans doute plus vrai pour les criminels que pour les agences de contrôle. Cela entraîne d'importantes implications pour la détection, l'investigation et la poursuite desdits criminels.

Deux problèmes à dimension internationale apparaissent en liaison avec la question de la poursuite des délinquants

en matière de télécommunications. D'une part, la détermination du lieu où le crime a été commis, afin de décider de quel système légal relève l'acte punissable ; d'autre part, la nécessité d'obtenir des preuves et l'assurance que le contrevenant pourra être localisé et traduit en justice. Ces deux questions soulèvent de complexes problèmes de droit en terme de juridiction et de convention d'extradition. Même dans les cas où il est possible de décider quelle loi est applicable, d'autres difficultés apparaissent dans le cadre de sa mise en œuvre. Dans le ressort d'une juridiction unitaire, comme en Nouvelle Zélande, où il existe une loi et une structure chargée de la faire appliquer, déterminer et appliquer la loi appropriée est déjà suffisamment difficile. Dans les systèmes fédéraux, comme au Canada, en Australie, ou aux États-Unis, l'application de lois extra-territoriales est encore plus compliquée.

Pourtant, les activités criminelles perpétrées depuis n'importe où dans le monde posent des problèmes plus difficiles encore. Les États souverains peinent à exercer leur contrôle sur ce qui se fait en ligne chez eux, pour ne rien dire de ce qui se fait ailleurs dans le monde. Du coup, la régulation sur la base d'une conception territoriale de la loi s'avère tout à fait inappropriée pour lutter contre ce type d'infractions<sup>1</sup>.

.....(1) POST (D.G.), 1995.

Les coûts relatifs à la mise en œuvre de poursuites extra-territoriales sont souvent prohibitifs. De plus, la coopération transfrontalière dans ce domaine requiert généralement une convergence de valeurs et de priorités qui, malgré une tendance dominante à la globalisation, n'existe encore que fort rarement. Les images, les idées et la pratique considérées comme parfaitement acceptables en un endroit peuvent être considérées comme odieuses ailleurs. Il y a fort peu de chances que telle autorité qui voit d'un œil indifférent des images électroniques de nudités, les œuvres de Salman Rushdie ou la propagande pour l'indépendance du Tibet consacre beaucoup de temps et d'efforts pour assister les autorités des États dans lesquels ces productions sont considérées comme des crimes.

Par exemple, il a fallu trois décennies pour aboutir à un modeste consensus à propos des mérites d'une assistance

mutuelle internationale en matière de combat contre le trafic de drogues et le blanchiment de l'argent sale. Même dans les pays ayant manifesté un accord de principe, la mise en œuvre effective peut s'avérer difficile<sup>1</sup>. Des problèmes similaires existent en ce qui concerne les *copyrights* et les accords bancaires au niveau international.

D'autres problèmes liés aux enquêtes peuvent rendre complexe la logistique nécessaire aux recherches et aux saisies de matériels en temps réel : le volume de documents dans lesquels les preuves du délit peuvent être contenues, et le cryptage de l'information qui peuvent le rendre entièrement inaccessible, ou accessible seulement après un effort massif et coûteux de décryptage.

On rencontre encore d'autres problèmes touchant à la difficulté qu'il y a à exercer la souveraineté nationale sur les flux de capitaux et d'informations. Des problèmes de compétences juridictionnelles peuvent surgir à propos des transmissions transfrontalières en ligne. Si une lettre de créance en ligne réalisée en Albanie contient des prévisions frauduleuses à propos d'une entreprise dont les actions sont cotées en Australie, on peut s'interroger sur le lieu du crime.

•••• (1) NADELMANN (E.), 1993.

## QUELLES RÉPONSES ?

Étant donné les difficultés qui viennent d'être mentionnées, il paraît approprié de penser à la variété des institutions et des instruments pouvant servir à lutter contre les formes d'illégalité en question. La diversité des formes de télécommunications pouvant donner lieu à des illégalités est telle qu'elle interdit la définition d'une politique univoque. En fait, chacune des formes basiques d'illégalités décrites *supra* est suffisamment complexe à elle seule pour interdire toute solution qui ne fasse pas appel à une combinaison d'instruments. En général, cette combinaison inclura des éléments d'auto-protection à l'initiative des victimes potentielles : des solutions fondées sur le marché ; des initiatives d'auto-régulation prises par les acteurs soumis à régulation ; des mesures coercitives ou régulatrices traditionnelles du ressort de l'État ; et enfin la « co-pro-

duction» par des tierces parties de formes de surveillance, autour d'initiatives privées ou de groupes de citoyens.

### *Autodéfense*

Étant donnée la capacité limitée des gouvernements à contrôler les infractions liées aux télécommunications, la première ligne de défense consiste à faire en sorte que les victimes potentielles adoptent des comportements prudents. De la même façon que la première chose à faire pour se prémunir des cambriolages consiste à s'assurer de ce que ses portes et fenêtres sont bien fermées, il est quelques principes de base à respecter en matière de sécurité de l'information.

Lorsqu'il existe un risque d'effraction informatique, de fraude ou de dévoilement d'informations confidentielles, les individus et les organisations doivent prendre quelques mesures positives de protection. L'exercice de la simple prudence, comme par exemple l'usage de procédures restreignant l'accès aux systèmes informatiques, doit suffire dans de nombreux cas. C'est d'ailleurs là la raison pour laquelle le secteur de la sécurité informatique connaît l'une des plus fortes croissances dans le monde de l'industrie. Ajoutées à des pratiques managériales plus rigoureuses et à l'introduction de mots de passe, et de procédures de vérification plus sophistiquées, de nouvelles technologies, comme par exemple la sécurité biométrique et les programmes de détection des anomalies, aident à améliorer la sécurité des systèmes informatiques.

Après qu'un délit a été commis, c'est encore aux victimes de prendre les premières mesures. Le recours habituel en cas de non respect de la propriété intellectuelle ou de diffamation est de recourir aux tribunaux pour tenter une action en dommages. Récemment, un universitaire de l'ouest de l'Australie a obtenu de substantiels dommages et intérêts après avoir été l'objet de commentaires fort peu flatteurs sur le Net<sup>1</sup> ? Là où les fournisseurs de service sont conscients de la nature injurieuse d'un contenu, ils peuvent également être poursuivis. Dans ces circonstances, le risque encouru devrait aider à augmenter leur degré de surveillance.

••••(1) RINDOS V  
HARDWICK, Supreme  
Court of Western  
Australia, 31 mars 1994)

Le marché lui-même peut fournir des produits permettant de soutenir les initiatives des individus pour se défendre des délits contre les télécommunications. Considérons, par exemple, la question de l'accès sur Internet à des documents douteux. Une grande variété de logiciels commerciaux existe avec lesquels il est possible de bloquer l'accès à certains sites. De plus, un marché est en train d'émerger autour des fournisseurs de service spécialisés dans des contenus adaptés à la consommation des familles, garantissant de ne rien laisser passer ayant trait au sexe, à la violence et à la diffamation.

Il est également probable que se développe un marché autour du contrôle des dégâts causés par une attaque sur les systèmes de télécommunications. Les organisations victimes seront évidemment plus soucieuses d'améliorer leur système de sécurité et de remettre tout leur système en bon état de marche que de porter plainte et de se lancer dans un procès qui attirerait l'attention du public sur leur vulnérabilité. Le développement d'équipes informatiques de traitement d'urgence (*computer emergency response teams* - CERTS), financées par l'industrie et soutenues par les agences de contrôle, aident à apporter un tel type de réponse.

Le potentiel commercial d'Internet, qui pourrait bien devenir le principal instrument commercial à l'horizon de nos vies, ne manque pas d'entrepreneurs partout dans le monde. La mise au point de technologies permettant de sauvegarder la confiance va devenir commercialement nécessaire car cette confiance constitue la base du commerce et minimise le risque d'abus. Quelquefois, il est possible de transformer les problèmes en solutions. Prenons par exemple les virus informatiques, la plaie des opérateurs partout dans le monde. Et bien, il est tout à fait envisageable d'introduire dans les logiciels commercialisés de telles bombes logiques qui, lorsque le logiciel sera copié une seconde fois, seront automatiquement activées.

Les forces du marché peuvent également exercer un contrôle de second degré. Au fur et à mesure que les vastes



organisations commencent d'entrevoir leur vulnérabilité aux actes de vandalisme ou de piratage informatique, elles vont devoir se prémunir contre d'éventuelles pertes. Il est très clairement de l'intérêt des compagnies d'assurance d'exiger de leurs clients la mise en œuvre de mesures de protection appropriées. De fait, l'acceptation des contrats d'assurance et le montant des primes dépendra de ce que les entreprises seront prêtes à faire pour se protéger.

*Auto-régulation*

Un minimum d'auto-régulation devrait également être exercé par les compagnies de télécommunications et les fournisseurs de services. Si le volume du trafic interdit certainement un contrôle systématique, de nombreux fournisseurs de service exigent maintenant comme condition d'accès un engagement garantissant que l'utilisateur s'interdira toute activité illégale, et respectera un certain nombre de règles protocolaires car le non respect de ces engagements pourrait conduire à une rupture du contrat.

Confrontés aux lourdes tentatives étatiques d'imposer une régulation des communications sur Internet, plusieurs groupes industriels développent des codes de bonne conduite afin de limiter les risques d'abus les plus probables dans le cyberspace.

*Co-production citoyenne*

La préoccupation des citoyens à propos de la mise à disposition de matériaux indésirables a donné lieu à des formes de contrôle et de surveillance privées du cyberspace. Deux des plus importantes organisations impliquées dans ce type de surveillance sont le centre *Simon Wiesenthal*, dont la *hotline CyberWatch* permet la dénonciation de tout matériel antisémite ou raciste, et les *Guardian Angels*, avec des *Cyber Angels*, volontaires recrutés pour patrouiller le cyberspace à la recherche de matériels illégaux. Parmi leurs cibles, la pornographie infantine, la calomnie et le harcèlement, le piratage de logiciels, le développement de virus informatiques et tout

ce qui a trait au terrorisme, à la fabrication des explosifs. L'information recueillie auprès des volontaires est ensuite transmise aux autorités compétentes en cas d'activité criminelle et aux fournisseurs de services, lorsque les codes de conduite sont violés. Les groupes d'intérêt public encouragent les sites web enregistrés sous la mention « sécurisés pour les enfants » ou « appropriés pour les enfants », afin de permettre aux parents d'utiliser les logiciels adéquats.

Le contrôle légal est empêché par les nombreuses considérations fiscales, technologiques et territoriales mentionnées plus haut. Pourtant, des procédures et des pratiques sont développées et de plus en plus souvent partagées, permettant d'enquêter sur les délits liés aux télécommunications. Les difficultés sont telles, cependant, que le contrôle conventionnel semble destiné à n'être réservé qu'aux plus sérieuses atteintes.

Malgré les défis posés par le cyberspace, les autoroutes de l'information sont une véritable aubaine pour le contrôle légal. Même si cela demeure pour l'instant à l'état de potentiel, l'usage de la technologie pour les relations publiques générales, pour la communication d'informations de base concernant la prévention des délits et pour l'échange d'informations dans le travail d'enquête devrait se développer énormément dans les années à venir. Déjà, des photographies diffusées sur le Net ont conduit à l'arrestation de personnes inscrites sur la liste noire du FBI.

### *Conséquences imprévues*

Le terrain des illégalités en matière de télécommunications est traversé de conflits et de contradictions : de nombreuses solutions se révèlent être à double tranchant et produisent des conséquences non voulues, quelquefois pires que le mal qu'elles entendent soigner. Tout comme dans d'autres domaines des politiques publiques et de la régulation, il faut s'assurer que les formes nouvelles de protection ne produiront pas plus de mal que de bien<sup>1</sup>.

De la même façon, on mentionnera ce que l'on peut regrouper sous l'expression « effet fruit défendu ». Les ten-

••••(1) GRABOSKY (P.), 1995.

tatives officielles pour bloquer l'accès à un site donné peuvent provoquer l'émergence de « sites miroirs » dans des juridictions plus permissives, servant de points d'accès aux matériaux en question. Les tentatives pour supprimer les sites canadiens faisant de la propagande nazie, ainsi que des informations sur un procès en cours, furent de ce point de vue particulièrement infructueuses.

## CONCLUSION

Le crime international de type conventionnel a posé des défis difficiles à relever pour les autorités judiciaires. Les atteintes concernant les télécommunications sont encore plus délicates de ce point de vue. Il se peut que l'on ne se mette pas d'accord sur la qualification du délit, sur le fait que le délit a vraiment été commis, sur l'identité du délinquant et sur celle de la victime, sur l'autorité compétente pour engager des poursuites, pour assigner en justice et pour condamner.

Il existe une tension fondamentale entre l'impératif de dérégulation caractérisant les économies avancées dans le monde et le désir de contrôler les aspects les moins licites des télécommunications. Pourtant, il nous semble qu'il est nécessaire de favoriser la marche vers la dérégulation, tout du moins pour l'instant. La mise en place de formes de régulation prématurées qui, non seulement sont susceptibles de ne pas produire les effets désirés, mais peuvent également avoir un impact négatif sur le développement de la technologie, pourrait en effet s'avérer un réel danger. Une sur-régulation, ou une régulation prématurée peut brider les investissements et l'innovation. Étant donné la nature de plus en plus compétitive du marché mondial, les gouvernements devront forcément choisir entre les impératifs paternalistes et ceux du développement commercial et de la croissance économique.

Le défi à relever pour ceux qui voudraient limiter la délinquance dans le domaine des communications revient à chercher un équilibre qui autoriserait un degré tolérable d'illégalité en échange d'une exploitation créative de la technologie. À ce stade encore premier de la révolution

technologique, il serait utile que les individus, les groupes d'intérêts et les gouvernements parviennent à clairement articuler leurs préférences pour envoyer des signaux au marché. Le marché devrait être capable de fournir des solutions plus efficaces que celles que pourraient mettre en place les États.

Les télécommunications ne sont pas le premier domaine, ni le seul, qui outrepassent les limites d'un État national. Le trafic aérien, le droit de la mer, les transferts de fonds et des questions environnementales comme l'amincissement de la couche d'ozone ou le réchauffement de la planète, parmi d'autres, ont nécessité des efforts concertés au niveau international. On peut s'attendre à ce que des règles internationales en réponse à la criminalité en matière de télécommunications se développent selon le même modèle que dans d'autres domaines posant des problèmes de territorialité, depuis le trafic de drogues jusqu'aux essais nucléaires, en passant par la chasse à la baleine. Reste à savoir si les efforts de coopération pour combattre la délinquance en matière de télécommunications donneront des résultats plus convaincants que dans les domaines précités.

■ **Peter GRABOSKY**

*Directeur de recherche*

**Russell G. SMITH**

*Chercheur senior*

**Paul WRIGHT**

*Chercheur mis à disposition du WA Police Service à l'Institut australien de criminologie.*

## BIBLIOGRAPHIE

- CHESWICK (W. R.), BELLOVIN (S. M.), 1994, *Firewalls and Internet Security*, Addison Wesley, Reading, MA.
- GRABOSKY (P.), SMITH (R. G.), WRIGHT (P.), 1998, *Crime in the Digital Age, Controlling Telecommunications and Cyberspace Illegalities*, Sydney, The Federation Press, and New Brunswick, NJ, Transaction Publishers.
- GRABOSKY (P.), 1995, « Counterproductive Regulation », *International Journal of the Sociology of Law*, vol 23, p. 347-369.
- HUNDLEY (R.), ANDERSON (R.), 1995, « Emerging Challenge : Security and Safety in Cyberspace », *IEEE Technology and Society Magazine*, vol. 14, p. 19-28.
- NADELMANN (E.), 1993, *Cops across Borders : The Internationalization of US Criminal Law Enforcement*, Pennsylvania State University Press, University Park.
- POST (D. G.), 1995, « Anarchy, State and the Internet : An Essay on Law-Making in Cyberspace », *J. Online L*, art 3, <http://warthog.cc.wm.edu/law/publications/jol>.
- STIX (G.), 1995, « Fighting Future Wars », *Scientific American*, vol 273, n° 6, p. 74-80.
- STOLL (C.), *The Cuckoo's Egg*, Pan Books, London.
- United States, General Accounting Office, 1996, *Information Security : Computer attacks at Department of Defense Pose Increasing Risks ; GAO/AIMD-96-94*, 22 mai.
- WAHLERT (G.), 1996, « Implications for Law Enforcement of the Move to a Cashless Society », in GRAYCAR (A.), GRABOSKY (P. N.), (dir.), *Money Laundering, Research and Public policy series n° 2*, *Australian Institute of Criminology*, Canberra, p. 22-28.



# TIERS DE CONFIANCE OU DE DÉFIANCE ?

## La sécurité collective face à la cryptographie asymétrique

par Gaël BOISSEAU

La cryptologie est, à ce jour, l'unique moyen de sécuriser les correspondances échangées sur Internet. À ce titre, elle fait l'objet d'un important débat et de rebondissements incessants en matière de législation, dans un contexte mondialisé.

La sécurité relève-t-elle du collectif et donc d'une prérogative étatique ou procède-t-elle au contraire d'un droit premier de l'individu, et doit-elle dès lors demeurer subordonnée à sa seule volonté ?

C'est l'enjeu primordial du statut de la confidentialité dans une société de l'information et de la transparence que présente et discute cet article.

Lors de son intervention du 15 octobre 1997 devant l'Assemblée générale des Nations Unies, Bill Clinton n'a pas hésité à placer les nouvelles technologies de l'information au rang des principales menaces pour la sécurité du prochain siècle. Dans le même discours, il se faisait pourtant l'ardent défenseur de ces technologies, mettant en exergue leur capacité à garantir les libertés et la circulation des valeurs de la démocratie. Cette dialectique entre crainte et espoir liée à la diffusion des technologies de transport, de production et de gestion de l'information numérique est la manifestation de leur importance croissante dans les sociétés modernes. En effet, si cette modernité se caractérise selon Ulrich Beck par la place centrale occupée par la gestion du risque, alors il n'est pas étonnant de constater que dans une société dite de l'information, celle-ci soit devenue l'objet et le sujet de risques majeurs, et apparaisse comme « *un problème touchant la collectivité et appelant une intervention publique* » (GILBERT, 1998 ; BECK, 1997).

D'une part, l'information véhiculée par les réseaux de télécommunication, aux premiers rangs desquels Internet, apparaît régulièrement comme une menace potentielle à l'ordre public. Ces réseaux deviennent le support d'activités criminelles comme la pédophilie, le blanchiment d'argent ou les trafics de tout type. Ils suscitent, en outre, de nouvelles formes de délinquance comme le piratage informatique. D'autre part, des affaires comme celle des écoutes de l'Élysée ont permis de prendre conscience de la persistance, même dans un régime démocratique, d'atteintes graves à la vie privée, du fait de l'action de la puissance publique et ce en dehors de tout motif légitime.

#### ENTRE L'INDIVIDUEL ET LE COLLECTIF

L'un des principaux problèmes soulevés par l'usage des réseaux informatiques réside dans l'existence de ces deux risques en matière de sécurité des informations, l'un individuel, l'autre collectif, dont les méthodes de réduction sont inconciliables. Les utilisateurs souhaitent en effet légitimement pouvoir se prémunir des menaces pesant sur leurs communications, au nom du respect de la vie privée mais aussi de leur intérêt économique. Pour ce faire, ils ont à leur disposition une technologie, la cryptographie, qui permet selon la définition de la loi du 26 juillet 1996, de « transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers ». Cependant, en agissant de la sorte, ils privent aussi l'État de toute capacité de contrôle sur les flux d'informations véhiculés par les réseaux informatiques. Entre les besoins de sécurité collective pris en charge par l'État et le développement d'une indispensable sécurité individuelle assurée par des moyens privés, la cryptographie est devenue en quelques années l'objet d'un débat profond.

Celui-ci s'est cristallisé au niveau international ainsi que dans de nombreux pays, aux premiers rangs desquels la France, dans une opposition entre militants pour une libéralisation totale de la cryptographie et partisans du maintien d'un contrôle public de sa production, de sa diffusion et dans certains cas de son usage. Malgré une faible visibi-



lité publique, les enjeux de ce débat ne sont autres que la définition des risques acceptables et de leur mode de gestion dans la société de l'information naissante. Afin d'en prendre la mesure, nous nous attacherons, dans cet article, à en présenter le contexte technique, juridique et politique, tout en étant conscient que ce choix conduira bien souvent à ne pas restituer l'entière complexité du sujet.

### LA CRYPTOGRAPHIE, UNE TECHNOLOGIE INDISPENSABLE

L'une des principales caractéristiques d'Internet réside dans son absence quasi totale de sécurité. Utilisé sans procédé de sécurisation additif, il est en effet extrêmement facile de détourner, de lire ou de modifier les informations transportées. De même, aucune procédure d'authentification fiable de l'émetteur ou du récepteur d'un message n'est prévue par les protocoles standards. Cette situation n'est cependant pas exceptionnelle, la majorité des moyens de communication à distance grand public n'offrant guère plus de sécurité. L'authentification de l'auteur d'un appel téléphonique repose ainsi sur la mise en œuvre de connaissances ou de procédés indépendants des technologies de transport elles-mêmes. Toute communication à distance est de fait exposée à la possibilité d'intervention d'un tiers ou d'un correspondant mal intentionné. Cependant, dans le contexte technique d'Internet, deux éléments contribuent à transformer un risque résiduel en risque majeur. Ils résident dans les caractéristiques techniques de ce réseau.

### INTERNET : UN ENVIRONNEMENT PEU SÉCURISÉ

Internet est un réseau informatique, ce qui signifie que l'information qui y circule est destinée à être traitée par des ordinateurs. En terme de sécurité, cela implique que toute personne accédant à l'information peut la dupliquer, la modifier et surtout la traiter en utilisant la puissance et la rapidité des ordinateurs actuels, et ce sans laisser de trace physique. Cette caractéristique entraîne une réduction considérable du coût des actes malveillants. Là où l'interception du courrier, à titre d'exemple, oblige à une ouver-

ture et à une lecture effective des correspondances - ceci ayant un coût important qui doit être proportionné au gain espéré - un programme de tri du contenu des messages permet de filtrer automatiquement des millions de messages pour en extraire les données pertinentes, comme par exemple des numéros de carte bleue.

Les conséquences de cette caractéristique sur le niveau général de sécurité dépendent du nombre de points où l'information est accessible sous forme exploitable entre l'émetteur et le récepteur. Dans ce domaine, un réseau comme Internet est malheureusement particulièrement exposé. En effet, l'acheminement des informations repose sur le protocole IP ; or, ce dernier fonctionne en mode non connecté, ce qui implique qu'aucune connexion permanente n'est établie entre les correspondants lors de la communication<sup>1</sup>. Plus simplement, il suffit de mesurer la différence qui existe entre un appel téléphonique et une communication par échange de courriers successifs. Dans une communication téléphonique, un premier message, la numérotation, permet de connecter les deux interlocuteurs. À partir de là, l'information est envoyée sur cette connexion qui peut donc être protégée de bout en bout jusqu'à la déconnexion. Le protocole IP fonctionne, quant à lui, sur le mode du courrier et n'établit donc aucune connexion ; de ce fait, tous les paquets d'information doivent comporter des éléments d'adressage utiles à leur acheminement. Dans ces conditions pour être expédiés, les messages ne peuvent être intégralement cryptés. L'acheminement implique, en effet, la lecture d'une partie des informations transportées (l'adresse), alors même que le mode de routage utilisé multiplie les points d'aiguillage. En tous ces points au sein du réseau, il est possible d'accéder à l'information ou d'en introduire.

La seule solution de sécurisation réside dans l'usage de technologies rendant le contenu des messages inutilisable sans pour autant modifier les éléments servant à l'acheminement. C'est là qu'intervient la cryptographie. Bien sûr, les messages pourraient être cryptés à un niveau très bas, au niveau du transport physique par exemple ; cela se fait sur certains réseaux mais ne peut se faire sur Internet du

••••(1) Pour une présentation complète du protocole IP, voir HUITEMA, 1995.

••••(1) BRANDSTAD, 1987 ;  
VOYDOCK, KENT, 1985.

••••(2) Étant donné la nature des paquets IP, le terme de lettre n'est pas le plus adapté. Il suggère en effet l'idée d'une enveloppe. La carte postale correspond mieux à la nature de ce type d'acheminement de l'information.

••••(3) CAMP, SIRBU, 1997.

fait de l'absence d'établissement de connexion.<sup>1</sup> Dès lors, le cryptage des informations est réalisé de façon active par l'utilisateur lui-même. Le réseau d'acheminement ne fournit donc aucun service en terme de sécurité. Pour continuer à utiliser la comparaison avec le service postal il n'y a que le contenu des lettres qui peut être crypté, et seule la personne qui rédige la lettre peut le faire<sup>2</sup>.

Avant d'entrer un peu plus avant dans la présentation des principes et des applications de la cryptographie, il est nécessaire de cerner les besoins des utilisateurs d'Internet en matière de sécurité, afin de mesurer en quoi cette technologie y répond.

#### LES ÉLÉMENTS CONTRIBUANT À SÉCURISER L'INFORMATION

La notion de sécurité au sein d'un réseau comme Internet recouvre plusieurs aspects. Il s'agit à la fois de la sécurisation des éléments physiques ou logiques constituant le réseau et de la sécurisation des informations. La cryptographie relève principalement de ce type de préoccupation. Bien qu'une attaque contre un élément du réseau menace bien souvent les informations qu'il véhicule, nous n'aborderons pas cet aspect du problème qui ne relève pas uniquement de l'usage de la cryptographie.

Assurer la sécurité en matière de transport de l'information consiste à répondre à quatre questions induites par la distance entre les correspondants et la possibilité d'action d'un tiers.<sup>3</sup>

*La confidentialité.* Lors de toute expédition ou réception d'un message, il est nécessaire de s'assurer que celui-ci sera utilisable uniquement par son destinataire légitime. Un tiers ne doit pas avoir la possibilité d'exploiter les informations transmises, même si celles-ci devaient, pour une raison ou un autre, tomber en sa possession.

*L'intégrité.* Dans le même ordre d'idées, il est nécessaire de pouvoir s'assurer que les informations reçues sont bien celles émises par l'émetteur. Toute modification ou altération par un tiers des informations transmises doit être décelable ou impossible.

*L'authentification.* Il s'agit là de se prémunir contre l'action non plus d'un tiers mais d'un correspondant malveillant. Lors de toute expédition ou réception d'un message, il est nécessaire de pouvoir garantir l'identité de son producteur. Les informations diffusées doivent donc pouvoir être identifiées au moyen d'une signature qui leur garantis- se un caractère authentique et permette en outre de s'assu- rer que l'émetteur ne pourra pas nier les avoir envoyées.

*La non-répudiation.* Il s'agit du corollaire de l'authentifi- cation. Elle permet de garantir à l'expéditeur la réception effective de son message par le correspondant, elle peut s'accompagner de la conservation de traces attestant de cet envoi d'information.

Sans adjonction de technologies additives de sécurisa- tion, Internet ne présente aucune garantie sur ces quatre points. Il s'agit là d'un problème très préoccupant dès lors que les informations échangées nécessitent un niveau de sécurité important. Si le courrier électronique personnel requiert un niveau de sécurité peu élevé pour un usage nor- mal, il n'en va pas de même pour les échanges générés par le commerce électronique ou le transfert d'informations médicales et administratives par exemple. Ce type d'appli- cation étant appelé à se développer sur Internet, les acteurs les mettant en œuvre ou désireux de le faire se sont tour- nés vers la cryptographie, qui permet de résoudre en gran- de partie ces problèmes.

#### PRINCIPES ET APPLICATIONS DE LA CRYPTOGRAPHIE ASYMÉTRIQUE

La cryptographie moderne repose dans sa quasi-totalité sur un modèle commun<sup>1</sup>. Afin d'être rendues inexploi- tables par un tiers, les données sont transformées grâce à une fonction : l'algorithme. Celui-ci permet d'assurer la permanence de la méthode de cryptage et sa portabilité d'un utilisateur à un autre. Cependant, pour maintenir l'unicité de chaque procédure de cryptage, il est nécessai- re de pouvoir paramétrer cet algorithme, à l'aide d'une clef logique<sup>2</sup>. Ainsi, l'utilisateur crypte ses données en utilisant un algorithme standard mais en recourant à une clef qui lui

••••(1) Pour une présen- tation beaucoup plus com- plète de la cryptographie d'un point de vue tech- nique, cf. SCHNEIER, 1994 ; d'un point de vue histo- rique, cf. KAHN, 1996.

••••(2) L'idée de baser la sécurité sur les clefs et non sur l'algorithme a été intro- duite au dix-neuvième siècle par August Kerckhoffs. Ce type de cryptographie vise à assurer une permanence de la sécurité dans l'hypo- thèse où l'algorithme est connu. Elle a naturellement trouvé une application dans le domaine des réseaux de télécommuni- cation civils où, pour des rai- sons de compatibilité, tous les utilisateurs doivent utili- ser les mêmes algorithmes (KERCKHOFFS, 1883).

est propre. Une personne désireuse d'accéder à l'information doit donc, soit essayer de comprendre le mécanisme de chiffrement en analysant l'algorithme afin de rétablir le document originel, soit posséder la clef. Cette possession peut être légitime mais elle peut aussi être obtenue par essais successifs. La sécurité d'un système de chiffrement repose donc sur trois éléments : la puissance de l'algorithme ; la taille des clefs, qui a dû croître considérablement avec l'augmentation des puissances de calcul informatique ; la gestion des clefs.

*L'invention de la cryptographie asymétrique*

Dans le cadre d'un usage en réseau, il est impératif de résoudre ce dernier problème et plus particulièrement celui de leur transmission. En effet, il est indispensable que le destinataire d'un message dispose de la clef ayant servi à le crypter ; or, celle-ci ne peut elle-même l'être. Il est donc nécessaire avant toute transmission sécurisée de transférer l'élément permettant cette sécurisation, sans aucune garantie. Il s'agit là d'une faille majeure. Ce problème a toutefois été résolu dès les années soixante-dix par la création de la cryptographie asymétrique<sup>1</sup>. Alors que la cryptographie traditionnelle, dite symétrique, utilise une seule clef pour chiffrer et déchiffrer un message, la cryptographie asymétrique utilise un couple de clefs dont une seule est diffusée, ce qui supprime le problème de la sécurité de leur transmission. L'une, la clef privée permet de déchiffrer les messages cryptés à l'aide de l'autre, la clef publique. Ainsi un individu A désireux d'envoyer un message chiffré à un individu B doit le crypter à l'aide de la clef publique de A. À la réception, celui-ci utilise sa clef privée pour déchiffrer le message.

••••(1) DEFFIE, HELLMAN, 1976.

Cette solution permet d'assurer la confidentialité des messages et leur intégrité. Une fois que les données ont été chiffrées à l'aide d'une clef publique, seul le possesseur de la clef privée peut y accéder : elles ne sont donc plus exposées durant leur acheminement.

La cryptographie asymétrique résout en outre le problème de l'authentification. La procédure repose sur le mécanisme inverse. L'expéditeur A d'un message pour un individu B

l'authentifie en y accolant une signature. Celle-ci est cryptée à l'aide de la clef privée de A, les deux clefs étant liées, si B peut décrypter cette information, alors A est bien l'auteur de la signature <sup>1</sup>.

La cryptographie asymétrique est un instrument de sécurisation extrêmement performant, qui permet d'établir des communications sécurisées au sein d'un réseau non sécurisé. Elle limite considérablement la capacité de nuisance des tiers et permet d'identifier l'expéditeur d'un message. Ce faisant, elle réduit le niveau de risque lors des échanges d'information à un niveau acceptable, bien qu'elle ne résolve pas tous les problèmes, notamment ceux liés à la non répudiation <sup>2</sup>.

En tant que technologie de réduction du risque, ses applications au sein des réseaux informatiques Internet mais aussi au sein des réseaux d'entreprises sont considérables. Le commerce électronique en est l'une des plus importantes (*International Institut of Communications*, 1998). Cependant, elle soulève un problème majeur. Le fondement de toute cryptographie est de supprimer aux tiers l'accès à des informations ; or, si cela est dans l'intérêt immédiat des protagonistes de l'échange, l'interception des messages devient par là-même impossible pour la puissance publique. La cryptographie permet donc de créer un espace privé immatériel échappant potentiellement au contrôle étatique.

Ici apparaît nettement le risque induit par cette technologie. En réduisant le risque au niveau interpersonnel, elle en génère de nouveaux au niveau collectif, la collectivité perdant toute capacité de contrôle des flux d'information. Or, il s'agit d'un enjeu majeur pour la société de l'information et la définition du rôle de l'État en son sein. Perdre le contrôle des flux d'information entraîne en effet l'incapacité de celui-ci à garantir le respect de ses lois au sein de ces échanges immatériels <sup>3</sup>. Indirectement, cela le prive même de la capacité de taxer les activités marchandes n'ayant aucun support physique. Une partie du commerce des informations et des flux financiers qui en découlent pourrait donc lui échapper.

Ainsi, la cryptographie en tant que technologie de réduction des risques de la sphère privée apparaît-elle aussi

••••(1) NEEDHAM, SHROEDER, 1978 ; RIVEST, SHAMIR, ADELMAN, 1978.

••••(2) Les systèmes de paiement électroniques utilisent la cryptographie asymétrique mais y adjoignent un tiers jouant le rôle d'intermédiaire entre le client et l'acheteur. Celui-ci permet de garantir la réalité de la transaction, mais aussi la solvabilité du client et l'honnêteté du commerçant.

••••(3) L'administration Clinton a d'ailleurs décidé de considérer pour l'instant Internet comme un espace de libre échange.

comme un risque au niveau collectif, nécessitant par là-même une intervention publique.

Cette opposition d'intérêts s'est cristallisée autour de la question du contrôle de l'usage de la cryptographie.

## LES TENTATIVES D'ENCADREMENT DE L'USAGE DE LA CRYPTOGRAPHIE

### UNE TECHNOLOGIE MILITAIRE DEVENUE CIVILE

La cryptographie est une technologie ancienne, utilisée de longue date principalement par les militaires et les services secrets désireux de transporter des informations sensibles dans des environnements peu sécurisés. De par son origine militaire, la cryptographie est longtemps demeurée soumise aux mêmes réglementations que les armes et munitions. Cependant, l'usage de cette technologie s'est progressivement étendu au-delà des applications militaires. L'informatique et les télécommunications sont en grande partie à l'origine de cette évolution. L'augmentation des puissances de calcul a rendu possible une diffusion de moyens de chiffrement puissants auprès d'utilisateurs disposant de simples micro-ordinateurs. Dans le même temps, l'émergence d'importants réseaux ouverts non sécurisés, comme Internet, a généré un réel besoin au sein d'une population de plus en plus nombreuse. Le développement d'Internet apparaît à ce sujet comme un tournant.

Ces besoins nouveaux en matière de technologie de sécurité se sont vite traduits par la création et la diffusion de logiciels de chiffrement puissants, reposant sur les principes de la cryptographie asymétrique. La création en 1991 du programme *Pretty Good Privacy* (PGP) par l'américain Phill Zimmerman a marqué définitivement la perte de contrôle des milieux militaires et des services du chiffre sur la production de moyens de chiffrement<sup>1</sup>. Jusque-là, l'élaboration et la diffusion des logiciels ou matériels de chiffrement à usage civil étaient restées relativement bien contrôlées par la puissance publique. Ainsi l'élaboration du *Data Encryption Standard* (DES) finalisé en 1974, s'est faite dans le cadre d'une collaboration étroite entre la

•••(1) L'histoire de PGP et de son créateur est relatée dans de nombreux ouvrages, on retiendra particulièrement, GARFINKEL, 1996.

National Security Agency (NSA) et la firme IBM (KAHN, 1996; BAMFORD, 1982). Le DES permet ainsi d'offrir un niveau de sécurité satisfaisant pour les utilisateurs, tout en maintenant la possibilité d'un contrôle de l'État, celui-ci disposant de toute évidence des moyens nécessaires pour le casser. La création d'un programme comme PGP, bientôt suivi par de nombreuses autres applications utilisant la cryptographie asymétrique, a bouleversé cet arrangement.

L'algorithme RSA utilisé par la plupart de ces programmes offre en effet un niveau de sécurité extrêmement élevé<sup>1</sup>. En l'état actuel, il semble qu'aucun service du chiffre ne soit capable de décrypter un message crypté par ce moyen. Confrontés à des logiciels de chiffrement actuellement incassables, les États se trouvent en outre incapables d'en contrôler la diffusion. Qu'il s'agisse de téléchargement *via* Internet ou de la simple copie à l'aide d'une disquette, la reproduction et la dissémination de ces logiciels ne posent aucun problème technique, pas plus qu'elles n'induisent de coût de production<sup>2</sup>. De ce point de vue, la cryptographie civile est donc devenue incontrôlable par les moyens classiques d'autorisation de production et d'importation. Or, celle-ci a, par ailleurs, des utilisateurs civils, des producteurs civils et des applications dont la nécessité apparaît aux États eux-mêmes. Cependant, la volonté d'un encadrement de l'usage, de la production et de la diffusion persiste. Certains États, conscients de l'impossibilité du maintien d'un contrôle strict ont donc tenté d'élaborer une législation autorisant l'usage et le commerce de cette technologie, mais qui préserverait leur capacité de contrôle sur le flux d'information<sup>3</sup>.

Le but d'un encadrement de l'usage, de la production et de la diffusion des procédés de cryptographie est de permettre à l'État de garder le contrôle sur des technologies susceptibles de soustraire à son pouvoir certains échanges d'informations. Ce contrôle a deux grandes finalités. Premièrement, il vise à empêcher l'usage de technologies trop puissantes, soit du fait de la taille des clefs soit du fait de la force de l'algorithme. Deuxièmement, il tend à empêcher que ces technologies tombent en possession d'États ou de groupements qui lui sont hostiles. Le deuxième objectif passe par un contrôle de la diffusion et notamment

••••(1) RSA est l'acronyme de Rivest, Shamir, Adleman nom des trois scientifiques du MIT, qui mirent en pratique, en 1977, le concept de cryptographie à clef publique inventé par Diffie et Hellman. RIVEST, SHAMIR ADLEMAN, 1978.

••••(2) La légende retient aujourd'hui que, pour tourner l'interdiction d'exportation frappant les procédés de cryptographie, le code source de PGP fut introduit en Europe tout à fait légalement sous la forme d'un *listing* papier qui fut ressaisi. Par la suite, certains libéraux américains proposèrent de tatouer les clandestins menacés d'expulsion avec ce même code source afin d'en interdire l'exportation et de garantir ainsi leur présence.

••••(3) Il est important de noter que tous les États n'ont pas tenté cette conciliation. Dans un certain nombre d'entre eux, notamment en Europe du Nord, l'utilisation de la cryptographie est libre. *L'Electronic Privacy Information Center* (EPIC) tient à jour une revue de l'ensemble des législations en matière de cryptographie au sein des pays de l'OCDE. Disponible sur Internet : [www.epic.org](http://www.epic.org).



de l'exportation, ce type de contrôle est au centre de la législation américaine actuelle. Le premier objectif nécessite soit que l'État possède des puissances de calculs considérablement plus élevées que celles disponibles dans la sphère privée, soit qu'il affaiblisse d'une manière ou d'une autre, et pour lui seul, le niveau de sécurité offert par les systèmes de sécurité mis en place.

LE DÉPÔT DES CLEFS PRIVÉES, L'IMPOSSIBLE CONCILIATION  
ENTRE SÉCURITÉ PRIVÉE ET SÉCURITÉ COLLECTIVE

Pour comprendre le fondement des débats actuels et plus particulièrement la législation française, il est nécessaire d'introduire une différence entre moyens de protection et système de sécurité. Les moyens de protection correspondent à l'ensemble des technologies utilisées pour résoudre un problème assimilé à un risque. La cryptographie en tant que technique permet de rendre inexploitable des données par un tiers, elle résout donc, comme nous venons de le voir, certains problèmes tels que celui de la confidentialité. L'absence de confidentialité ne constitue cependant pas, en elle-même un risque. De nombreuses activités ne sont pas confidentielles et cela ne prête pas à conséquence. C'est uniquement du fait de certaines pratiques telles que le transfert d'informations considérées comme sensibles et de l'existence de tiers potentiellement mal intentionnés que cette caractéristique d'Internet se transforme en source de risque pour ses utilisateurs. Une personne se contentant d'utiliser son courrier électronique pour envoyer des messages anodins ne court guère de risque même en l'absence de confidentialité. C'est donc uniquement dans un cadre collectif qu'intervient la notion de sécurité et que se mettent en place des systèmes de sécurité, qui correspondent au mode d'utilisation de ces moyens de protection par un groupe partageant une définition commune des risques et donc des pratiques nécessaires pour les réduire. Il s'agit d'un système artificiel, au sens où l'entend Herbert Simon, visant à la satisfaction d'un objectif : atteindre ce qui est considéré comme la sécurité, en mobilisant des technologies selon des procédures organisées (SIMON, 1969).

Un moyen de protection garantit un niveau de sécurité évaluable de façon relativement objective. Ainsi, il est possible de calculer, en fonction de la longueur de la clef, le temps nécessaire pour la découvrir par essais successifs. Il n'en va pas de même pour les systèmes de sécurité qui renvoient quant à eux, à des définitions collectives du risque, parfois antinomiques. Pour utiliser une comparaison en dehors du domaine de l'acheminement de l'information, la résistance d'une porte et de sa serrure peut être évaluée, elles sont plus ou moins fragiles. Il existe donc de bonnes portes et de mauvaises portes. Il n'en va pas de même pour leur utilisation. Aucune considération technique n'apporte en effet de solution à la question de la détention des clefs. De nombreuses personnes choisissent par exemple de laisser un double de leur trousseau à un tiers. Cela implique qu'elles aient une confiance très élevée en celui-ci. En agissant de la sorte, elles multiplient les chances de voir leurs clefs tomber entre de mauvaises mains, mais elles s'assurent en même temps contre les conséquences de la perte de leurs clefs. Il n'existe pas en la matière de choix optimal. La réponse dépend en fait de la conception que chacun se fait des risques potentiels et de leur probabilité d'occurrence ; de là, découleront les pratiques d'utilisation des technologies de protection, qui relèvent d'une ingénierie technique, mais aussi humaine. L'agencement de technologies de protection et de pratiques d'utilisation en vue de réduire ce qui apparaît comme un risque constitue ce qu'il est possible de nommer un système de sécurité.

Dans le cadre de la sécurisation des échanges d'information, au sein d'un réseau informatique, s'opposent deux modes d'organisation de ces systèmes, que nous construisons ici comme des types idéaux. Le premier mode vise avant tout à protéger les utilisateurs à titre individuel contre l'action des tiers. À ce titre, l'individu est le premier responsable de sa sécurité. Une large part de cette dernière repose donc sur la capacité de chacun à maintenir certains éléments cruciaux du système de sécurité hors de portée de tiers, quels qu'ils soient. Ils représentent en effet

le risque principal soit directement, soit parce que la transmission et la conservation de certains éléments augmentent les risques d'action de tiers réellement malveillants, le tout sans possibilité de contrôle. À l'opposé, se trouve une conception où la sécurité des individus est assurée dans la mesure où elle contribue à la sécurité collective. Dans cette optique, le niveau de sécurité individuelle peut être réduit pour garantir une sécurité collective plus élevée, notamment si certains individus sont soupçonnés de menacer la collectivité.

Cette deuxième approche est défendue par certains États, dont la France, pour laquelle l'usage de la cryptographie en tant que technologie de protection ne doit pas entraîner une perte de la capacité des pouvoirs publics à contrôler les flux d'information. Mais ils ne sont pas les seuls, la sécurisation des réseaux d'entreprises pose des problèmes du même ordre pour une collectivité plus réduite (DENNING, BRANSTAD, 1996 ; RAVI, 1996). En effet, la protection des informations y est assurée avant tout pour préserver les intérêts de l'entreprise et non le respect de la vie privée. La cryptographie pose donc dans ce cadre autant de problèmes qu'elle en résout, puisqu'elle assure la protection de l'information contre les tiers, mais retire à la direction d'une entreprise ou à un État, toute capacité d'y accéder, ce qui peut être particulièrement grave en cas de perte des clefs.

Dès les premières réflexions sur la cryptographie asymétrique, ce problème est apparu central (NEEDHAM, SCHROEDER, 1978). Ces technologies assurent, en effet, un niveau de protection individuel maximum, cependant certains tiers, la direction d'une entreprise ou un État, peuvent revendiquer la possibilité d'accéder à l'information, au nom de la sécurité collective. Il est nécessaire pour cela que la résistance du système de sécurité soit réduit au bénéfice du seul tiers légitime ou s'estimant comme tel. Concrètement, cela peut être réalisé en agissant directement sur la technologie. Ce qui implique un affaiblissement de l'algorithme ou une réduction de la taille des clefs, à un niveau juste suffisant pour casser le cryptage. Ce choix a été retenu lors de la création du DES. La loi française utili-

se partiellement cette possibilité puisque l'usage de logiciels utilisant des clefs de moins de 40 bits, facilement cassables, est soumis à un régime très assoupli. Cependant, le transfert d'informations sensibles se satisfait très mal d'un tel affaiblissement. Le système du dépôt des clefs privées, retenu dans le cas de la cryptographie asymétrique, ne vise donc pas à affaiblir la technologie de protection mais à organiser le système de sécurité de telle sorte que les clefs privées soient accessibles pour un tiers capable d'imposer un tel système<sup>1</sup>. Il introduit donc autoritairement un tiers de confiance, auprès duquel les clefs privées sont déposées. La grande difficulté réside naturellement dans la capacité à imposer une telle organisation du système de sécurité. Au sein d'une entreprise les usages peuvent être relativement facilement contrôlés, il n'en va pas de même au niveau d'un État.

#### UNE CRYPTOLOGIE D'ÉTAT : LE TIERS DE CONFIANCE EN FRANCE

Le gouvernement américain est le premier à avoir élaboré ce type de régulation de l'usage de la cryptographie. En 1994, sur proposition de la NSA, il tenta d'imposer un système de cryptographie pour les communications numériques utilisant le principe du dépôt des clefs<sup>2</sup>. Comme il paraissait évident que cela ne saurait se faire sur un mode totalement volontariste, il fallut trouver une solution pour imposer le dépôt des clefs. La solution qui fut alors envisagée reposait sur la mise à disposition par le gouvernement d'une puce spéciale, la puce *clipper*, intégrée dans les équipements de télécommunication et assurant le cryptage<sup>3</sup>. Partant du principe qu'il était beaucoup plus facile de convaincre les producteurs d'ordinateurs que l'ensemble de leurs utilisateurs, le gouvernement tenta d'encourager l'utilisation de *clipper* en rendant son usage obligatoire pour toute personne traitant avec l'État. Ainsi, plus besoin de collecter a posteriori les clefs, celles-ci étaient en fait indirectement fournies par une agence gouvernementale qui avait tout loisir d'en garder un double. Cette solution fut rejetée par le Sénat. La puce *clipper* apparut en effet

••••(1) Plusieurs expressions désignent des types de système de sécurité extrêmement proches : *key recovery* ; *trusted third party* ; *key escrow*.

••••(2) La Maison Blanche présenta ce projet comme un « projet volontaire visant à renforcer la sécurité et le caractère privé des communications téléphoniques, tout en offrant la possibilité de veiller au respect de la loi ».

••••(3) Le chiffrement des données informatiques devait quant à lui être assuré par la carte Fortezza. L'algorithme utilisé dans les deux cas fut baptisé *Skypjack* et ne reposait pas totalement sur le principe de la cryptographie asymétrique.

comme une forme de contrôle par trop totalitaire, malgré l'absence d'obligation formelle d'utilisation. Les rapprochements avec le Big Brother de George Orwell étaient faciles à faire. En introduisant un élément physique directement sous contrôle du gouvernement dans chaque moyen de communication, l'État s'introduisait physiquement dans la sphère privée. En outre, cela posait le problème plus concret du remplacement des puces en cas d'obsolescence et du surcoût généré par cet élément. Le projet fut donc abandonné aux États-Unis sous cette forme, mais l'idée d'un contrôle des clefs privées par le gouvernement demeure et l'administration Clinton tente régulièrement d'introduire une loi dans ce sens<sup>1</sup>. À ce jour, le seul exemple de mise en œuvre légale du système de dépôts des clefs privées est la loi française du 26 juillet 1996.

••••(1) *L'Electronic Frontier Foundation (EFF) et l'EPIC jouèrent un rôle important de sensibilisation dans le cadre du débat qui accompagna ce projet. Il est possible de suivre son évolution et son histoire sur les sites : [www.eff.org](http://www.eff.org) / [www.epic.org](http://www.epic.org).*

Jusqu'en 1990 la cryptographie est demeurée soumise en France au décret-loi du 18 avril 1939 relatif aux matériels de guerre de seconde catégorie qui correspondent aux «*matériels destinés à porter ou à utiliser au combat des armes à feu*». Cette réglementation se traduisait par un régime strict d'autorisation pour sa production, sa diffusion et son usage<sup>2</sup>. Elle était donc à cette date complètement obsolète tant au regard des nouveaux usages de la cryptographie qu'au regard de l'article 233 du traité de Rome, qui n'autorise pas les mesures de protection pour «*les produits non destinés à des fins spécifiquement militaires*». La réforme de 1990 fut menée dans le cadre de la refonte de la réglementation sur les télécommunications, ce qui, en soi, constituait une prise en compte des évolutions en matière d'usage. La principale innovation fut l'introduction d'une distinction entre la cryptographie à des fins d'authentification et la cryptographie à des fins de confidentialité, la première n'étant soumise qu'à un régime de déclaration alors qu'une autorisation du Premier Ministre demeurait indispensable pour la seconde. Le principal point de débat porta alors sur la nécessité ou non de contrôler l'usage de celle-ci, qui fut finalement réintégré dans la loi.

••••(2) Pour une présentation plus détaillée de l'évolution de la législation française en matière de cryptographie, cf. BENSOUSSAN, 1996.

Relevant désormais de la réglementation des télécommunications, la législation s'appliquant à la cryptographie fut modifiée en 1996 à l'occasion des bouleverse-

ments provoqués par la privatisation de France Telecom et la déréglementation du secteur. Les textes préparatoires révèlent une importante prise de conscience quant à l'importance de cette technologie pour le développement notamment du commerce électronique<sup>1</sup>. Le texte final précise ainsi à l'article 17 que le deuxième alinéa de la loi du 29 décembre 1990 est modifié comme suit « *pour préserver les intérêts de la Défense nationale et de la sécurité intérieure ou extérieure de l'État, tout en permettant la protection des informations et le développement des communications et transactions sécurisées* ». La sécurité collective demeure donc l'objectif prioritaire de la législation française, cependant les besoins en matière de sécurité privée sur les réseaux ont été pris en compte. Le texte tente de réaliser un compromis. La protection de la confidentialité des communications n'a cependant guère été mise en avant à l'époque. Outre une certaine méfiance à l'égard d'Internet lors des débats, l'idée qui domine est tout simplement que la confidentialité des correspondances et des données informatiques est déjà garantie par le code postal et par la loi *Informatique et Libertés*<sup>2</sup>.

La distinction entre confidentialité et authentification est maintenue. Seule la première demeure soumise à l'autorisation préalable, accordée par le Service central de sécurité des systèmes d'informations (SCSSI). En outre, au terme du décret d'application n°98-101, la cryptographie faible, dont les clés sont inférieures à 40 bits et l'algorithme connu, se voit dispensée des formalités d'autorisation. L'usage ou la fourniture des autres moyens ou prestations permettant d'assurer la confidentialité par cryptographie forte demeurent quant à eux soumis au principe d'autorisation préalable. Il en va de même pour leur importation et leur exportation en direction de pays n'appartenant pas à l'Union européenne. La principale innovation réside dans la mise en place du système des tiers de confiance.

Afin de garantir une diffusion de la cryptographie à des fins privées, l'État a en effet libéralisé son usage, à la condition que les procédés utilisés soient fournis et gérés directement ou indirectement par un tiers de confiance ayant

••••(1) Voir notamment  
GAILLARD, 1996.

••••(2) Voir notamment :  
*Journal Officiel, Question*,  
tome mai-juin 96, question  
de M. Bonnacarrère,  
p. 42060.  
*Journal Officiel, Question*,  
tome mai-juin 96, question  
de M. Terrot, p. 41777.  
*Journal Officiel, Question*,  
tome juillet-août 96, question  
de M. Broisier, p. 3614.

reçu l'autorisation du SCSSI. Ce tiers de confiance constitue l'élément central du dispositif créé par la loi du 26 juillet 1996. Son rôle est de fournir des procédés de cryptographie à ses clients, mais aussi de tenir à la disposition de la puissance publique leurs clefs privées. Il constitue donc un élément relativement inutile pour les utilisateurs, la conservation des clefs privées n'est pas indispensable pour le fonctionnement d'un système de sécurité utilisant la cryptographie asymétrique à grande échelle, à la différence de celles des clefs publiques. Par contre, il est indispensable pour l'État, si celui-ci désire conserver la possibilité d'accéder aux informations. Par cette loi, l'État a donc tenté de libéraliser l'usage de la cryptographie en gardant comme objectif prioritaire la sécurité collective. De ce fait, le cœur de la loi ne réside pas dans le contrôle des technologies utilisées mais dans l'encadrement de leur usage. Conscients de leur incapacité à interdire de telles technologies, les législateurs ont essayé d'en faciliter l'usage dans un cadre légal conforme à la préservation de la sécurité collective. Ils comptaient sur le caractère indispensable de la cryptographie asymétrique pour assurer la diffusion du système de tiers de confiance et créer ainsi un standard *de facto*, ce qui reprend l'idée de la puce *Clipper*. Ce projet fut cependant rapidement dénoncé comme une fausse libéralisation et fortement critiqué<sup>1</sup>.

•••(1) Le principal support de cette contestation est naturellement Internet, on consultera par exemple les sites :  
[www.pasteur.fr/other/rfc/19xx/1984](http://www.pasteur.fr/other/rfc/19xx/1984).  
[www.planete.net/~jbaa-goe/loi\\_crypto.html](http://www.planete.net/~jbaa-goe/loi_crypto.html).  
[194.51.213.11/lij/cryptoTC.htm](http://194.51.213.11/lij/cryptoTC.htm).  
[www.censure.org/cryptographie/crypto1.htm](http://www.censure.org/cryptographie/crypto1.htm).

**QUELLE PLACE POUR LE CONTRÔLE DE L'ÉTAT ?**

Imposer un contrôle des modalités d'usage de la cryptographie à clefs publiques ne peut être réalisé que par une autorité disposant d'une forte légitimité ou d'un pouvoir de coercition extraordinaire. La direction d'une entreprise dispose en théorie d'un tel pouvoir, dans la mesure où elle peut définir les logiciels utilisés et leur mode d'utilisation en commun. Pour un État démocratique, il n'en va pas de même. Il est nécessaire que les utilisateurs de moyens de cryptographie s'accordent sur sa légitimité à mettre en œuvre un tel encadrement de l'usage pour qu'il devienne une réalité. Il est en effet impossible dans les faits d'obliger les individus à utiliser des logiciels produits par des sociétés se pliant à la loi française, alors qu'un programme

---

Tiers de confiance ou de défiance ?

comme PGP est disponible partout sur Internet. C'est cette légitimité qui est aujourd'hui mise en cause par les détracteurs de la législation française.

On peut distinguer deux types de critiques, qui se trouvent souvent imbriquées, mais relèvent pourtant de logiques totalement différentes. L'une porte sur le principe même de ce type de contrôle, l'autre sur sa faisabilité.

#### L'EXPRESSION DE NOUVELLES FORMES DE LIBERTARISME

Les critiques portant sur le fondement du contrôle par l'État des procédés de cryptographie repose sur une théorie commune. Le contrôle de l'État est à titre individuel potentiellement plus dangereux que les usages criminels d'Internet. On retrouve là une conception individuelle de la sécurité, qui vise avant tout à réduire des risques directs pour la personne physique ou morale. Par extension, la sécurité peut être étendue à un groupe choisi sur un mode volontaire, celui des correspondants, mais ce groupe ne possède aucune forme de contrôle central. Chacun assure sa sécurité et ce faisant la sécurité collective est garantie. La confiance dans cette optique ne va donc pas vers l'État mais vers les autres utilisateurs qui ne sauraient représenter une menace directe.

Cette vision poussée à l'extrême aboutit à une forme d'anarchisme<sup>1</sup>. L'État y est rejeté d'autant plus facilement que, dans un espace immatériel comme Internet, la coercition par la force physique apparaît inutile, chacun pouvant y assurer sa sécurité par des moyens techniques. Ce type de critique est important aux États-Unis. Il trouve naturellement son fondement dans le premier amendement de la Constitution, qui garantit la liberté d'expression et d'association. Mais surtout dans le quatrième et le cinquième amendements qui protègent les citoyens contre les investigations secrètes et les aveux contraints (BARLOW, 1993). Ces amendements qui trouvent leur origine dans un profond mouvement anti-fédéraliste, assurent la défense des individus face à l'État fédéral. On retrouve ici l'opposition entre sécurité collective et sécurité individuelle qui se pose d'ailleurs aux États-Unis sous d'autres formes, notamment celle du débat sur la vente et la détention des armes à feu.

••••(1) La « déclaration d'indépendance du cybermonde » prononcée le 8 février 1996 à Davos par Perry Barlow, président de l'EFF, illustre parfaitement cette idéologie.  
Disponible sur Internet <http://www.eff.org/~barlow>.



••••(1) La faiblesse du contrôle en matière de protection de la vie privée aux États-Unis en constitue certainement un autre.

••••(2) Il est intéressant de noter à cet égard que Stéphane Borzmeier figure tutélaire d'Internet en France et qui fut l'un des premiers à rendre public le débat sur la cryptographie en France, fut l'une des victimes des écoutes de l'Élysée. Parmi ses nombreuses interventions, voir notamment BORZMEIER, 1996.

••••(3) La NSA dispose aujourd'hui d'un site sur Internet : [www.nsa.gov:8080](http://www.nsa.gov:8080).

La France est beaucoup moins marquée par ce type d'opposition à l'État central, c'est là certainement une des raisons expliquant la faible audience de ce type d'arguments<sup>1</sup>. Dans ce pays, la dénonciation de la légitimité de la détention des clefs privées par la puissance publique repose sur des bases nettement moins radicales. Elle pose en fait la question du contrôle des institutions de contrôle au sein d'une démocratie. La critique se fait donc au nom de la démocratie et du respect de ses lois actuelles et non au nom d'un certain libetarisme aboutissant à une forme de communautarisme. Ce n'est donc pas le principe du contrôle qui est mis en cause mais sa dangerosité dans les faits. Tout contrôle est en effet exercé au nom de l'intérêt collectif par des hommes détenteurs à ce titre du monopole de la puissance publique ; or, si le principe n'est pas contestable, il pose inmanquablement le problème de son détournement pour le seul profit d'intérêts non collectifs. L'affaire des écoutes de l'Élysée a sur ce point créé un précédent largement mis en avant par certains détracteurs du contrôle par l'État<sup>2</sup>.

De par ses caractéristiques techniques, Internet permet la mise en œuvre d'écoutes à grande échelle, automatisées, difficilement décelables et peu coûteuses. Dans ces conditions, le moindre doute sur les intentions de l'État ou de ceux qui agissent en son nom constitue un risque insupportable. Ces doutes peuvent se situer à différents niveaux. Tout d'abord, les administrations des services du chiffre ne constituent pas des modèles de transparence et de contrôle démocratique. Ainsi la NSA a du mal à faire oublier sa non inscription au budget de l'État américain pendant des décennies et ce malgré une politique aujourd'hui résolument tournée vers la communication institutionnelle<sup>3</sup>. De même, en France, le SCSSI, par l'opacité de ses modes de fonctionnement, perpétue l'image d'une institution mue par des intérêts autres que la seule défense de l'intérêt collectif. Cependant, les soupçons ne portent pas uniquement sur la garantie de la vie privée. L'espionnage industriel a pris une importance nouvelle depuis la fin de la guerre froide ; or, celui-ci n'est pas le seul fait des entreprises, les services d'espionnage et du chiffre y contribuent activement.

*Tiers de confiance ou de défiance ?*

Dans ces conditions, rien ne garantit à une entreprise étrangère que ses communications ne sont pas espionnées en dehors de tout besoin légitimé par la sécurité nationale. L'émotion suscitée par le projet américain Échelon a permis de mettre au grand jour certaines de ces pratiques et de raviver les craintes de telles déviations au sein des systèmes de sécurité reposant sur l'usage de tiers de confiance (MURRAY, 1992).

La mise en cause de la légitimité de l'État, ou de ceux qui agissent en son nom, à contrôler les flux d'informations constituent une critique radicale du système des tiers de confiance, cependant elle n'est pas la seule. Un autre type de critiques porte sur la possibilité de mise en œuvre d'un tel système. Refusant de se positionner au niveau d'un débat de nature politique, il vise à établir une remise en cause fondée sur des critères objectifs. Il s'appuie sur une évaluation des risques induite par une législation imposant le dépôt de clefs privées au regard de ses objectifs.

#### LA DÉNONCIATION DES RISQUES INDUITS PAR LE SYSTÈME DES TIERS DE CONFIANCE

Face au développement d'appels à la mise en place de système de dépôt des clefs privées, un certain nombre de spécialistes de la cryptographie sont intervenus pour mettre en lumière les faiblesses et les coûts d'un tel contrôle. La présentation la plus complète et la plus claire de ces arguments se trouve dans les deux rapports de 1997 et 1998, *the Risks of key recovery, key escrow, trusted third party and encryption*, rédigés par un groupe de onze spécialistes mondialement reconnus en matière de cryptographie<sup>1</sup>. Les arguments utilisés sont complexes et relativement techniques, nous n'en ferons dans le cadre de cet article qu'une présentation résumée. Les principaux arguments allant à l'encontre d'un dépôt des clefs privées sous contrôle de l'État peuvent être regroupés en quatre catégories.

L'État, en imposant un dépôt des clefs privées, introduit de nouveaux risques dans un système de sécurité destiné avant tout à assurer la sécurité des communications privées. Le simple fait de collecter les clefs privées et de les

••••(1) Ces rapports sont disponibles sur Internet : [www.cdt.org/crypto/risks98/](http://www.cdt.org/crypto/risks98/).

stocker contribue en effet à constituer des points sensibles dont l'attaque serait particulièrement profitable. De fait certains problèmes que la cryptographie asymétrique vise justement à résoudre sont réintroduits comme par exemple le transport des clefs. En outre, les utilisateurs possèdent peu de moyens pour évaluer la qualité de la sécurité offerte par les instruments de cryptage disponibles sur le marché. Dans le cadre de la loi française, le SCSSI qui accorde les agréments, est le seul juge de la puissance des technologies et des procédures utilisées. L'utilisateur doit se contenter de lui faire confiance quant à la qualité des prestations. Les décrets n° 98-101 et 98-102 du 24 février 1998 fixant les conditions d'agrément des tiers de confiance apportent fort peu de précision sur les obligations contractuelles à l'égard des particuliers en matière de respect de la confidentialité et sur les moyens techniques devant être mis en œuvre. La seule précision porte sur la nécessité d'un engagement relatif à la sécurité des conventions, engagement dont la portée n'est pas précisée. De même, les modalités de remise des clefs privées aux autorités seront fournies dans une annexe classifiée. Ce type de réglementation va ainsi à l'encontre des habitudes de la communauté des spécialistes civils de la cryptographie pour lesquels le secret des procédures constitue plus une source de risque qu'un surplus de sécurité, dans la mesure où il limite les possibilités d'évaluation par la communauté scientifique.

Le principe de l'agrément national des technologies n'est pas compatible avec un usage au sein d'un réseau global et technologiquement instable. En imposant une procédure lourde et nécessairement longue, le législateur fait courir à ces technologies un important risque d'obsolescence. En outre, il est peu probable que l'ensemble des utilisateurs d'Internet adoptent les technologies ayant reçu l'agrément du SCSSI. Il faudra donc que celles-ci soient compatibles notamment en ce qui concerne le dépôt des clefs privées avec les systèmes de sécurité étrangers, c'est là un deuxième sujet d'interrogation. Cette compatibilité sera d'autant plus délicate à assurer qu'il sera difficile de suivre l'évolution technique tout en respectant la procédure d'agrément.

Le risque serait donc réel de voir émerger un système hexagonal ne permettant pas aux particuliers et aux entreprises de communiquer dans des conditions d'égalité avec le reste du monde.

Le système du dépôt des clefs privées tend à s'immiscer dans les procédures d'utilisation des technologies de cryptage à clef publique sans pour autant faire de distinction entre authentification et confidentialité. Tout d'abord, le dépôt des clefs privées tend à être associé abusivement au dépôt des clefs publiques auprès d'un tiers certificateur, ce qui entretient une ambiguïté préjudiciable. Au sein d'un système de sécurité utilisant la cryptographie à clefs publiques, il est en effet utile de recourir à un tiers auprès duquel les clefs publiques, et uniquement celles-ci, sont déposées. Cette procédure permet d'en centraliser la distribution, mais aussi d'authentifier l'identité des personnes associées aux clefs. La cryptographie asymétrique n'empêche pas, en effet, l'usurpation d'identité lors de la création du couple de clefs. Ce tiers certificateur est donc souvent nécessaire mais il ne doit pas être assimilé au tiers de dépôt de clefs privées. Dans le même ordre d'idées, le dépôt des clefs privées, notamment dans la loi française, ne permet que difficilement de différencier authentification et confidentialité<sup>1</sup>. Or, si la seconde peut en effet nuire à la sécurité collective en restreignant l'accès potentiel de la puissance publique à l'information, la seconde n'est qu'une forme de signature. L'authentification qui constitue une application indispensable pour les échanges d'informations au sein d'Internet est donc limitée par un cadre législatif dont les finalités lui sont totalement étrangères.

La mise en œuvre d'un système de sécurité incluant un dépôt des clefs privées a un coût risquant d'être important et dissuasif pour la diffusion de ces technologies. L'accès de la puissance publique aux informations cryptées est l'objectif de ce type d'organisation de l'usage. Or, pour qu'il satisfasse à ses objectifs, il faut que la récupération des clefs et le déchiffrement soient rapides, ce qui implique une organisation lourde, centralisée, fonctionnant de manière permanente. Tout cela nécessite des hommes et du matériel et a donc un coût qui s'ajoute à celui de la fabrication

••••(1) La loi française reconnaît cette différence depuis 1990.

L'authentification est même totalement libéralisée par la loi de 1996. Cependant la portée de cette disposition reste limitée dans la mesure où la plupart des logiciels de chiffrement, dont le célèbre PGP, assurent ces deux fonctions.

de la technologie. Contrairement aux systèmes de sécurité reposant sur une mise en œuvre par les utilisateurs finaux où le seul coût est lié à l'achat de la technologie, l'introduction d'intermédiaires implique leur rémunération. Pour l'instant, nul ne peut encore préciser qui devra supporter ces coûts et la Commission européenne s'en est d'ailleurs inquiétée.

*L'évolution de la relation entre sécurité collective et individuelle*

Ces quatre éléments contribuent à faire apparaître le dépôt des clefs privées comme un système lourd, coûteux et potentiellement dangereux. Il menace en outre d'être en grande partie inefficace tant qu'il ne sera pas généralisé à l'ensemble des États, ce qui est peu probable. L'importance du coût rapporté à la faiblesse des gains potentiels en terme de sécurité collective suscite aujourd'hui d'importantes remises en cause du dépôt des clefs privées organisé en France. Celles-ci sont fondées principalement sur le constat de la difficulté de sa mise en œuvre et non sur un rejet d'un contrôle de l'État. Face au constat de la nécessité d'une réelle sécurité au sein d'Internet et de l'importance pour ce faire de la cryptographie à clef publique, de nombreux rapports ont attiré l'attention directement ou indirectement sur les problèmes posés par la loi française.<sup>1</sup> Ces arguments ont eu une large audience auprès des utilisateurs mais aussi des pouvoirs publics, confrontés par ailleurs aux difficultés de mise en œuvre du système des tiers de confiance. La Commission Interministérielle pour la Société de l'Information (CISI) a ainsi publié le 19 janvier 1999 un appel à la libéralisation complète de l'usage de la cryptographie en France reprenant en grande partie ce type d'argumentaire. Toutefois, de telles déclarations malgré leur caractère consensuel, essayant elles aussi de concilier sécurité collective et privée, masquent un débat profond sur la définition des relations les unissant. La législation française actuelle trouve en effet ses origines dans une conception sécuritaire du rôle de l'État. Le but premier est d'assurer la sécurité collective, il s'agit d'un

••••(1) Commission européenne, 1997 ; OCDE, 1997 ; ART, 1997 ; Conseil de L'Europe, 1997.

objectif qui prime sur tout autre. Le système des tiers de confiance tente ainsi de maintenir cet objectif tout en reconnaissant l'importance de la sécurité privée. De leur côté, les propositions se fondant sur une étude des risques induits par la sécurité collective sur la sécurité privée, reposent-elles sur une hiérarchisation inverse. La sécurité collective est un objectif qu'il est nécessaire de prendre en compte dans le cadre d'un système qui vise avant tout à assurer la sécurité privée.

Au-delà des déclarations de principe reconnaissant l'importance de la préservation d'un contrôle étatique, aucune solution concrète pour garantir la préservation des deux objectifs n'est aujourd'hui proposée par les tenants d'une approche privilégiant la sécurité privée. Ce revirement en matière de définition des priorités au niveau de l'État entraîne donc, en l'état actuel des technologies, un affaiblissement notable de ses capacités de contrôle des flux d'informations numériques. Naturellement, celui-ci était déjà patent. Cependant, sa reconnaissance par les pouvoirs publics sous la forme d'une acceptation de l'inutilité voire de la dangerosité de son intervention dans un système de sécurité privée aboutit, nous semble-t-il, à une modification de la relation unissant sécurité privée et collective au sein des espaces virtuels. La notion de sécurité collective y devient uniquement une résultante de la sécurité privée, elle n'en est plus la source. Cela aboutit à la mise en place de systèmes de sécurité où chacun se protège en recourant à des technologies et services privés de sécurisation et où le contrôle par la puissance publique tend à perdre de sa légitimité faute d'un caractère de nécessité. Ainsi, les problèmes soulevés par l'utilisation de la cryptographie asymétrique contribuent à poser aujourd'hui la question de la place et des prérogatives de l'État au sein des réseaux informatiques et plus particulièrement d'Internet.

■ **Gaël BOISSEAU**

*Formateur Internet HEC-CNFPT*

- AUTORITÉ DE RÉGULATION DES TÉLÉCOMMUNICATIONS, 1998, avis du 8 octobre 1997, Paris, *Journal Officiel*, 28 février.
- BARLOW (J. P.), 1993, « A plain text on crypto policy », *Communication of the ACM*, vol. 36, n°11, nov.
- BAMFORD (J.), 1982, *The Puzzle Palace : a Report on America's Most Secret Agency*, Boston, Houghton Mifflin.
- BECK (U.), 1997, « Le concept de société du risque », *Risques*, n°32, octobre-décembre.
- BENSOUSSAN (L.) (dir.), 1996, *Les télécoms et le droit*, Paris, Hermes.
- BORZMEYER (S.), 1996, in LAFFITTE (P.), *Rapport sur la France et la Société de l'information, un cri d'alarme et une croisade nécessaire*, Tome II. Paris, La documentation française.
- BRANDSTADT (D.), 1987, « Considerations for security in the OSI Architecture », *IEEE network Magazine*, vol. 1, avril.
- CAMP (J. L.), SIRBU (M.), 1997, « Critical Issues in Internet Commerce », *IEEE Communication Magazine*, mai.
- COMMISSION EUROPÉENNE, 1997, *Assurer la sécurité et la confiance dans la communication électronique*, 8 octobre.
- CONSEIL DE L'EUROPE, 1997, *Recommandation du Conseil relative aux lignes directrices régissant la politique de cryptographie*, 27 mars.
- DAM (K.), LIN (H.), (dir.), 1996, *Cryptography's Role in securing the Information Society*, Washington D.C., National Academy Press.
- DEFFIE (W.), HELLMAN (M.E), 1976, « New Direction in cryptography », *IEEE Transaction on Information Theory*, vol. 22, p. 524-543.
- DENNING (D.), BRANSTAD (D.A.), 1996, « A taxonomy for key-escrow encryption systems », *Communications of the ACM*, vol. 39, n°3, mars.
- GAILLARD (C.), 1996, Rapport fait au nom de la commission production et des échanges sur le projet de réglementation des télécommunications, Paris, *Assemblée nationale*, 6 mai, n°2750.
- GARFINKEL (S.), 1995, *PGP, Pretty Good Privacy*, Paris, O'Reilly International Thomson.
- HUITEMA (C.), 1995, *Le routage IP*, Paris, Eyrolles.
- GILBERT (C.), 1998, « Le sens caché des risques collectifs », *La recherche*, n°307, mars.
- KAHN (D.), 1996, *The Codebreakers : The Comprehensive History of Secret Communication from Ancient Times to the Internet*, New York, Scribner (édition originale 1972).
- KAMATA (H.), PETERS (T.), 1997, « A consensus on cryptography », *The OECD Observer*, n°207, août-sept.
- KERCKHOFFS (A.), 1883, « La cryptographie militaire », *Journal des sciences militaires*, vol. IX, janvier.
- INTERNATIONAL INSTITUTE OF COMMUNICATION SPÉCIAL REPORT, 1996, *Digital Signatures and Cryptography: Trusted Keys to secur Electronic commerce ?*, vol. 26, n°6, décembre.
- MCHUGH (J.), 1997, « Politics for the really cool », *Forbes*, 8 septembre, p. 172-179.
- MURRAY (W. H.), 1992, « Who holds the Keys », *Communications of the ACM*, vol. 35 n°7, juillet.
- NEEDHAM (R.M.), SCHROEDER (M. D.), 1978, « Using encryption for authentication in large networks », *Communication of the ACM*, vol. 21 n°12, décembre.
- OCDE, 1997, *The OECD cryptography guidelines and report on background and issues of cryptography policy*, mars.
- RAVI (G.), 1996, « the Yaksha System », *Communication of the ACM*, Vol. 39, n°3, mars.
- RIVEST (R.), SHAMIR (A.), ADELMAN (L.), 1978, « A Method for Obtaining Digital Signatures and Public key Cryptosystems. », *Communications of the ACM*, vol. 21, n°2, février.
- SCHNEIER (B.), 1994, *Applied Cryptography : Protocols, Algorithms and Source, Code in C*, New York, Wiley et Sons.





# INTERNET ET LE DROIT À LA SÉCURITÉ

L'expérience actuelle de liberté totale sur l'Internet est-elle la marque d'une révolution encore mal comprise ou d'une impossibilité à fixer un cadre juridique standard dans un contexte mondialisé ? Pour le Conseil d'État qui a rendu son rapport au premier ministre en juillet dernier, il n'est nul besoin d'appliquer au réseau des réseaux un droit sectoriel spécifique et c'est au contraire le type de service en cause (messagerie, activité commerciale, etc.) qui doit déterminer le régime juridique applicable. Les conclusions de la Commission européenne sont proches, avec toutefois un complément intéressant sur le statut futur des fournisseurs d'accès et l'obligation de territorialisation des sites.

## INTERNET ET LES RÉSEAUX NUMÉRIQUES

CONSEIL D'ÉTAT

Le Premier Ministre a demandé au Conseil d'État, en septembre 1997, d'analyser les questions juridiques liées au développement d'Internet et des réseaux et de mettre en lumière les adaptations nécessaires, au plan national et international. Les propositions devaient, « tout en assurant la liberté de communication, permettre de lutter efficacement contre les dévoiements auxquels Internet peut donner lieu ». Cette commande s'inscrivait dans le cadre du programme de travail visant à faire entrer la France dans la société de l'information, annoncé à Hourtin en août 1997 et confirmé en janvier 1998. Un rapport<sup>1</sup> d'étape a été remis au Premier ministre au mois de mars 1998.

Pendant les huit mois de son travail, la démarche du Conseil d'État s'est voulue pragmatique et concrète, s'ap-

•••(1) Le rapport est publié à la Documentation française (266 pages) et disponible sur Internet sur le site <http://www.internet.gouv.fr/français/textes-ref/rapce98/accueil.htm>.

puyant sur l'expérience des professionnels, qui ont été largement consultés tant en France qu'à l'étranger. Le souci a toujours été de privilégier le conseil au Gouvernement, à la fois juridique et stratégique, plutôt que de proposer un état des lieux exhaustif sur les enjeux juridiques de l'Internet. La priorité du Conseil d'État a été de donner au Gouvernement les éléments d'analyse pour l'aider à définir les positions françaises sur les sujets les plus urgents de l'actualité internationale. À ce titre, le groupe de travail a d'ailleurs été consulté, en cours d'étude, sur la signature électronique, la gestion internationale des adresses Internet (noms de domaines), et les incidences réglementaires de la convergence entre l'informatique, l'audiovisuel et les télécommunications.

## LE CONTEXTE

Ce rapport s'inscrit dans le cadre de négociations internationales très actives, menées pour le moment dans une large mesure à l'initiative des États-Unis et qui se déclinent dans les grandes enceintes internationales (OCDE, Conseil de l'Europe, OMC, OMPI, CNUDCI, etc.). Ces négociations risquent de structurer définitivement les usages et les comportements sur les réseaux numériques. Il importe dès lors de permettre à la France et à l'Union européenne de participer activement à ce débat mondial, faute de quoi il sera trop tard, ensuite, pour défendre une conception différente de la personne ou du consommateur, et pour établir sur les réseaux un « État de droit » conforme à nos valeurs.

Évidemment, cette émergence du raisonnement juridique dans le monde d'Internet, qui s'est nourri jusqu'à présent de liberté - et ceci avec succès - peut surprendre. Mais à l'heure où Internet devient un phénomène « grand public » reliant plus de cent millions de personnes dans le monde, il est légitime de s'interroger sur le mode de fixation des règles de ce nouvel espace. Les réponses ne peuvent plus être celles d'un petit nombre de spécialistes mais doivent faire l'objet d'un réel débat démocratique entre l'ensemble des acteurs, publics et privés. L'enjeu est en effet essentiel : il faut accompagner le dynamisme des

- Mettre en place un dispositif de coordination interministérielle des positions françaises dans les négociations internationales concernant Internet et les réseaux numériques et instituer un dispositif de veille et d'observation juridiques des réseaux numériques.

*Protéger les données personnelles et la vie privée*

- Adapter et renforcer le rôle de la CNIL (suivi des procédés d'auto-régulation, contrôle a posteriori des pratiques des acteurs).

- Élaborer un accord international fixant des principes déontologiques communs pour la collecte et l'utilisation des données personnelles.

*Commerce électronique : Favoriser les échanges par une confiance accrue des acteurs*

- Mieux protéger le consommateur par une clarification du régime juridique de la transaction électronique, une meilleure information et une adaptation de la loi du 4 août 1994 sur l'emploi de la langue française.

- Définir dans une convention internationale un socle minimal de principes relatifs à la protection du consommateur.

- Reconnaître dans le code civil la valeur juridique du document et de la signature électroniques.

- Libéraliser davantage l'usage des moyens de cryptologie.

- Adapter le régime de la TVA et de l'impôt sur les sociétés aux spécificités des réseaux numériques, et envisager de nouvelles modalités de recouvrement des taxes sur Internet.

- Adapter, dans un cadre international, le régime juridique du droit d'auteur, notamment en ce qui concerne les possibilités de « copie privée », en maintenant un haut niveau de protection des auteurs.

- Renforcer la lutte contre la contrefaçon sur les réseaux, par une coopération accrue des acteurs et par une adaptation de la procédure judiciaire.

*Lutter contre les contenus et les comportements illicites*

- Clarifier le régime de responsabilité des différents acteurs de l'Internet.

- Adapter la procédure judiciaire pour faciliter les poursuites et renforcer les pouvoirs du juge.

- Créer un pôle interministériel pour la criminalité de haute technologie.

- Renforcer et simplifier la coopération internationale en matière d'entraide judiciaire.

- Développer l'auto-régulation des acteurs par la création d'un organisme de « corégulation ».

*Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications*

- Maintenir la distinction entre le régime de la communication au public et celui de la correspondance privée.

- Adapter la réglementation de la communication pour tenir compte des effets de la convergence : maintenir une réglementation sectorielle pour les services offerts au public mais uniformiser progressivement les règles applicables aux différents réseaux de télécommunication.

- Définir par la loi un socle minimal d'obligations applicables à toute communication au public (protection des mineurs ; respect de la dignité humaine, de la vie privée, des données personnelles, de la propriété intellectuelle ; identification de la publicité comme telle, etc.).

acteurs privés en veillant à bâtir une nouvelle forme de «civilité», respectueuse de la personne humaine, car ce nouvel espace est porteur de nouvelles opportunités de croissance économique, d'échanges et de connaissances.

## PRINCIPALES CONCLUSIONS

Tout d'abord, le monde en réseau, même s'il s'est souvent bâti à l'écart du droit, n'est pas un espace de non-droit. L'ensemble de la législation existante a vocation à s'appliquer aux acteurs d'Internet, notamment les règles de protection de la vie privée et du consommateur et celles qui garantissent le respect de l'ordre public. Les réseaux constituent des espaces dans lesquels tout type d'activité peut être pratiqué dans le respect des règles de droit commun régissant un domaine particulier (publicité, fiscalité, propriété intellectuelle, etc.). Ainsi, il convient d'appliquer le *corpus* juridique existant, en l'adaptant le cas échéant, et il n'est nul besoin de créer un droit nouveau et sectoriel de l'Internet comme il en existe un par exemple pour l'audiovisuel. Peu importe, en effet, la technologie ou le réseau utilisés, c'est le type de service en cause (messagerie, activité commerciale, etc.) qui doit déterminer le régime juridique applicable.

La deuxième conclusion est que la «régulation», c'est-à-dire la capacité à mettre de l'ordre dans ces espaces en réseau, doit procéder d'une approche entièrement nouvelle : dans un monde international, hétérogène et décentralisé comme Internet, la réglementation d'origine étatique ne peut suffire. Elle doit nécessairement se combiner avec l'auto-régulation des acteurs, c'est-à-dire l'intervention de ceux-ci pour décliner les principes de la règle de droit dans des environnements non prévus par celle-ci ou pour en assurer préventivement le respect. Les États et les acteurs privés doivent donc collaborer dans des missions d'encadrement et de surveillance du réseau, afin d'assurer une lutte efficace contre les contenus illicites (délinquance, pédophilie, contrefaçon, etc.) et de veiller à la protection effective de la vie privée et des droits des consommateurs.

Enfin, il apparaît clairement qu'aucun pays ne peut résoudre seul les questions suscitées par le développement

des réseaux numériques. La coopération internationale est essentielle pour mener une action efficace d'impulsion et, lorsque cela s'avère nécessaire, de répression. Parmi les questions les plus urgentes qui doivent faire l'objet de conventions internationales, on peut notamment relever les problèmes de la protection des données personnelles, des droits du consommateur et de la signature électronique. De même, l'architecture générale de l'Internet, dont notamment les règles d'attribution des noms de domaine, doit être définie dans un cadre réellement international et non seulement américain comme c'est le cas actuellement. La coopération judiciaire internationale doit par ailleurs être renforcée sous peine de voir se développer des « paradis numériques » abritant les activités illicites.

La France doit donc, de façon urgente, définir des orientations stratégiques claires. Elle doit, pour cela, renforcer son dispositif de coordination interministérielle. La mise en place d'une cellule interministérielle dotée d'une forte légitimité et apte à faire travailler de concert administrations et acteurs privés paraît indispensable, si la France souhaite véritablement peser sur l'issue des négociations internationales en cours.

Au-delà de ces réflexions générales, cinq sujets ont fait l'objet d'une étude approfondie (voir sur ce point le résumé, ci-joint, des principales propositions), compte tenu de leur importance et de leur urgence : la protection des données personnelles et de la vie privée sur les réseaux, qui est l'un des sujets les plus sensibles aux yeux des utilisateurs.

Ces quelques remarques et le rapport lui-même ne prétendent pas épuiser l'analyse juridique des réseaux numériques. Certains sujets comme la fiscalité ou les « droits de la personne virtuelle » n'ont été que défrichés et devront faire l'objet de travaux complémentaires. En outre, dans un environnement en perpétuelle évolution, il est illusoire de vouloir proposer des réponses définitives. La réflexion ouverte par ce rapport n'est donc pas close et a vocation, dans le cadre d'une veille juridique régulière, à s'enrichir d'apports ultérieurs permettant de mieux adapter les règles de droit aux spécificités du monde en réseau.

■ **Isabelle Falque-Pierrotin**

*Maître des Requêtes*

## COMMERCE ÉLECTRONIQUE : ENFIN UN CADRE JURIDIQUE

COMMISSION EUROPÉENNE

La Commission vient de présenter une proposition de directive visant à la mise en place d'un cadre juridique cohérent pour le développement du commerce électronique dans le marché unique<sup>1</sup>. Grâce à la directive proposée, les prestataires de services de la société de l'information seront assurés de bénéficier de l'application des principes de libre prestation de services et de libre établissement qui sont à la base du marché unique et ils pourront offrir leurs services partout dans l'Union pour peu qu'ils respectent la législation de leur pays d'origine. Par service de la société de l'information, on entend tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un client. La directive proposée n'introduira des règles harmonisées spécifiques que dans les domaines où cela est strictement nécessaire pour faire en sorte que les entreprises et les citoyens puissent effectivement fournir et recevoir des services de la société de l'information dans toute l'Union, indépendamment des frontières. Ces domaines correspondent notamment aux questions suivantes : définition du lieu d'établissement des opérateurs, conclusion en ligne de contrats, responsabilité des intermédiaires, règlement des litiges et rôle des autorités nationales. Dans d'autres domaines, la directive s'appuiera sur les instruments communautaires existants en matière d'harmonisation ou de reconnaissance mutuelle des législations nationales. La directive ne s'appliquera qu'aux prestataires de services établis au sein de l'Union et non à ceux établis dans des pays tiers.

«*Le cadre juridique du marché unique, associé à la monnaie unique, offre à l'Union européenne une occasion unique de stimuler le développement du commerce électronique*» a déclaré M. Mario Monti, commissaire chargé du marché unique. «*Grâce au commerce électronique, le marché unique se dote d'une nouvelle dimension puisque les consommateurs bénéficieront désormais d'un accès*

•••(1) Les éléments ici présentés (IP/98/999) sont un résumé de la proposition de directives du parlement européen et du conseil relative à certains aspects juridique du commerce électronique dans le Marché intérieur. Cette proposition a été présentée à la Commission le 18/11/98. Nous remercions la Commission européenne de nous avoir autorisé à reproduire ce rédactionnel.

*plus aisé à des biens et services de meilleure qualité et meilleur marché. L'essor du commerce électronique permettra de stimuler les échanges, de promouvoir l'innovation et la compétitivité et de créer des emplois durables. L'objectif de la proposition est de faire en sorte que l'Union soit en mesure d'exploiter tous les avantages du commerce électronique : pour ce faire, elle entend renforcer la confiance des consommateurs et offrir aux opérateurs une sécurité juridique exempte de lourdeurs administratives excessives.»*

Au niveau mondial, les activités de commerce électronique connaissent une croissance exceptionnellement rapide puisque le volume de transactions pourrait atteindre 200 milliards d'écus en l'an 2000. En 1996, 86 millions de personnes étaient connectées à l'internet dans le monde, un chiffre qui devrait passer à 250 millions en l'an 2000. Dans l'Union, on estime que plus de 400 000 emplois liés à la société de l'information ont été créés entre 1995 et 1997 et que le quart des nouveaux emplois provient de ces activités.

#### CHAMP D'APPLICATION

La proposition de directive, que la Commission avait annoncée dans sa communication sur le commerce électronique d'avril 1997 (cf. IP/971313), couvre tous les services de la société de l'information, d'entreprise à entreprise ou d'entreprise à consommateurs, y compris les services fournis gratuitement aux destinataires (financés par la publicité ou le parrainage, par exemple), ainsi que les services autorisant des transactions électroniques en ligne comme le télé-achat interactif de biens et services et les galeries marchandes électroniques. À titre d'exemple des secteurs et activités couverts, on citera les journaux en ligne, les bases de données en ligne, les services financiers en ligne, les services professionnels en ligne (avocats, médecins, experts-comptables, agents immobiliers, etc.), les services de divertissement en ligne comme la vidéo à la demande, les services en ligne de publicité et de marketing direct et les services fournissant un accès à la « Toile mondiale » (*World Wide Web*).

Dans la proposition, le lieu d'établissement sera défini comme le lieu où se situe l'établissement stable à partir duquel l'opérateur exerce son activité économique, indépendamment de la localisation des sites Web ou des serveurs utilisés par cet opérateur ou de l'endroit où il dispose éventuellement d'une boîte postale. Cette définition est conforme aux principes consacrés par le traité CE (article 52) et à la jurisprudence de la Cour de justice. Elle permettrait de supprimer les incertitudes juridiques actuelles et d'assurer que les opérateurs ne peuvent contourner la surveillance prudentielle, puisqu'ils seraient soumis au contrôle des autorités prudentielles de l'État membre où ils sont établis. La proposition interdira aux États membres d'imposer, pour les services de la société de l'information, des régimes d'agrément spécifique qui ne seraient pas applicables à des services identiques fournis par d'autres moyens. Les États membres seront également tenus d'imposer aux prestataires de services de la société de l'information de mettre à la disposition de la clientèle et des autorités compétentes, de manière permanente et facilement accessible, des informations de base concernant leurs activités (nom, adresse, adresse électronique, numéro du registre commercial, agrément professionnel et appartenance à un organisme professionnel (le cas échéant), identification TVA).

#### CONCLUSION EN LIGNE DE CONTRATS

Pour que le commerce électronique se développe pleinement, la conclusion des contrats doit pouvoir se faire en ligne, sans être entravée par des règles qui ne seraient pas appropriées (par exemple l'obligation de rédiger les contrats sur support papier). La proposition obligera donc les États membres à revoir leur législation nationale pour en éliminer toute interdiction ou restriction pesant sur l'utilisation de moyens électroniques pour la conclusion de contrats. En outre, la proposition apportera une plus grande sécurité juridique en précisant, dans certains cas, le



moment de la conclusion du contrat, tout en respectant pleinement la liberté contractuelle. Ces propositions viendront compléter utilement la proposition de directive relative aux signatures électroniques (*cf.* IP/98/423).

#### RESPONSABILITÉ DES INTERMÉDIAIRES

Pour faciliter le commerce électronique, il y a lieu de préciser la responsabilité des prestataires de services en ligne pour ce qui est de la transmission et du stockage des informations appartenant à des tiers (ces prestataires agissant alors en qualité d'« intermédiaires »). Mais d'éliminer le flou juridique actuel et d'éviter que des approches divergentes ne se fassent jour au niveau des États membres, la proposition prévoit une dérogation pour les cas où ces intermédiaires ne jouent qu'un rôle passif de « simple canal » de l'information fournie par des tiers et elle limite également la responsabilité du prestataire de services pour les autres activités d'« intermédiaire » comme le stockage d'informations. La proposition recherche un équilibre prudent entre les différents intérêts en jeu, de manière à encourager la coopération entre les parties et, partant, de limiter le risque d'activités en ligne illicites.

#### COMMUNICATIONS COMMERCIALES

Les communications commerciales du type publicité et marketing direct, qui sont une composante essentielle de la plupart des services de commerce électronique seront soumises à des règles clairement définies par la directive. Ainsi, après avoir défini la notion de communications commerciales, la proposition soumet ces communications à certaines exigences de transparence, de manière à renforcer la confiance des consommateurs et à encourager des pratiques commerciales loyales. Afin de permettre aux consommateurs de réagir plus rapidement en cas d'ingérence préjudiciable, la proposition stipule que les communications commerciales effectuées par courrier électronique doivent être clairement identifiables. De plus, en ce qui concerne les professions réglementaires (telles que les

avocats ou les experts-comptables), elle pose le principe général selon lequel la prestation de services en ligne est autorisée et que les règles nationales en matière de publicité ne doivent pas empêcher les professionnels d'ouvrir des sites Web. Toutefois, ces professionnels seront tenus de respecter certaines règles de déontologie, lesquelles devront être intégrées aux codes de conduite élaborés par les organisations professionnelles de leur secteur.

#### MISE EN ŒUVRE

Plutôt que d'élaborer de nouvelles règles, la proposition s'efforcera d'assurer que les législations nationales existantes sont effectivement appliquées. Tout renforcement des mécanismes d'application de la réglementation favorise en effet la mise en place d'un véritable marché intérieur, fondé sur la confiance mutuelle entre États membres. Pour y parvenir, la proposition prévoit d'encourager l'élaboration de codes de conduite à l'échelle communautaire, de stimuler la coopération administrative entre les États membres et de favoriser la mise en place de nouveaux mécanismes efficaces de règlement des litiges transfrontaliers. En vertu de la proposition, les États membres seront également tenus d'instaurer des systèmes de recours juridique rapides et efficaces, adaptés à l'environnement en ligne, et de veiller à ce que les infractions aux règles établies en vertu de la directive soient sanctionnées de manière effective, proportionnée et dissuasive.

#### RECONNAISSANCE MUTUELLE, DÉROGATIONS

La directive proposée stipulera clairement que les principes du marché unique de reconnaissance mutuelle des législations nationales et de contrôle par le pays d'origine doivent être appliqués aux services de la société de l'information, de sorte que la prestation de tels services, lorsqu'ils sont fournis dans un autre État membre, ne soit pas entravée dans les domaines ou pour des motifs relevant du champ d'application de la proposition. Ce champ d'application ne s'étend pas à des domaines comme la fiscalité,

les données à caractère personnel (dont la libre circulation est organisée par la directive 95/46/CEE - *cf.* IP1981925), les activités des notaires, la représentation et la défense de clients devant un tribunal, ou les jeux de hasard. De plus, la directive proposée sera sans préjudice de l'application de la convention de Bruxelles sur la juridiction, la reconnaissance et l'application des jugements en matières civile et commerciale et la Convention de Rome relative au droit applicable aux obligations contractuelles.

La directive proposée autorisera également les États membres à imposer des restrictions, sur la base d'un examen au cas par cas, pour les services de la société de l'information fournis à partir d'un autre État membre, mais à condition que cela s'avère nécessaire à la protection de l'intérêt du public, par exemple pour des motifs comme la protection des mineurs, la lutte contre les discriminations basées sur la race, le sexe, la religion ou la nationalité, la santé ou la sécurité publiques et la protection des consommateurs. De telles restrictions devront toutefois être proportionnées à l'objectif recherché. De plus, hormis dans les cas d'urgence, elles ne pourront être imposées que si l'État membre d'établissement du prestataire du service a été invité à prendre les mesures adéquates et ne l'a pas fait de manière satisfaisante, et que si l'intention d'imposer des restrictions a été préalablement notifiée à la Commission et à l'État membre dans lequel le prestataire de services est établi.

Dans les cas d'urgence, les raisons des restrictions (et de leur caractère urgent) doivent être notifiées dans les délais les plus brefs à la Commission et à l'État membre d'origine du prestataire de services. Dans l'hypothèse où la Commission considérerait que les restrictions proposées ou effectivement appliquées ne sont pas justifiées, les États membres concernés seront invités à ne pas les appliquer ou à les lever le plus rapidement possible.

La proposition de directive visant à instaurer un cadre juridique pour le commerce électronique sera adressée au Parlement européen et au Conseil de ministres de l'Union européenne en vue de son adoption dans le cadre de la procédure de co-décision.



# POLICE ET INNOVATIONS TECHNOLOGIQUES

par Nicole SOULLIÈRE

Une analyse historique des processus de technicisation montre que chaque innovation technique tend à modeler profondément les organisations policières. Une description de la situation nord-américaine semble indiquer que l'introduction des technologies de l'information contribue à redéfinir les métiers policiers et les structures des organisations. Enfin, la capacité de contrôle induite par ce changement favorise une nouvelle approche du pouvoir en terme de simulation.

•••(1) Congrès *Vie privée sans frontière*, Montréal, automne 1997.

•••(2) MARX, 1988 ; BOGARD, 1996 ; LYON, 1992 ; MANNING, 1992 ; ERICSON, HAGGERTY, 1996.

•••(3) Sur le bracelet électronique, cf. l'article de J.C. Froment dans ce même numéro. (NDLR).  
Sur la vidéo-comparution, cf. MARIAGE (C.), « L'enregistrement vidéo du témoignage de l'enfant victime », *Les Cahiers de la sécurité intérieure*, n°28, p. 149-151.

Les technologies font couler beaucoup d'encre depuis un certain nombre d'années. Elles sont analysées dans leurs rapports divers, multiples et complexes avec la société en général et des secteurs plus particuliers dont celui de la justice et de la police. On discute par exemple de leurs impacts sur la vie privée<sup>1</sup>, de l'amplitude que prennent la surveillance et l'obsession de la sécurité, amplifiée par les technologies de l'information, des communications et de la surveillance<sup>2</sup>. On s'intéresse à leurs rapports avec le droit (BRODEUR, 1988 ; CADOUX, 1993), à la mise en forme d'une utilisation légale (TRUDEL, 1997) et à l'utilisation de certaines d'entre elles par le système de justice criminelle comme dans le cas de l'assignation à domicile (LANDREVILLE, 1987) et de la vidéo-comparution<sup>3</sup>. Certains justifient l'utilisation des technologies en soulignant leur capacité d'augmenter la sécurité publique et de combattre le trafic des drogues ou la délinquance des gangs (NIJ, 1996). On s'intéresse également à leur capacité de

modifier les frontières territoriales d'intervention (MARX, 1997 ; BOGARD, 1996). Si elles sont considérées comme un support aux agences de contrôle social (MARX, 1988) et amplificatrices du pouvoir policier (NOGALA, 1993), elles sont également conçues comme un médium capable de contrôler le travail de la police (ERICSON, HAGGERTY, 1996 ; MANNING, 1992), voire comme une menace par ceux-là même qui ont en main le pouvoir (MARX, 1992).

L'histoire de la police dans son rapport aux technologies nous apprend qu'elle réclame depuis le début du siècle toujours et davantage de technologies pour mieux contrôler la criminalité, mieux faire face aux utilisations délinquantes de la technologie tout en invoquant des promesses d'économie pas nécessairement tenues.

La police dans son rapport aux technologies est une problématique complexe. Dans cet article, nous traitons de ce thème dans une perspective historique, afin d'avoir une meilleure vue d'ensemble du processus de technicisation de la police en Amérique du Nord. Nous faisons par ailleurs état des technologies actuellement utilisées par la police dans le monde et proposons finalement quelques réflexions sur l'ensemble.<sup>1</sup>

## CENT ANS DE TECHNICISATION

Dans cette première section, nous présentons une synthèse des acquis technologiques en deux parties. La première concerne la période qui va de la fin du XIX<sup>e</sup> siècle jusqu'aux années quatre-vingt et, dans la deuxième, est présenté un bilan des technologies actuelles.

### DE LA FIN DU XIX<sup>e</sup> SIÈCLE AUX ANNÉES QUATRE-VINGT

#### *Avant 1945*

À la fin du XIX<sup>e</sup> siècle, les policiers travaillent dans un isolement presque total. Les patrouilles se font à pied dans la plupart des cas et les moyens de transport disponibles sont limités : des bicyclettes et des charrettes tirées par des chevaux. Les premiers véhicules motorisés sont acquis dès

•••(1) Cet article se veut la synthèse d'une réflexion plus vaste faite dans le cadre d'un programme de doctorat à l'université de Montréal et d'un programme de recherche au Collège canadien de la police.

•••(1) Le *call box* est une cabine contenant un téléphone, une tablette et un crayon. Plusieurs de ces cabines sont installées un peu partout dans la ville. Les policiers et certains résidents peuvent y accéder à l'aide d'une clé. Les patrouilles (charrettes à chevaux appelées *Paddy Wagon*) postées à la station de police sont prêtes à intervenir sur appel. Chicago installe ces cabines en 1881 et Toronto en 1888. L'isolement du policier se termine avec l'installation des *call box* : «à l'origine, on note de véritables réticences de la part des agents, car ils craignaient de devoir justifier l'ensemble de leurs faits et gestes durant le service» (site du *Chicago Police Headquarters*, section historique, p.3).

•••(2) Le patrouilleur peut recevoir des messages du poste central, mais il ne peut communiquer avec le central.

•••(3) Pour Montréal, 1914 et pour San Francisco, 1919.

•••(4) Dès le début du siècle, des lois concernant les véhicules à moteur ainsi que la conduite en état d'ivresse sont promulguées aussi bien au Canada qu'aux États-Unis. Par exemple, au Québec, la loi de 1904 concernant les automobiles (Statuts du Québec, 1904, c.30). Il n'y a aucun véhicule immatriculé dans la province à ce moment. En Ontario, la loi date de 1903 et 178 véhicules sont déjà immatriculés cette année-là. Les lois concernant la conduite en état d'ivresse suivent de près, en Ontario en 1906 et au Québec en 1907. Chacune des provinces en fait autant, sauf le Nouveau Brunswick (SOULLIÈRE, 1989).

le début du siècle en Amérique du Nord. Ce n'est cependant que vers la fin des années trente que l'ensemble des services de police sera motorisé. Quant au premier système de communication, le télégraphe, son importance n'est pas soulignée de manière spéciale dans les documents historiques des services de police. L'installation des «*call box*»<sup>1</sup> est par contre considérée comme la première acquisition technologique ayant une incidence sur leur travail. À la fin des années vingt sont installées les premières communications radio à bord des véhicules (*one-way radio*)<sup>2</sup>. À la fin des années trente, ce système est remplacé par une communication dans les deux sens (*two-way radio*). Par ailleurs, de petits laboratoires judiciaires existent depuis le début du siècle<sup>3</sup> mais ce sont des laboratoires restreints à un ou deux employés munis des connaissances de base en médecine légale, en chimie et en physique, connaissances servant à élaborer une preuve scientifique. Mais c'est seulement au cours des années trente que sont créés les premiers laboratoires judiciaires des grands services de police à travers le monde. Entre 1932 et 1939, on voit apparaître les laboratoires judiciaires du FBI, de New Scotland Yard, du New York State Patrol, de la Gendarmerie royale du Canada, ainsi que les laboratoires des services de police de Chicago et de San Diego (cf. le site Internet respectif de chacun de ces Services).

La période est marquée par deux guerres mondiales et les progrès effectués par «l'effort de guerre» ont sans aucun doute accéléré plus spécifiquement le processus de développement des communications. Bref, au cours de la première période, la police acquiert une plus grande mobilité, des moyens de télécommunications et accède à un nouveau type d'informations fournies par les spécialistes des laboratoires judiciaires. Ces trois grands développements technologiques ont sur le travail des policiers et l'organisation policière au moins sept impacts qui ne sont pas nécessairement de même niveau.

Premièrement, la création de nouvelles lois a des répercussions sur le travail de la police<sup>4</sup>. Suit une augmentation des tâches particulièrement dans le domaine du contrôle routier, l'automobile se démocratisant rapidement.

Deuxièmement, l'augmentation des tâches donne elle-même lieu à la création de sections nouvelles dans la police : création de la police de la route, de la police spécialisée dans les communications radio, ainsi que des laboratoires judiciaires, à tout le moins dans les grands services. Par conséquent, la structure de l'organisation policière commence à se modifier. Troisièmement, les technologies deviennent progressivement des outils de travail dont la police ne pourra jamais plus se passer. Quatrièmement, les technologies ont un impact majeur sur l'élargissement du territoire policier. L'automobile permet en effet de couvrir un territoire plus grand et plus rapidement ; les communications de donner et recevoir des renseignements sur de grandes distances. Quant aux technologies de laboratoire, elles donnent accès à des informations autrefois impossibles à obtenir à cause de l'état antérieur des sciences de la biologie, de la chimie et de la physique. Cinquièmement, les technologies acquises sont conçues par des spécialistes qui ne cessent de progresser dans la recherche et le développement de leur spécialité respective et partagent leurs progrès avec la police, ce qui a pour effet de rehausser l'image de la police perçue dès lors comme plus « scientifique ». Sixièmement, la sécurité du policier augmente progressivement par l'usage de nouveaux moyens de transport et de communication. Finalement, l'ensemble des développements technologiques, l'augmentation des tâches et la création de sections spécialisées génèrent une organisation policière progressivement plus complexe et plus centralisée. La centralisation est l'une des conséquences des acquis technologiques mais elle devient aussi une nécessité pour maintenir un usage efficace des nouvelles technologies.

*De la fin de la deuxième guerre mondiale aux années soixante*

Dans cette période, on enregistre peu de progrès technologiques spectaculaires, si ce n'est la ligne téléphonique d'urgence 911<sup>1</sup> en Amérique du Nord. Elle sera adoptée progressivement par l'ensemble des services d'une certai-

•••(1) Cette ligne permet d'établir un lien entre les divers services d'urgence dans une ville, tels que la police, les pompiers et les services hospitaliers d'urgence.



••••(1) L'ancêtre du radar actuel et l'ivressomètre.

ne importance, quoique, dans la plupart des cas, beaucoup plus tard dans les années soixante-dix, quatre-vingt, voire quatre-vingt-dix. La police de la route se dote des premiers instruments qui servent à mesurer les excès de vitesse et l'état d'ivresse<sup>1</sup> des conducteurs de véhicules automobiles. La police de la route devient ainsi plus légitime avec l'usage d'instruments « scientifiques ». Ces deux instruments sont des outils de travail dont la police ne se départit pas avec les années. Améliorés avec le temps, ils sont utilisés d'une manière plus ou moins systématique encore aujourd'hui. Ils sont directement liés à l'application de la loi et utilisés par un type spécifique de police, à savoir la police de la route. L'organisation policière devenant plus complexe, la centralisation des fichiers débute vers la fin des années cinquante. C'est l'émergence de la bureaucratisation moderne de la police.

#### *Le Boom des années soixante et soixante-dix*

••••(2) Pour le *New York State Patrol*, l'informatisation débute en 1965 ; en 1969, pour la Sûreté du Québec et en 1975, pour le service de police de London en Ontario.

••••(3) En 1965, le Service de London (Ontario) accède aux données de l'*Ontario Police Forces Network*. En 1969, le Service de police d'Orlando est relié au *Florida Crime Information Center* (FCIC). En 1972, le *New-York State Patrol* est relié au *New-York State Criminal Justice*. En 1973, le *New-York State Patrol* est relié au *New-York State Department of Motor Vehicles*, etc.

L'émergence de la technicisation moderne de la police se situe au cours de cette période. L'arrivée de la nouvelle technologie de l'informatique est à l'origine de plusieurs innovations dans les services de police. Vers le milieu des années soixante, l'informatique commence à faire partie du décor. L'informatisation des fichiers de police donne lieu à la création de sections informatiques dans les services les plus importants<sup>2</sup>, l'informatisation ne se faisant pas de manière linéaire.

Les moyens de communication s'améliorent aussi largement. Dans les années soixante-dix, les centrales téléphoniques sont réaménagées à l'aide du système informatisé de répartition des appels (*Computer Aid Dispatch*). Les services de police accèdent également aux premiers réseaux informatisés de banques de données. C'est un des acquis majeurs de cette période. Les grands services de police sont en effet désormais reliés entre eux et à certaines agences gouvernementales et peuvent ainsi accéder à leurs banques de données respectives.<sup>3</sup> Parallèlement, la gestion devient une priorité et plusieurs services de polices procèdent à des restructurations. La Sûreté du Québec, par

exemple, procède à une première réorganisation en 1961. En 1969, elle se réorganise à nouveau selon les concepts de gestion moderne et crée, cette même année, une section pour les services informatiques. En 1974, le Centre de renseignement policier du Québec (CRPQ) devient fonctionnel et est relié au Centre d'information de la police canadienne de la GRC (CIPC), lui-même en fonction depuis 1972.

Au cours de la période, les policiers voient une augmentation globale de leurs capacités de récolter des renseignements à l'aide de l'informatique et d'accéder à des renseignements par les réseaux informatisés de banques de données. Une des conséquences de l'informatisation est l'augmentation du personnel policier et l'embauche des premiers policiers civils spécialisés dans les grands services de police en Amérique du Nord. La bureaucratisation et la gestion en général connaissent une expansion conséquente. Quant à la sécurité des policiers, elle s'améliore sensiblement grâce à la capacité qu'ils ont désormais d'obtenir sur le champ des renseignements concernant un citoyen interpellé.

Les organisations policières cumulent depuis le début du siècle et ce progressivement, les technologies utiles à l'ordre public. Les années soixante et soixante-dix se caractérisent par l'abondance du point de vue des technologies mais la police doit tout de même remplacer le matériel usagé et entretenir l'ensemble. Les organisations policières doivent désormais assumer un fardeau financier considérable. Devant cet état de fait, les gouvernements vont réagir et créer des infrastructures vouées à la recherche et au développement de technologies destinées à la police. C'est ainsi que se créent les centres de recherches policières tel que le *National Institute of Justice* américain.

## UN BILAN ACTUEL

Avec les années quatre-vingt et quatre-vingt-dix, les communications sont plus sophistiquées et plus complexes. Les renseignements sont abondants et en provenance de sources diverses, dont certaines inaccessibles sans les technologies. Les logiciels de supports se multiplient.

L'intégration des systèmes ou leur création va bon train. Nous sommes au cœur du paradigme de la technologie de l'information (CASTELLS, 1998). La deuxième partie de ce texte est consacrée à la présentation d'un bilan des technologies utilisées par la police depuis les années quatre-vingt. Ce bilan n'est pas exhaustif, les armes technologiques aussi bien que les technologies clandestines n'en font pas partie. Pour être retenue dans ce bilan, la technologie en question doit être actuellement utilisée par un service de police ou une agence gouvernementale. Elle doit de plus permettre à la police soit d'obtenir des informations et/ou davantage d'informations, soit de les obtenir plus rapidement, soit encore d'obtenir des informations inaccessibles sans la technologie. Les innovations technologiques de n'importe quel service de police du monde occidental peuvent ici entrer en ligne de compte parce que, d'une part, les technologies de l'information facilitent les contacts entre les policiers à l'échelle mondiale et que, d'autre part, les policiers assistent plus fréquemment à des congrès internationaux sur le thème des technologies destinées à la police. Il est donc plus probable qu'ils s'influencent mutuellement.

#### LES TECHNOLOGIES DE L'INFORMATION

*«Les véhicules de police ressemblent désormais plus à des bureaux mobiles et des laboratoires technologiques - ils sont reliés par radio locale, téléphonie cellulaire, terminaux informatiques de dispatch, ordinateurs portables, radars, caméras vidéo, micros à distance, étylomètres, fax, imprimantes et appareils de repérage des véhicules. La police est reliée et il suffit pour s'en convaincre de jeter un coup d'œil à l'aspect extérieur des véhicules : un véritable champ d'antennes pour la bonne raison que chacune de ces applications électroniques nécessite sa propre réception».*<sup>1</sup>

••••(1) ERICSON,  
HAGGERTY, 1996, p. 135.

#### *La patrouille assistée par informatique*

Il existe dans les services policiers à travers le monde divers systèmes de télécommunications en réseaux qui fonctionnent soit par secteurs, soit au niveau national ou

international. Ces réseaux de télécommunications aident les policiers dans le domaine de la gestion, de l'enquête et de la prise de décision. Ce dernier domaine est particulièrement complexe, voire le plus complexe des secteurs de technologies utilisées par la police. Au-delà de la terminologie spécialisée, on retiendra que le maximum semble être fait pour procurer aux policiers des ondes de communication les plus sécurisées possibles, un accès le plus direct et le plus rapide possible aux banques de données qui contiennent les divers fichiers de renseignements. L'organisation vise l'efficacité quant à la répartition des appels et la standardisation des communications. La tendance est à la multiplication et à l'intégration des systèmes de communications que ce soit pour la police ou pour les agences gouvernementales.

L'ordinateur installé dans les voitures de patrouille (*Mobile Data Terminal*)<sup>1</sup> permet au policier de faire des recherches sur les banques de données.<sup>2</sup> Il peut envoyer des messages et des rapports, chercher un numéro dans la banque de données et changer son statut à partir du véhicule. Il peut également communiquer avec les autres véhicules de patrouille sans passer par la communication radio. Lorsqu'il y a un appel, l'information est envoyée directement à l'agent chargé de l'affaire. Il est possible de télécharger un fichier, de le mettre à jour et de le fermer sans avoir à se rendre au bureau. L'accès aux données est direct et augmente la rapidité d'obtention des résultats. Ce type de communication serait par ailleurs sécurisé du fait de l'absence de trafic radio. Ceci empêche, en principe, en effet les communications d'être interceptées par les journalistes ou les utilisateurs de scanners.<sup>3</sup>

Aux États-Unis, les divers niveaux de décision investissent beaucoup en subventions pour équiper les services de police, quelle que soit la taille du service. En 1997, 1,29 milliard a été attribué à l'équipement des services de police américains de MDT (*Mobile Data Terminal*) et de CAD (*Computer Aid Dispatch*). En 2002, le budget prévu à cet effet est de 2, 59 milliards.<sup>4</sup>

L'Internet est également un réseau de télécommunications qui existe sous sa forme actuelle depuis 1993. Il est utilisé par les services de police à travers le monde.

••••(1) Les patrouilleurs à pied en Grande-Bretagne auront tous bientôt des micro-ordinateurs comme les patrouilleurs. Où qu'ils se trouvent, ils auront accès aux mêmes informations que les policiers en véhicules de patrouilles. Ce système comprend un bouton d'urgence qui permet au policier de demander de l'aide en cas de besoin. La position exacte du policier peut être repérée par satellite. Le premier service à utiliser ce type d'appareil est Hartlepool, Cleveland. L'appareil est petit et léger. Il coûte 1000 £ (9 juillet 1998 : *BBC News*). Également, les patrouilleurs à bicyclette : à Alexandria en Virginie, les policiers qui patrouillent à bicyclette sont désormais équipés d'un terminal (*the unwired Cop*). Le tout est installé à l'arrière de la bicyclette (*Law and Order*, vol. 46, n°4, 8 avril 1998).

•••• (2) Tous les policiers canadiens sont en mesure d'effectuer des recherches sur le système du Centre d'information de la police canadienne (CIPC) ainsi que sur le système intégré de récupération de renseignements judiciaires (SRRJ).

••••(3) Cependant, il existe actuellement sur Internet un site concernant les *Mobile Data Terminal*. On y indique le matériel (disponible chez RadioSchack) et les codes nécessaires au décryptage, ce qui permet un accès aux données contenues sur le MDT: <http://www.people.qualcomm.com/ppomes/Crypto/MDT.html>.

••••(4) *Washington Technology*, vol. 13, n°7 p. 20, July 2, 1998 sur le site du NLECTC.

Plusieurs services de police ont désormais un site Web dont le *Home Office* britannique, le FBI américain, *Scotland Yard*, *Interpol*, la Police nationale française aussi bien que la GRC, la Sûreté du Québec, le Service de police de la Communauté urbaine de Montréal, la Police provinciale de l'Ontario et une multitude de services de police américains, canadiens, européens et asiatiques.

Cette présence sur l'Internet permet, entre autres, aux services de police de s'afficher sous la bannière de la police communautaire, de mettre en ligne les photos de personnes recherchées et à la population de faire des dénonciations anonymes. De plus, parmi les outils utilisés pour la formation policière à distance, on compte maintenant en plus des vidéo-cassettes et des systèmes audiovisuels de téléconférence, l'Internet<sup>1</sup>.

Il existe par ailleurs, aux États-Unis, plus spécifiquement en Ohio, un site constitué d'une base de données sur les personnes incarcérées<sup>2</sup>. Il s'agit d'un site à partir duquel, avec le nom ou le numéro de la personne incarcérée, on accède aux données suivantes : nom, délits au casier, date d'entrée au pénitencier, sentence minimum et maximum, date de la comparution devant la commission des libérations conditionnelles et date possible de la sortie. Quatre États américains ont déjà ce genre de site en ligne.

La démocratisation de l'Internet donne lieu à la création de nouveaux créneaux de travail pour la police. Internet ouvre en fait un nouveau territoire de criminalité (utilisation illégale de logiciels, par exemple) et permet à des délits conventionnels de s'opérer dans un nouvel espace (pornographie infantile, fraude, blanchiment d'argent, prostitution de mineurs, propagande haineuse, etc.). Des unités policières travaillent déjà exclusivement sur la criminalité technologique incluant la criminalité sur Internet. C'est le cas de la GRC au Canada (site de la GRC sous criminalité technologique) et du *FBI's Computer Squad* aux États-Unis (site du FBI). Le vocabulaire policier s'est enrichi d'expressions nouvelles telles que gendarmes internautes, police virtuelle, enquête électronique, etc. Dans ce contexte, avoir accès aux clefs de cryptage est un enjeu important pour la communauté policière. Le cryptage permet en effet

••••(1) Aux États-Unis, les policiers peuvent recevoir de la formation, en ligne, de l'université Christopher Newport en Virginie qui est l'hôte de deux programmes d'éducation en ligne, le CNU online et *The Mid-Atlantic Police Supervisory Institute* (MAPSI) et ce depuis 1993. *Law Enforcement Bulletin*, février 1998, p. 10 -14.

••••(2) *Ohio Offender Database Search*:  
<http://www.drc.state.oh.us/inmate/search.htm>.

aux utilisateurs d'Internet de conserver leurs communications à l'abri des intrus et d'échapper par conséquent à la surveillance des autorités policières<sup>1</sup>.

Parmi les technologies utilisées par la police, les technologies de l'information sont celles auxquelles s'intéressent le plus les chercheurs. Manning (1995) pense que la question de l'utilité et de l'impact des nouvelles technologies de l'information demeure sans réponse. Ces technologies peuvent être utilisées pour augmenter la qualité et l'équité des services de police et humaniser la pratique policière comme elles peuvent être utilisées pour contrôler les officiers, éliminer et filtrer les appels pour réduire le travail. Quant au rapport du policier avec le citoyen, il semble être réduit à l'usage de l'ensemble des technologies dont dispose la police : « *Ils sont synchronisés à la seconde par l'ordinateur. Leur travail est assuré par un ordinateur automatique qui leur distribue les appels dès qu'ils sont libres : l'ordre dans lequel s'accomplit leur travail est déterminé par l'ordinateur. Ils n'ont que de nom le service public. Bien qu'ils soient payés par le public, ils travaillent pour les machines, qui les menacent par-derrière, qui leur rougeoient le visage, font des clics et bourdonnent dans leurs oreilles et remplissent l'air de bruits électroniques.* » (MANNING, 1988, p.155). Il constate également qu'elles sont le plus souvent utilisées dans le cadre d'une stratégie répressive. (MANNING, 1992).

#### Interconnexions

L'utilisation des technologies de l'information pose aussi le problème des interfaces avec les autres institutions. Si la police peut être connectée à la SAAQ<sup>2</sup>, par exemple, l'inverse est-il vrai ? Il semble en effet que les renseignements de la police circulent vers les autres institutions de gestion des risques, publiques ou privées, telles que les compagnies d'assurances et les fabricants d'automobiles (ERICSON, HAGGERTY, 1996). Ericson et Haggerty démontrent comment le travail même de la police, dans son utilisation des technologies de l'information, consiste à alimenter les institutions de gestion des risques et fait des policiers, des « *knowledge workers* ».

••••(1) Le directeur du FBI américain a présenté un projet de loi qui rendrait illégal l'utilisation de la technologie qui permet le cryptage des messages, si elle ne permet pas aux policiers de les casser (*Encryption : Impact on Law enforcement*, 1<sup>er</sup> mars 1998). De même, le 30 janvier 1998 la ministre britannique Joyce Queen souligne que l'on ne peut pas lutter contre la criminalité du XXI<sup>e</sup> siècle avec des outils du XX<sup>e</sup> siècle « : les États membres de l'Union européenne veulent garder la haute main sur le cryptage Internet, autrement dit que leur police ait un accès garanti aux clés pour décrypter les messages codés sur Internet (BBC News, 30 janvier 1998).

••••(2) Société d'assurance automobile du Québec.

••••(1) Centre de renseignements policiers du Québec.

••••(2) Entretien informel avec un policier.

••••(3) Par exemple avant d'aller prendre une pause, ils doivent en principe l'indiquer sur leur MDT et envoyer le message. Ils inscrivent le message mais ne l'envoient pas. Si le superviseur vient à passer, ils montrent le message et invoquent que l'ordinateur n'a pas envoyé le message (ERICSON, HAGGERTY, 1996, p. 413).

••••(4) *Le West Midland Police* (Grande-Bretagne) est en train de mettre au point une banque de données informatisées d'empreintes de souliers (*shoe print data base*) qui sert à identifier les contrevenants par les chaussures qu'ils portent (*BBC News*, 2 mars 1998).

••••(5) Grande-Bretagne, Nouvelle-Zélande, France et Canada.

••••(6) Le NAFIS britannique (*National Automated Fingerprint Identification*) peut, en l'occurrence, comparer un million d'empreintes à la seconde. Il est en fonction depuis mai 1998 (Site du *Home Office*).

Quant aux usages dérivés, voire pervers des technologies de l'information, on peut les illustrer par divers exemples. L'usage des banques de données en réseaux n'est pas toujours orthodoxe. Les policiers utilisent parfois les données contenues sur le CRPQ<sup>1</sup> pour régler des litiges personnels<sup>2</sup>. Ils ont par ailleurs développé l'habitude d'effectuer des vérifications au hasard sur la banque de données lors des patrouilles de quartiers. L'informel prend ainsi le dessus sur le légal (ERICSON, HAGGERTY, 1996). Les données, ainsi obtenues, sont litigieuses car elles sont acquises sans raison valable et non dans le cadre formel de l'accomplissement du travail policier. Par ailleurs, les technologies de l'information exercent une forme de contrôle sur les policiers qui ont commencé à réagir en développant des méthodes de contournement (ERICSON, HAGGERTY, 1996 ; MANNING, 1992).<sup>3</sup> L'utilisation des ordinateurs dans les véhicules de patrouille aurait une incidence sur la hiérarchie policière. La manière dont les logiciels de support sont formatés fait en sorte que les rapports sont plus précis et plus complets. Le sergent qui assumait un rôle de superviseur voit son rôle réduit, la machine accomplissant déjà cette tâche (ERICSON, HAGGERTY, 1996).

#### LES BANQUES DE DONNÉES ET LES SYSTÈMES EXPERTS

L'informatique a donné lieu à des systèmes puissants de banques de données à partir d'éléments utilisés depuis longtemps, tels que les empreintes digitales et les photos de personnes condamnées ou à partir de données plus récentes telles que les empreintes de pas<sup>4</sup> et les empreintes génétiques dans certains pays<sup>5</sup>. Avec l'informatique, la police procède aussi plus facilement à la constitution de portraits robots des personnes recherchées. Les données ainsi transposées se consultent plus facilement et plus rapidement.<sup>6</sup>

Les systèmes experts sont, par ailleurs, des combinaisons de fichiers, contenant un grand nombre d'informations. Ils sont supportés par des logiciels qui permettent de recouper et d'analyser les données. Ce sont essentiellement des outils d'enquête. Certains sont utilisés dans le contexte de

la criminalité grave<sup>1</sup>, d'autres pour la reconstitution animée d'accidents. Le Centre canadien de recherches policières a mis au point deux systèmes experts particuliers. Le premier (CLEIMS) permet aux policiers d'enregistrer les éléments de preuve sur disque compact pour les produire devant les tribunaux. Ces délits nécessitent l'examen et l'étude de nombreux documents. Le système permet de parcourir l'information rapidement pour obtenir les éléments de preuve. Le deuxième (*InvestigAid*) contient des données portant sur les entrées par effraction<sup>2</sup>.

Le *crime mapping* est également considéré comme un système expert qui peut être traduit par géographie du crime. Cette technologie est effectivement empruntée aux géographes et aux militaires qui l'utilisent sous l'appellation GIS (*geographic information system*). Le *crime mapping* est une technologie permettant de réunir avec rapidité de nombreuses données, de les organiser, les classifier et d'en faire un graphique en deux ou trois dimensions. Il permet ainsi de visualiser rapidement l'état de la « criminalité » officielle d'une ville. Ce système est utilisé par les services de police canadiens, américains et européens. Aux États-Unis, des recherches sont menées pour tirer le meilleur parti de cette technologie et le *National Institute of Justice* américain a créé, en l'occurrence, le *Crime Mapping Research Center* qui organise fréquemment des congrès internationaux dont l'objet est l'utilisation et l'amélioration du système.

Les technologies ne sont pas neutres. Peuvent-elles, en ce sens, permettre à un organisme de renforcer ses valeurs ou à tout le moins certaines d'entre elles ? L'usage par la police du *crime mapping* peut, à cet égard, servir d'exemple: sans la technologie, cette tâche prendrait un temps considérable.

Ericson et Haggerty (1996) citent la réponse d'un policier à qui l'on demandait s'il n'était pas gêné de ne prendre en compte que la criminalité officielle : « *C'est ce qui correspond pour nous à la réalité. Nous ne pouvons traiter que la criminalité effective, non celle qui pourrait se produire.* » (p. 137). Ironiquement, cette technologie sert également à faire de la prospective.

Utilisé dans le cadre de la police communautaire, le *crime mapping* est justifié par le fait que ce type de police

••••(1) SALCV (Système d'analyses des liens entre les crimes de violence de la GRC) qui est un système national. Les concepteurs de ce système se sont inspirés d'autres systèmes existants, en l'occurrence aux États-Unis : *Violent Criminal Apprehension Program* (VICAP du FBI), *Sex Crimes Analyses System*, de l'Iowa ; *Sex Crimes Analysis System* (MINN/SCAP), Minnesota Homicide, etc.

••••(2) Ce logiciel est loué à plusieurs organismes policiers canadiens dont le Service de police régionale d'Ottawa - Carleton, le service de police de Thunder Bay, la police de la communauté urbaine de Toronto et la Gendarmerie Royale du Canada (CCRP, 1997).



•••(1) Chaque plante utilise différemment les longueurs d'onde du soleil lors de la photosynthèse. Chaque plante possède donc une signature lumineuse qui est un peu son empreinte digitale. C'est justement de cette propriété dont se servent les chercheurs pour aider la police à repérer les champs clandestins de marijuana (Découverte, Radio Canada, le 28/9/97). C'est de la caméra hyperspectrale de la Sûreté du Québec, dont il était question à cette émission. Elle est surtout utilisée par la police de la section antidrogue.

•••(2) Un spectromètre en tandem coûte 600 000 \$. Le spectromètre utilisé en tandem avec le chromatographe permet de retrouver des traces microscopiques d'explosifs et d'accélérateurs dans des débris incendiés très contaminés. Ceci permet aux enquêteurs de confirmer leurs soupçons d'incendie criminel ou de terrorisme (JOHNSON, 1997).

•••(3) Appareil qui peut confirmer ou infirmer la présence d'une personne à bord d'un véhicule et fonctionne un peu comme un électrocardiogramme. Il est utilisé dans une institution pénitentiaire du Tennessee (Riverbend Maximum Security Institution).

amène davantage d'informations au système (ERICSON, HAGGERTY, 1996). Certains services de police utilisent par ailleurs des données portant sur la race. Cette manière de procéder est justifiée comme étant une aide à l'enquête : « *En pratique, cela signifie que l'élément race apparaissant sur l'écran est un élément à considérer lorsque le policier répond à un appel ou identifie proactivement des lieux potentiels de délits. Le policier est amené à considérer l'élément race comme une variable pertinente à prendre en compte dans ses rapports avec les citoyens.* » (ERICSON, HAGGERTY, 1996, p. 283).

### *Les autres technologies*

Parmi les autres technologies, il y a les technologies de l'image, les technologies des laboratoires judiciaires et les technologies biométriques. Elles sont toutes des technologies qui informent le policier et ont, dans certains cas, un support informatique.

Les technologies de l'image sont nombreuses et largement utilisées par la police, à tout le moins par les grands services. Parmi ces technologies, notons le radar photographique, l'aide à la vision nocturne, l'imagerie électronique (*imagery analysis*), la caméra hyperspectrale<sup>1</sup>, les caméras de vidéosurveillance, la caméra vidéo sans fil, le *nooklooker*. Les rayons X, quoique d'origine différente, sont utilisés le plus souvent pour la détection de matériel illicite ou dangereux. Les laboratoires judiciaires ont toujours contribué à rehausser l'image de la police auprès du grand public. Cela est plus vrai que jamais. Les laboratoires permettent à l'organisation policière de se donner une image de professionnels, un statut scientifique, bien que le travail soit accompli par des professionnels civils. La chimie, la biologie, la physique, aussi bien que la robotique, voire l'entomologie judiciaire sont au service de ces laboratoires. Le personnel civil est hautement qualifié et le coût du matériel généralement élevé<sup>2</sup>. Quant aux technologies biométriques, elles peuvent être classées selon un usage d'identification (empreintes digitales et dentaires, empreinte vocale et empreinte génétique) de détection (détecteur de battements de cœur<sup>3</sup> et vision de nuit)

ou de contrôle (contrôle frontalier automatisé, bracelet électronique et antidémarrreur, détecteur d'alcool<sup>1</sup>).

Les usages, impacts et enjeux de la plupart de ces technologies ne font pas pour l'instant l'objet d'études particulières<sup>2</sup>, au même titre que les technologies de l'information, si ce n'est pour discuter de leurs utilisations possibles, des procédures d'utilisation et de leur efficacité. Ce sont surtout les centres de recherches policières qui s'y intéressent. Par ailleurs, le pragmatisme, une des grandes caractéristiques de certaines de ces technologies, refoule facilement ceux qui s'opposent à leur utilisation dans le cadre du système pénal. L'empreinte génétique<sup>3</sup> est une des technologies qui suscite un débat. Elle est déjà utilisée, depuis 1989, au Canada. De plus, une banque nationale de données génétiques a été créée en décembre dernier. Deux remarques sur les effets indirects de cette loi.

Parmi les infractions désignées par la loi, trois retiennent plus particulièrement l'attention : ce sont les voies de faits simples, les voies de faits contre un agent de la paix et finalement l'action indécente. Deux groupes particuliers pourraient être des cibles privilégiées lors de l'application de la loi, à savoir les personnes souffrant de maladies mentales ainsi que les manifestants. Sachant que les personnes du premier groupe sont souvent accusées de voies de fait contre un agent de la paix et d'actions indécentes (LABERGE *et alii*, 1995) et que le second groupe peut facilement être accusé de voies de fait contre un agent de la paix lors d'une manifestation qui tourne mal, nous suggérons que les empreintes génétiques de ces personnes sont susceptibles de grossir la banque nationale de données génétiques, incluant ainsi une partie de la population qui, à l'origine, ne tombe pas sous le coup de la loi. L'impact de ces technologies biométriques sur le processus de criminalisation des personnes «malades mentales» (ou perçues comme telles) et des manifestants pourrait faire l'objet d'une recherche intéressante lorsque la loi entrera en vigueur.

Par ailleurs, une dérive dans les usages de cette banque de données est toujours possible. Imaginons par exemple, que, dans le cadre de la justice pénale, un chercheur, bien intentionné, décide de faire une recherche à partir des don-

•••(1) Appareil installé obligatoirement dans le véhicule d'une personne trouvée coupable de conduite en état d'ivresse au Québec. Le conducteur doit «souffler» régulièrement dans l'appareil et ce sur commande de l'appareil. Dans le cas où la personne ne se conformerait pas à cette commande de la machine, un système d'alarme se déclenche automatiquement.

•••(2) Exception faite de la vidéosurveillance et du bracelet électronique.

•••(3) L'empreinte génétique est utilisée par la police canadienne depuis 1989. En 1995, des mesures législatives autorisent la police à prélever des échantillons d'ADN sur des suspects après obtention d'un mandat. En décembre dernier, la loi concernant la création d'une Banque nationale de données génétiques recevait la sanction royale. Son fonctionnement est confié à la Gendarmerie royale du Canada qui, dans les dix-huit mois à venir, devra mettre en place l'infrastructure requise par la loi.

nées contenues dans la banque nationale de données génétiques afin de vérifier quels peuvent être les gènes communs à tous les «criminels». Il faut voir aussi que, à partir du moment où un pays se dote d'une banque nationale de données génétiques, une extension à la population en général est toujours envisageable. Cela a déjà été suggéré, en l'occurrence en Grande-Bretagne, par Peter Gammon (Président de la *Police Superintendents' Association*). Son argument était le suivant : « *Cela rend l'identification des contrevenants plus facile ; le temps consacré à la collecte et à l'analyse des échantillons prélevés sur un suspect, après la commission d'un crime, est du temps perdu, ce qui peut retarder l'enquête.* » (*BBC News*, 5 mai 1998). En contrepartie, Alec Jeffries, à l'origine de l'utilisation de l'ADN pour l'identification s'oppose à cette mesure : « *Un criminel déterminé pourrait être tenté de pénétrer cette base de données et en modifier les entrées, se donnant ainsi l'alibi ultime pour la commission éventuelle d'un délit* ». (*BBC News*, 5 mai 1998).

#### QUELQUES RÉFLEXIONS À PROPOS DU PROCESSUS DE TECHNICISATION

##### UN PROCESSUS IRRÉVERSIBLE ?

L'historique du processus de technicisation de cette organisation fait ressortir comment et à quel point au fil des années, la police s'est progressivement et intimement liée aux technologies (SOULLIÈRE, 1998). Les technologies de base (transports, communications, technologies de laboratoire et informatique) sont acquises, conservées et améliorées au cours des périodes successives. La police est aujourd'hui dépendante de ces ensembles technologiques et ne peut effectuer un retour en arrière soudain et systématique.

Une fois les technologies acquises, il faut répondre aux exigences du travail policier par davantage de matériel : cela est vrai dans le cas de l'automobile où, dans les débuts, deux ou trois véhicules par service suffisaient à la tâche. Progressivement, on parle de parcs de véhicules, d'hélico-

ptères, de bateaux, de véhicules d'intervention, etc. Cela est vrai également dans le cas des équipements des laboratoires judiciaires ainsi que dans le domaine de l'informatique où, par exemple, les données sont tellement importantes (de nouvelles banques de données s'ajoutent régulièrement), qu'il faut de nouveaux logiciels de traitement et d'analyse, des ordinateurs plus puissants et davantage de spécialistes en informatique.

En outre, l'utilisation délinquante des technologies oblige la police à développer de nouvelles applications en même temps qu'elle lui sert d'arguments pour s'en procurer davantage. La technologie appelle la technologie. Les policiers ont dû se procurer des automobiles pour intercepter les utilisateurs contrevenants de cette nouvelle machine. Aujourd'hui la fraude électronique, la criminalité informatique, les infractions aux lois sur les télécommunications et le piratage de logiciels sur Internet, sans compter les inégalités de toutes sortes autrefois commises sur le territoire traditionnel (fraude, pornographie, pédophilie, etc.), ont amené des policiers à se mettre à l'heure des communications électroniques, à s'équiper pour être en mesure de faire face à cette nouvelle «criminalité» (NIJ, 1996). Cet exemple illustre bien ce que Nógala (1993) appelle «la course aux armements technologiques». Et dans ce domaine, l'habileté des contrevenants dépasse souvent la capacité et les moyens policiers.

Dans un autre contexte, celui de la manifestation, nous savons que les manifestants se sont adaptés, au fur et à mesure de leurs interactions et confrontations avec la police du maintien de l'ordre. Une des illustrations de cette adaptation est l'équipement technologique acquis. Les manifestants, forts de leurs expériences se sont progressivement équipés, aussi bien que la police, de véhicules, de cellulaires, de télécopieurs, etc. La police, en réaction à cet état de fait, s'est équipée davantage (LEBEUF, SOULLIÈRE, 1996a). Avec la venue de l'Internet, une autre forme de manifestation émerge. On pourrait assister à plusieurs manifestations pour une même cause en des endroits différents (MARX, 1997). L'Internet permet, en effet, de contacter en même temps des groupes situés dans des

villes différentes, voire des pays différents. Selon Marx (1997), cette nouvelle procédure pourrait s'avérer relativement déstabilisante pour les policiers désignés au contrôle de foules et remettre en question leurs méthodes traditionnelles d'intervention.

Les technologies policières sont, par ailleurs, vulnérables. La vulnérabilité des technologies s'illustre d'une part par la capacité pour une personne bien équipée et douée dans le domaine de l'abstraction de pénétrer les données policières accessibles sur les terminaux des véhicules de patrouille. Certaines institutions de prestige voient également leurs données menacées par l'intrusion de *hackers*. Le Pentagone, la NASA et la Défense nationale ont été tour à tour victimes de ces habiles adeptes de l'informatique. Désormais, les barrières sont abstraites. Elles sont constituées de codes et il est impossible par la seule force physique ou par une force mécanique de protéger les données. Dans ce domaine de l'abstraction, le plus doué gagne, pas nécessairement le mieux équipé. D'où la nécessité pour la police de faire appel à des spécialistes de l'information. Les données policières sont donc vulnérables aux intrusions et il est impossible de les retourner dans un classeur standard pour les protéger. La loi sur l'accès à l'information suffit-elle dans ce contexte à protéger la vie privée des gens? Avoir la haute main sur le cryptage devient dans ce contexte, un enjeu de taille pour les policiers du monde entier.

D'autre part, plus les technologies sont sophistiquées, plus les systèmes supportés par ces technologies sont fragilisés. Le bogue de l'an 2000 en est une illustration. Il a généré de nombreux rapports dans les organisations policières du monde entier et le travail nécessaire à les rendre compatibles à la date du 1<sup>er</sup> janvier 2000 coûte très cher aux organisations. Toutefois, ces investissements massifs ne donnent en aucun cas l'assurance qu'au 1<sup>er</sup> janvier de l'an 2000, tous les systèmes seront opérationnels et que des coûts supplémentaires ne seront pas nécessaires pour contrer l'effet du bogue.

Les coûts sont justement l'un des enjeux liés à l'irréversibilité du processus de technicisation et à la dépendance à la technologie : coûts occasionnés par l'achat, l'entretien,

le renouvellement du matériel et la formation. Par exemple, le Centre d'information de la police canadienne (CIPC) doit être modernisé après vingt-six ans d'utilisation au coût de douze millions. Peut-on imaginer que l'on renonce à cet investissement ? Les budgets ont tendance à être préparés en fonction de cette dépense et des coupures sont effectuées ailleurs pour remplir cette obligation.

Ce constat de l'irréversibilité et de la dépendance à la technologie ne permet cependant pas d'occulter les forces d'opposition suggérées par Nogala (1993). Elles jouent un rôle important, mais ne font que retarder le développement, sans pour autant l'arrêter, au même titre que les forces de stimulations internes et externes ont tendance à amplifier le phénomène. Mais la technicisation se poursuit tout de même.

#### SPÉCIALISATION ET DIFFÉRENCIATION

Le processus de technicisation de la police participe de la constitution de cette organisation. Tout se passe comme si la police s'adaptait et se modifiait selon les technologies disponibles et surtout acquises.

La technicisation de l'organisation policière se fait sensiblement à l'intérieur des mêmes périodes que le processus de technicisation de la société en général. Les acquis sont progressifs, et non linéaires, en ce sens que tous les services de police ne bénéficient pas au même moment des bienfaits de chacune des technologies. Les grands services sont toujours les mieux nantis en technologies nouvelles. De plus, ils ont à la fois la connaissance et de la méta-connaissance c'est-à-dire qu'ils disposent du personnel spécialisé pour enseigner aux policiers utilisateurs.

On constate également que, si les technologies ne sont pas distribuées de manière linéaire à travers tous les services de police en même temps, elles ne sont pas non plus destinées à tous les policiers d'un même service<sup>1</sup>. Cette distribution différenciée va participer progressivement à la mise en forme de nouvelles fonctions policières : policiers de la route, des enquêtes criminelles, policiers techniciens ; policiers ambulanciers ; policiers membres du groupe tac-

.....(1) À l'exception des ordinateurs dans les véhicules des *constables*.

tique d'intervention ; policiers spécialisés dans le contrôle des foules ou de la criminalité informatique, etc. Il y a des technologies spécifiques pour chaque service de police. Nogala suggère même que la police semble se scinder en un corps orienté sur la communication et un policier citoyen d'une part et en des équipes hyper équipées d'agents spéciaux d'autre part (1993). Difficile, à l'heure actuelle, de vérifier cette prédiction, mais nous pouvons à tout le moins constater une diversification de la police en plusieurs polices. Le policier isolé du début du siècle travaille progressivement au sein d'une organisation policière, puis d'un réseau d'organisations nationales puis internationales. Aujourd'hui, ses moyens sont multipliés par autant de contacts au sein de son organisation qu'au sein d'autres organisations.

L'acquisition d'un nouvel ensemble technologique participe au processus d'extension du territoire physique du policier (automobile, communications) et éventuellement à la possibilité de franchir les barrières traditionnelles de ce territoire dans le cas du cyberspace et de l'ADN (MARX, 1997 ; BOGARD, 1996). Les frontières du territoire policier sont donc peu à peu modifiées. De plus la collaboration des divers spécialistes scientifiques a permis à l'organisation policière de rehausser progressivement son image.

#### *Une masse de données*

La police accède actuellement à une masse d'informations *via* les technologies de l'information, les systèmes experts, les technologies de l'image et biométriques. Cette expansion des renseignements rendus disponibles par cet arsenal technologique pose, entre autres, le problème de leur gestion. Comment la police peut-elle, en effet, gérer efficacement un tel flot de renseignements ? En Grande-Bretagne, la police de Manchester possède dix millions de dossiers dans cinquante bases de données différentes. À Hampshire dont la population est de deux millions d'habitants, 80 000 personnes sont fichées<sup>1</sup>. Ces données sont-elles utiles ? Nécessaires ? L'abondance des renseignements disponibles et des données informatisées pose

.....(1) BBC, News, 28 juillet 1998.

également le problème de l'accessibilité, les grands services étant mieux lotis que les services de petite taille.

Quant à savoir si cet arsenal technologique et cette masse de renseignements génèrent une plus grande efficacité policière, les évaluations restent encore à faire. Plus n'est pas toujours synonyme de mieux comme le souligne Marx (1988). En l'occurrence, le FBI est en retard de dix-huit mois sur le traitement des preuves et doit solliciter les services de sociétés privées telle que *Per-Se Technologies*, spécialisée dans le domaine des technologies de l'information pour les soins de santé<sup>1</sup>. La privatisation du traitement des données de la police pourrait-elle s'accroître ?<sup>2</sup>

La masse de données pose également le problème de la pertinence des données. Le registre des personnes condamnées mis en ligne sur Internet par le tribunal correctionnel de l'état de l'Ohio pose certains problèmes d'ordre éthique. Comment, en effet, justifier que des données judiciaires soient ainsi livrées au grand public de l'Internet ? L'argument de sécurité ne répond pas véritablement à la question. Comment interpréter cette procédure ? Et comment justifier l'utilisation de l'empreinte génétique, au-delà de l'argument de sécurité ?

•••(1) Federal Computer Week, vol. 12, n°.12, p.1, April 27, 1998.

•••(2) Autre fait intéressant, mais anecdotique dans le contexte, l'ancien directeur du *Criminal Justice Information System* de l'État du Maryland possède un site web à partir duquel il agit à titre de conseiller pour l'utilisation des numéros d'identification, les photos et empreintes numérisées ainsi que la reconnaissance faciale : <http://www.cjs.com/domain.htm>

### *Le pouvoir de la simulation*

L'homme s'est doté depuis toujours d'un certain environnement technologique. L'environnement technologique moderne touche la police et les autres institutions publiques et privées aussi bien que l'ensemble des citoyens. Les technologies de l'information et de surveillance sont maintenant largement utilisées dans les écoles, les universités, le milieu médical, le milieu carcéral, les compagnies, les espaces commerciaux, en fait dans tous les ensembles bureaucratiques.

L'image du *panopticon* de Bentham utilisée par Foucault dans *Surveiller et punir* (1975) surgit rapidement en écho à la situation moderne. On assiste en effet à une multiplication de moyens de surveiller et de contrôler les citoyens, tout le temps et partout : ils sont surveillés sans savoir d'où vient la surveillance. À cette image se superpose celle de



Stanley Cohen, celle du filet de pêche dont les mailles se sont resserrées et renforcées (cité par MARX, 1988). La surveillance carcérale s'est déplacée vers l'ensemble de la population. Mais il faut maintenant compter avec les technologies de l'information, la démultiplication des moyens de détection, de surveillance et de contrôle, sans oublier l'accroissement de la surveillance de ceux qui surveillent (MARX, 1992).

Pour expliquer le rôle des technologies de l'information et de surveillance dans notre société moderne, Bogard (1996) avance le concept post-moderne de « simulation de la surveillance » dans son livre *The simulation of surveillance: hypercontrol in a telematic society*. Bogard emprunte l'idée à Baudrillard. Pour cet auteur, la tour des gardes du *panopticon* suffit désormais à dissuader. Nul besoin d'une présence humaine, la présence de l'appareil, du symbole de la surveillance, suffit. Selon lui, cette simulation de la surveillance n'est pas la négation du *panopticon*, mais l'apothéose du contrôle panoptique : « *L'apothéose (et non sa négation) du contrôle panoptique nous permet de parler clairement, non seulement de la simulation du pouvoir, mais du pouvoir de la simulation. La simulation n'est pas l'opposé du pouvoir, mais un autre mode d'exercice, son expression la plus élevée et la plus paradoxale* » (p.72).

La technologie n'est ni bonne ni mauvaise, pas plus qu'elle n'est neutre (KRANZBERG, 1985, cité par CASTELLS, 1998, p. 25). Comment appliquer cette loi de Kranzberg à la police dans son rapport aux technologies ? Il faut comprendre que la lecture des usages faits d'une technologie par une personne ou une organisation pourrait bien révéler les valeurs et les intérêts de cette personne ou de cette organisation. Ces valeurs et intérêts pourraient varier selon le poste occupé par une personne ou le statut de l'organisation. Dans son rapport aux technologies, la police demeurant accrochée à ses propres limites, lesquelles sont déterminées par des liens étroitement entretenus avec le pouvoir politique et ceux de sa culture professionnelle.

■ **Nicole SOULLIÈRE**

*Université de Montréal*

- BOGARD (W.), 1996, *The simulation of surveillance : hypercontrol in telematic society*, Cambridge, University Press.
- BRODEUR (J.-P.), 1997, « La police en Amérique du Nord : Modèles ou effets de mode », *Les Cahiers de la Sécurité intérieure*, n° 28, 2<sup>e</sup> trimestre, p. 171-184.
- BRODEUR (J.P.), 1988, « Droit, Procédure pénale et technologie » in LEBLANC (M.), TREMBLAY (P.), BLUMSTEIN (A.) (dir.), *Nouvelles technologies et Justice pénale*, p. 555-578.
- CADOUX (L.), « L'adaptation du droit aux nouvelles technologies intéressant la sécurité », *Les Cahiers de la sécurité intérieure, Sécurité et Technologies, Actes du Comité d'experts réuni les 2 et 3 décembre 1993 à l'IHESI*.
- CASTELLS (M.), 1998, *La société en réseaux. L'ère de l'information*, tome 1, Paris, Fayard.
- ERICSON (R. V.), HAGGERTY (K. D.), 1996, *Policing the Risk Society*, Oxford, Clarendon Press, 487 p.
- KRANZBERG (M.), 1985, « The information age : evolution or revolution ? », in GUILÉ (B. R.) (dir.), *Information, Technologies and Social Transformation*, Washington DC, National Academy of Engineering.
- LABERGE (D.), LANDREVILLE (P.), MORIN (D.), ROBERT (M.), SOULLIÈRE (N.), 1995, *Maladie mentale et Délinquance : deux figures de la déviance devant la justice pénale*, Montréal, Les Presses de l'Université de Montréal.
- LANDREVILLE (P.), 1987, *Surveiller et prévenir : l'assignation à domicile sous surveillance électronique*, École de criminologie, Université de Montréal.
- LEBEUF (M.-E.), SOULLIÈRE (N.), 1996a, *Ordre et désordre social au Canada. Un bilan des connaissances*, Ottawa, Institut des cadres de la police, Collège canadien de police.
- LYON (D.), 1992, « The new surveillance: Electronic technologies and the maximum security society », in *Crime, Law and Social Change*, 18 1/2, p.159-175
- MANNING (P. K.), 1995, « Economic Rhetoric and Policing Reform » in *Police and Society*, Touchstone Readings, KAPPELER (V. E.), p.375-392.
- MANNING (P. K.), 1992, « Information Technologies and the Police », in TONRY (M.), MORRIS (N.) (dir.), *Modern Policing*, p. 349-398, Chicago, University of Chicago Press.
- MARX (G.T.), 1997, « Le maintien de l'ordre, un champ renouvelé », *Les Cahiers de la sécurité intérieure*, n°27, 1<sup>er</sup> trimestre, p. 11-15.
- MARX (G.T.), 1992, « When the Guards Guard themselves : undercover tactics turned inward » in *Policing and Society*, Vol. 2, p. 151-172.
- MARX (G. T.), 1988, « La société de sécurité maximale », *Déviance et société*, vol.12, p. 147-166.
- NATIONAL INSTITUTE OF JUSTICE, 1996, *Technology for public Safety* (Rapport de conférences).
- NOGALA (D.), 1993, « Le rôle de la technologie dans la police de demain », *Les Cahiers de la Sécurité intérieure*, n°14, août-octobre, p. 137-157.
- SOULLIÈRE (N.), 1998, *Historique de la technicisation de la police en Amérique du Nord*, papier inédit, École de criminologie, Université de Montréal, août.
- SOULLIÈRE (N.), 1998, *Police et technologies : Bilan actuel*, papier inédit, École de criminologie, Université de Montréal, août 1998.
- SOULLIÈRE (N.), 1989, *L'émergence de la pénalisation de l'alcool au volant au Canada*, Mémoire de Maîtrise, École de criminologie, Université de Montréal.
- TRUDEL (P.), 1997, *Droit du Cyberspace*, Montréal, Éditions Thémis, Université de Montréal.

# DU RENSEIGNEMENT AU PARTAGE DES INFORMATIONS L'INTELLIGENCE PROTÉIFORME

par *Nicholas Dorn*

En quelques années, l'échange circonstancié du renseignement entre une ou plusieurs agences de contrôle distinctes a fait place à une circulation de flux d'informations ininterrompus et institutionnalisés entre une multitude d'agences à vocation multiple. Si cette situation est largement imputable à l'avènement progressif de l'Europe de la sécurité, elle est aussi le fait de la révolution informationnelle. La complexité qu'elle induit pose le problème légendaire de la qualité et de l'authenticité de l'information et contribue, selon l'auteur, de façon non négligeable à la construction sociale de la notion de crime organisé.

Il y a quelque temps encore, les différentes agences de contrôle de l'État (police, douanes, services secrets, les administrations, et plus particulièrement les administrations fiscales, les agences de régulation du marché, etc.) considéraient leurs missions comme non convergentes. Le partage d'informations entre elles se faisait au coup par coup. À présent et de façon croissante, elles ont pour la plupart tendance à se sentir investies dans un combat commun contre les nombreuses facettes d'un phénomène dangereux et étendu, le crime organisé.

Cet article pose d'abord un cadre de travail visant à cerner la problématique émergente du renseignement et du partage des informations entre les différentes agences en charge de la lutte contre le crime organisé. Il aborde ensuite l'hypothèse, communément admise par les forces de l'ordre et la théorie sociale, selon laquelle l'évolution des formes de la criminalité dépend dans une certaine mesure, et non des moindres, des stratégies de contrôle mises en

place. Une question pratique se dégage alors tant d'un point de vue scientifique que politique : quelles conséquences et quels effets inattendus en terme de criminalité et de risque social génèrent les échanges de données entre agences de contrôle ? La situation actuelle en matière de renseignement pose de nouvelles questions pour la recherche.

## HISTORIQUE D'UNE COOPÉRATION RENFORCÉE

Depuis plusieurs décennies, on considérait les économies parallèle, irrégulière, grise et/ou criminelle comme des entités distinctes et séparées les unes des autres. Corruption de hauts fonctionnaires ou de responsables économiques, fraude en direction du secteur privé, de l'État ou du budget européen, évasion fiscale à grande échelle, vols d'objets de haute valeur, trafics de drogues, d'armes, d'autres biens interdits ou d'organes humains, tous ces problèmes n'étaient pas considérés comme liés. Ils méritaient bien une forme de réponse, mais généralement non coordonnée et à l'initiative d'agences de contrôle distinctes.

Mais à partir du milieu des années quatre-vingt-dix, sous l'impulsion de nombreux décideurs publics, de hauts fonctionnaires, de magistrats et de policiers en interaction aux niveaux international, européen et national, ces phénomènes économiques ont été de plus en plus perçus comme structurellement semblables, fonctionnellement parallèles, constituant empiriquement le *continuum* relié du crime organisé<sup>1</sup>. Un observateur a inventé l'expression de « criminalité protéiforme » pour qualifier cette évolution<sup>2</sup>. Ce changement de perception correspond exactement à une tendance d'accroissement de la coopération entre les différents organes et agences relevant tant de la sphère publique que du marché et de la société civile, et concernés, à des degrés divers, par la problématique de la régulation du crime organisé et des phénomènes afférents.

À quoi doit-on le maillage de ces deux sphères jusque-là séparées ? C'est l'objet de cet article que de tenter de peser les arguments qui, d'un côté, vont dans le sens d'une augmentation des menaces objectives que fait peser globale-

•••(1) Pour une approche générale, cf VAN DEN WYNGAERT, 1998.

•••(2) Expression que l'on doit à Alexandro Missir di Lussigana, alors en poste à la Direction générale XX de la Commission européenne.

ment le crime organisé, et de l'autre insistent sur un processus de construction sociale du danger. On a coutume de penser que l'effondrement du communisme s'est soldé par la dégénérescence de la vie politique et économique de certains pays, les conduisant à une forme de capitalisme sauvage, un gangstérisme international et une disparition des frontières entre crime et affaires. On trouve trace de constatations semblables entre la sphère de décision politique et le monde des affaires dans de nombreux pays développés. Et bien sûr, il y a eu à nos frontières des scandales majeurs, tels que le très remarqué *Willygate* en Belgique (l'affaire Willy Claes). Quoi qu'il en soit, d'autres commentateurs insistent sur le fait qu'il existe des menaces objectives et que les dangers n'ont jamais été surévalués, même si cultures populaire et politique ont toujours pu avoir besoin d'entretenir le danger de fortes menaces extérieures et si, plus spécifiquement, les agences de sécurité de l'État se cherchent par là une nouvelle légitimité dans un monde post-communiste.

Je me contenterai de dire qu'il semble exister des menaces tant globales que régionales et nationales dépassant les frontières politiques et économiques ; et qu'il semble que tout, dans notre culture, tant d'un point de vue politique que médiatique, contribue à une valorisation de cette menace. En conséquence, le crime organisé est défini comme un phénomène à grande échelle, traversant non seulement les frontières géographiques mais aussi le secteur économique.

#### SPHÈRES DE COOPÉRATION INTER-INSTITUTIONNELLES

Le phénomène « crime organisé » légitime la formidable motivation des agences à coopérer pour le combattre. La forme la plus récente de coopération - et la plus approfondie - est relative à l'information qui, une fois partagée, échangée, recoupée puis formatée, devient du renseignement. Le renseignement est en train de s'autonomiser des sphères spécialisées et cloisonnées desquelles il émanait auparavant. Le renseignement sur le crime organisé est par définition un matériau provenant de multiples agences.

Nous avons recensé quatre principaux acteurs :

- Les agences chargées du maintien de l'ordre et du respect de la loi : police, gendarmerie, douanes, qu'elles agissent dans un cadre judiciaire ou sous couverture, quand leur intention est de récolter suffisamment de preuves contre leurs cibles <sup>1</sup>.

- Toujours ces agences, et notamment la police, mais cette fois-ci dans le cadre de tactiques déstabilisantes : il s'agit de désorganiser temporairement les actions menées par des cibles suspectées de délinquance, d'endommager les capacités de l'organisation criminelle, ou de la démanteler à jamais, par de l'action cachée, de la désinformation, etc.<sup>2</sup>.

- Les autorités et organismes administratifs exerçant leurs pouvoirs de police administrative pour recouvrer des contraventions (par exemple, les contraventions du Trésor public, dénommées contraventions civiles en Grande-Bretagne), ou confisquer les gains d'un crime, réels ou suspectés comme tels <sup>3</sup>, ou encore retenir des sommes d'argent, suspendre différentes autorisations économiques ou privilèges <sup>4</sup>.

- Les agences de régulation publiques ou hybrides. Ces agences sont chargées de réguler d'importants pans de la vie économique, telle la Direction générale IV-Concurrence de la Commission européenne ou les organes de gestion des services financiers <sup>5</sup> ou du commerce international <sup>6</sup>.

Ces quatre secteurs de contrôle définissent l'environnement dans lequel le crime organisé évolue.

L'historique de la coopération entre de telles agences peut être décrit en plusieurs étapes : tout d'abord, des relations interpersonnelles, en passant par des relations formelles entre agences de même statut, puis au partage d'informations entre agences de statut différent, pour aboutir enfin à des plans d'action coordonnés au niveau européen.

Il y a une vingtaine d'années, la coopération entre les polices, les administrations et autres agences d'État se limitait à des contacts occasionnels et informels entre individus y travaillant ; ils avaient appris à faire confiance à un nombre limité d'interlocuteurs des autres agences. Il s'agissait de l'époque de « l'informel » dans l'action et la poursuite judiciaires. Cela permit de grands pas en avant dans cer-

••••(1) Le manque de place nous empêche d'entrer dans une discussion détaillée des conséquences de telles pratiques sur l'activité policière, mais on en trouvera une bonne description in BRANTS, FIELDS, 1995 ; pour une version française, se reporter à la revue *Déviance et Société*, 1997, n°4. Pour une approche compréhensive de l'intégration institutionnelle de la coopération policière, cf. VAN DEN WYNGAERT, *op. cit.*, sections 3 à 6.

••••(2) Cf. les rapports annuels successifs des douanes (*Her Majesty's Customs and Excise*) et les sections relatives aux indicateurs de performance concernant dix ans de stratégie de lutte contre la drogue du gouvernement britannique, *Tackling drugs to Build a Better Britain*, Londres, HMSO, 1998.

••••(3) *Home Office Working Group on Confiscation*, 1998.

••••(4) DORN (dir.), 1999.

••••(5) Notamment pour une perspective britannique, cf. RIDER, 1998, p. 196-203.

••••(6) Reste la question controversée de l'extraterritorialité (trop complexe pour être développée ici) : toute réclamation potentielle des autorités de régulation d'un État vis-à-vis de la juridiction d'un autre État, nécessitant la coopération d'un troisième État. C'est une difficulté plus particulièrement rencontrée par les autorités américaines pour faire respecter l'application de sanctions commerciales.

tains domaines, comme par exemple le travail reconnu et courageux de certains juges d'instruction en Italie. Revers de la médaille, l'absence de formalisation et de contrôle réciproque prédisposait à une forme rampante et proliférante de corruption policière.

À partir des années quatre-vingt, malgré des disparités géographiques, on remarque un commencement de relations de travail entre les agences, à la fois au sein des États et entre eux, jusqu'à voir se former des coopérations plus routinières sur le plan opérationnel. Dès lors, le lien se raffermirait entre les équipes - et non plus seulement entre individus - pour constituer des systèmes, le tout défini par des règles. On entre progressivement dans l'ère de la coopération policière formalisée au sein de l'Union européenne, cette étape est actuellement en plein développement.

Avec les années quatre-vingt-dix, on peut estimer que l'élargissement le plus significatif de la coopération inter-agences en matière de crime organisé s'est fait autour du renseignement. La constitution du renseignement, c'est-à-dire le processus par lequel chaque agence formatait auparavant sa propre information, est en passe de s'appuyer sur un partage des informations. Étant donné que le crime organisé tend à recouvrir des domaines et des formes d'activité économique des plus variées - à la fois licites et illicites - ainsi que des secteurs et des types d'activités commerciales diversifiées, on considère qu'il faut le combattre à partir d'une sorte de géographie compréhensive, dépassant les frontières spatiales, judiciaires et administratives. Ainsi, se propage l'argument d'un *continuum* dans le discours de la coopération, de l'information et du risque concernant le crime organisé en Europe et au niveau international. Et quoique ce développement suscite nombre d'intérêts, il ne sera pas facile de revenir en arrière.

La création de l'espace Schengen et l'extension du marché unique ont permis à la Communauté européenne et aux États membres d'intensifier la lutte en direction du crime organisé. Après le traité de l'Union économique signé à Maastricht, et malgré une discussion acharnée sur les difficultés institutionnelles de sa mise en œuvre, des mesures pratiques ont été décidées. À la suite du traité

d'Amsterdam, on s'est arrêté sur l'objectif primordial d'un espace de liberté, de sécurité et de justice qui s'est traduit par une série de mesures dans les premier et troisième piliers. Le conseil de la justice et des affaires étrangères a arrêté, en décembre 1998, un plan d'action pour l'établissement d'un espace de liberté, de sécurité et de justice, qui synthétise les tâches à accomplir pour les cinq ans à venir<sup>1</sup>. Concernant la coopération policière et judiciaire en matière de problèmes criminels, le plan d'action stipule que « *le but est de donner aux citoyens un haut niveau de protection tel qu'il est défini dans le traité d'Amsterdam, et de favoriser l'application de la loi. La coopération entre les autorités chargées du respect de la loi doit donc être renforcée en portant une attention particulière à la légalité. Il s'agit de donner lieu concrètement à un espace judiciaire dans lequel les autorités judiciaires puissent coopérer plus efficacement, plus rapidement, et plus soupagement. Il faut encourager une approche intégrée par l'intermédiaire d'une coopération rapprochée des forces de police, de la justice et des autres autorités en charge de la prévention et de la lutte contre le crime, qu'il soit organisé ou non* »<sup>2</sup>.

D'après ce plan d'action, l'expérience récente de coopération douanière européenne doit être prise comme exemple pour l'intensification de la coopération entre les agences de police et de gendarmerie et judiciaire. Il est prévu d'examiner comment et dans quelle mesure EUROPOL pourrait avoir accès au fichier d'information douanier (SID).<sup>3</sup> En fait, il semble que les administrations des douanes - qui, dans certains pays, ont à la fois des compétences administratives et judiciaires - ont servi de laboratoire à l'intensification des échanges d'informations, notamment entre administrations. L'autre secteur d'innovation en matière de partage de l'information réside incontestablement dans les activités de lutte contre la fraude économique, diligentée par l'UCLAF, qui est responsable de la coordination de la lutte contre la fraude affectant le budget européen. Du fait des intérêts convergents entre différentes agences, telles que les douanes et l'UCLAF, le système d'échange d'informations SCENT (*System Customs*

••••(1) UNION EUROPÉENNE, 1998.

••••(2) Plan d'action, *op. cit.*, article 42.

••••(3) plan d'action, *op. cit.*, articles 44(c) et 48(v).



••••(1) Commission européenne, Secrétariat général, 1998.

*Enforcement Network*) institué en 1985 a été intégré dans un dispositif plus large, dit AFIS (*Anti Fraud Information System*)<sup>1</sup>. Celui-ci est constitué de plusieurs niveaux de confidentialité, de sécurité, d'accès et de différents ensembles cloisonnés. L'activité d'Europol semble avoir été conçue en ce sens.

Plus généralement, du fait que dans les États membres, des agences équivalentes n'ont pas forcément des responsabilités identiques en matière criminelle, administrative ou civile, la coopération européenne rassemble des partenaires dissemblables : la police peut avoir à s'adresser aux douanes, les procureurs aux enquêteurs, des institutionnels à des partenaires officieux, etc. Par ailleurs, il est évident que la dynamique européenne d'un nombre croissant d'actions en relation avec les premier et troisième piliers favorise un partage inter-institutionnel croissant de l'information dans chaque pays.

#### CADRE DE TRAVAIL : LE RENSEIGNEMENT COMME INTERACTION

97

••••(2) PAOLI, 1999. NDLR : on trouvera un article en français du même auteur dans le n°32 des *Cahiers de la sécurité intérieure*, « Éléments pour une compréhension de la mafia en Italie », p.189-212, deuxième trimestre 1998.

Trop souvent, l'étude de la criminalité et celle de son contrôle sont distinctes. C'est malheureusement le cas du présent travail, du fait de limites d'ordre pratique, mais aussi parce que nous souhaitons rester aussi distanciés que possible de notre objet. Cela nous oblige à nous focaliser sur la problématique du contrôle plutôt que sur celle du crime, parce que le contrôle s'avère sans cesse plus convergent, à la différence de la criminalité qui reste éclatée du fait de la diversité de ses origines.<sup>2</sup>

Quoi qu'il en soit, on progresse dans la compréhension de la situation actuelle en considérant le processus information/renseignement comme un phénomène interactif, constitutif d'un environnement en perpétuelle évolution, structuré par une pléthore d'agences comme par le crime organisé. La piste est féconde qui consiste à déterminer les formes émergentes du crime organisé comme une réaction de ses auteurs à la généralisation diffusion du partage de l'information. En clair, le fait que le partage de l'information s'accroisse au sein des agences de régulation n'est pas

sans implication sur les stratégies des criminels. De même, les criminels les plus chevronnés cherchent à manipuler les agences de contrôle par le biais de l'information dans une posture que l'on pourrait qualifier de « contre-intelligence ». Les recherches à ce sujet sont pour le moins fragmentaires, restent de l'initiative de chaque agence et ne sont pas encore souvent dévoilées aux autres partenaires. Il y a là une véritable question. Jusqu'à quel point les investigations - et non pas seulement les informations - sont-elles mises en commun, et quelle devrait être à ce sujet la situation future ? <sup>1</sup>.

En préalable à un programme européen cohérent de recherche sur les réactions du crime organisé au partage de l'information entre les agences, il nous faut tout d'abord penser un cadre théorique dans lequel nous pourrions représenter la sphère des agences de contrôle et de régulation, le crime organisé dans l'ensemble de ses composantes économiques et organisationnelles et les interactions entre ces différents ensembles. Dans un tel cadre, l'information peut être considérée comme symétriquement interactive : premièrement, le fait qu'une information donnée n'est pas échangée entre agences sans un certain nombre de conditions tend à la promotion et au développement de la dite information. Ensuite, il existe un flux d'informations antagonistes entre les agences et les *leaders* du crime organisé.

Sur le premier point, on comprend bien que la confrontation de plusieurs bribes d'informations à propos d'un fait suspect - dénommé « cible » - n'autorise pas pour autant à penser qu'on obtient systématiquement une information de meilleure qualité ou même plus importante en quantité. Par exemple, une agence peut détenir une information sur une cible particulière que les autres agences ne connaissent pas et accepter de mettre en commun cette information disponible. Dans cette optique, un effort tout particulier est rendu nécessaire si l'on veut augmenter le stock d'informations : dans le cas où l'information détenue par les diverses agences est contradictoire, cela implique ensuite d'effectuer des vérifications. Ou, autre branche de l'alternative, l'information peut être fautive dans un ou plusieurs cas, sans que cela soit évident pour chaque partie.

••••(1) La question de la dimension de partage des résultats de commissions d'enquête et de recherches stratégiques menées en interne par les agences est intéressante. Nous pensons que le plus souvent, les agences sont très peu au fait des résultats des commissions d'enquête ou de consultations lancées en interne par leurs partenaires. Il semble que nous en soyons arrivés à ce stade de développement à partir duquel les informations opérationnelles concernant des cibles précises du crime organisé - et considérées dès lors comme moins sensibles - sont plus faciles à partager que des résultats de recherche-développement non directement opérationnels inscrits dans les objectifs propres stratégiques ou planifiés de chaque agence. Le plan d'action de l'Union européenne fixe l'obligation d'instituer un réseau de recherche et de documentation sur le crime transfrontière d'ici cinq ans (article 48-ii) et d'autres initiatives peuvent contribuer à débloquer la situation, si l'on arrive à instituer de nouvelles formes de travail (cf. Conclusion).

Intrinsèquement, rien ne garantit que le fait de passer de l'information d'une agence à une autre en augmente la qualité.

De même, la transmission d'une information de l'agence A vers l'agence B tend à accroître sa complexité, en dépit de toutes les précautions que pourrait prendre l'agence B ou qu'elle pourrait exiger de l'agence A pour des raisons de bonne ou de mauvaise entente. Une des explications à cette tendance réside dans le fait que le stock total d'informations détenues par une agence sur une cible relève de domaines dispersés et diversifiés. Puisque les unités de contrôle spécialisées, celles par exemple dédiées à un seul type de criminalité ou d'irrégularité comme le trafic de drogues ou l'évasion fiscale, tendent naturellement à récolter une information plus pertinente sur leurs objets de prédilection, le renseignement ensuite partagé devient plus large et couvre une multiplicité de champs. C'est un élément parmi d'autres de la composante interactive du renseignement, illustré par le tableau 1 sur le processus informationnel. La deuxième colonne de ce tableau représente l'importance croissante du champ de partage de l'information inter-agences, et résultant d'un renseignement de nature à embrasser les intérêts de la police et des autres agences engagées dans la poursuite criminelle : des agences chargées d'affaiblir, de désorganiser ou de démanteler les organisations suspectées de criminalité ; des agences consacrées au recouvrement de l'impôt ; des agences de régulation des marchés et des intérêts professionnels, etc. À la lumière des potentialités d'interaction entre ces informations de nature si diverse, et en référence au développement parallèle d'une *criminalité protéiforme*<sup>1</sup>, nous qualifierons ce processus de *renseignement protéiforme*.

••••(1) NDLR : en français dans le texte.

••••(2) Et bien trop vaste pour être discutée ici. (NDLR) On pourra se reporter aux autres contributions de ce numéro des Cahiers de la sécurité intérieure traitant plus précisément de cette question.

Toujours dans ce tableau, la quatrième colonne représente à son tour les problèmes de contrôle judiciaire et de légalité. Parmi ces catégories, certaines relèvent directement de la protection des données : que les garanties qui devraient être respectées le soient toujours, la question reste ouverte <sup>2</sup>. En tout cas, il existe de nombreuses possibilités de légitimer des échanges d'informations par des

accords dérogatoires aux dispositifs juridiques de protection des données les plus variés, fondés sur des motifs de sécurité publique et de lutte contre le crime. L'essentiel, pour notre propos, est que la propension à l'échange d'informations et les capacités techniques mises en œuvre suivent la même courbe ascendante.

## LE PROCESSUS : LA NATURE CONTESTÉE DU RENSEIGNEMENT

Nous avons vu que la première caractéristique du renseignement comme phénomène interactif réside dans le fait qu'il s'agit d'un flux entre les agences de contrôle, dont le spectre s'élargit d'autant. Mais le renseignement est aussi un flux d'informations entre les agences d'un côté et les instigateurs du crime organisé de l'autre même s'il s'agit d'un flux hostile. Les agences récoltent d'une part de l'information venant du crime organisé, qu'elles espèrent fiable ; d'autre part, elles tentent d'éviter toute fuite vers le crime organisé ou désinforment ses protagonistes. Pour leur part, les acteurs du crime organisé tentent de dissimuler les informations concernant leurs activités ou d'intoxiquer les

100

TABLEAU N°1 : LE PROCESSUS INFORMATIONNEL (SELON LA PERSPECTIVE DU CONTRÔLE)

Étape 1 Processus simple	Étape 2 Processus complexe	Étape 3 Interventionnisme formel ou informel	Étape 4 Contrôle judiciaire et de légalité
Il s'agit de récolter et de traiter de l'information pour les objectifs suivants :	Suite aux échanges entre différents domaines de contrôle, l'information est plus précise	L'intervention prend les formes suivantes :	Cette étape se caractérise par des incertitudes concernant :
instruction et passage en jugement		Voie judiciaire	Les moyens du contrôle judiciaire de la conformité du renseignement criminel
désorganisation ou démantèlement	Espace du renseignement interactif	Désorganisation	le manque de bases juridiques pour les opérations de désorganisation
finalités administratives, de recouvrement, etc.		Action administrative	le principe de proportionnalité et le droit procédural de la confiscation
régulation du marché		Régulation	la moindre efficacité des instances de régulation face aux acteurs forts du marché

••••(1) DORN, OETTE,  
WHITE, 1998, p.537-560.

agences. Ce faisant, ils récoltent des renseignements sur les activités et les intentions des agences de contrôle. Par exemple, une recherche effectuée en Grande-Bretagne<sup>1</sup> avec des délinquants purgeant une peine de prison et des informateurs des douanes interrogés à condition de préserver leur anonymat, nous a permis d'arriver aux conclusions suivantes : d'après eux, les personnes liées au crime organisé qui agissent sous couvert d'une façade et d'activités commerciales légales veillent à payer en temps et en heure leurs impôts. Ils cherchent par ce moyen à éviter tout risque d'investigation de la part de l'administration fiscale, qui, par ricochet, pourrait mener à une enquête de police ou des douanes. Certes, il s'agissait tout au plus de la conviction des personnes interrogées - il n'est pas question pour nous d'en déduire que l'administration fiscale ou d'autres forces procèdent de la sorte. Mais le fait est que certains délinquants pensent que les choses se passent ainsi.

Il semble que le crime organisé réagisse toujours aussi prudemment au partage de l'information entre agences. Évidemment, les façons de réagir diffèrent selon les organisations criminelles, leur évaluation de la situation, des croyances et des actions plausibles des autorités. Nous avons désormais besoin d'en savoir un peu plus sur ces estimations et la façon dont elles sont effectuées

#### DÉPASSER LA DISTINCTION CRIMINEL/NON CRIMINEL

Le secteur privé éprouve de plus en plus de difficultés à se définir par rapport à des catégories de moralité et empiète souvent sur des pratiques relevant de la criminalité grave. Par exemple, la majorité des affaires en cours en matière de crime organisé sont liées à la lutte contre la fraude vis-à-vis des finances publiques - tant au niveau national dans la passation de marchés publics, qu'à un niveau européen dans la défense des intérêts financiers de la Communauté européenne. Il y a là un paradoxe ou une contradiction. D'un côté, c'est peut-être par cette menace en particulier, sous la forme de la délinquance économique et financière, que le crime organisé est le plus manifeste, touchant les hommes politiques élus au suffrage universel,

comme les hauts fonctionnaires - mais aussi les dirigeants du secteur privé. D'un autre côté, précisément parce que des gens puissants et de grosses entreprises sont impliqués, on constate une forte nervosité vis-à-vis de mesures de lutte qui pourraient diviser les intérêts légitimes et les attentes. Ainsi, bien que le terme de liste noire ait été utilisé de nombreuses fois dans un contexte administratif pour désigner des organisations économiques suspectées de corruption ou de fraude, cette expression est désormais facteur de nervosité. Elle implique en effet qu'une entité économique puisse se voir refuser un contrat sur la base de la seule suspicion, ou pour le dire autrement, à partir d'informations non vérifiées. Des observateurs américains remarquent que l'on préfère parfois utiliser des expressions comme «liste approuvée». Une telle liste est constituée de la façon suivante : les contractants potentiels sont encouragés à délivrer des informations sur leurs propres procédures de lutte contre la fraude et contre la corruption, c'est-à-dire une auto-certification qui pourra ensuite faire l'objet d'un contrôle par échantillonnage aléatoire et évaluation de risque. Comme le secteur privé est soumis à des signalements et des examens plus fréquents, le débat sur la fiabilité et la légitimité du partage des informations dans le cadre de la lutte contre le crime organisé acquiert plus de visibilité.

De même que le secteur privé évolue dans des systèmes d'information qui empiètent sur le renseignement d'ordre criminel, les criminels traitent aussi l'information dans une perspective plus large que le traditionnel renseignement criminel. Les tactiques de désorganisation ou de démantèlement qui sont en train de s'imposer dans plusieurs États-membres ont des implications particulières sur le développement du traitement de l'information. En Grande-Bretagne, cette méthode est évaluée comme suffisamment performante pour être mise en œuvre dans le cadre d'opérations vis-à-vis des trafiquants de drogues par les services des douanes et droits indirects de sa Majesté. Courant 1999, elle a été modifiée et adoptée par le *National Crime Squad* (police auparavant régionale et désormais organisée sur une base nationale) <sup>1</sup>. Quant à savoir si de telles mesures sont adoptées à la fois par les services de sécurité intérieure-

••••(1) Source : Home Office.

re et extérieure, nous l'ignorons, mais si cela n'était pas le cas, on disposerait de chiffres d'opérations de désorganisation distinguant résultats policiers et/ou douaniers, pour pouvoir comptabiliser la somme des faits. Le renseignement utilisé pour ces opérations est par nature moins certifié que celui utilisé en matière criminelle, car il n'a pas besoin de résister aux récusations et à la procédure de jugement. Il est donc tout à fait possible qu'une large part de l'information provenant des agences de statut administratif et civil - information plus souvent indicative que véritablement sûre - soit précisément utile dans le but d'identifier des cibles de désorganisation.

Quelques résultats peuvent désormais être rappelés. Tout d'abord, le partage de l'information peut donner lieu, soit à un règlement pénal, soit à une désorganisation, une confiscation d'actifs, une amende administrative, ou enfin à une admonestation. En deuxième lieu, un nombre important d'agences participe du partage d'information utilisé pour mettre les gens hors circuit des affaires. Troisièmement, des entreprises légitimes et de bonne réputation peuvent devenir des cibles du traitement de l'information ou tout au moins croire qu'elles font l'objet d'une telle intention. Quatrièmement, les entreprises utilisent déjà les services de sociétés privées dans des buts variés, dont celui de vérifier dans quelle mesure elles font l'objet d'un contrôle de la part des agences de régulation et d'extraire le type d'information qu'on détient sur elles. Il est fort probable que de tels modèles de sociétés privées d'enquête se développent à l'avenir. Le rôle des sociétés de sécurité privée et leurs relations avec l'information multi-sources sont importants, mais trop complexes pour que l'on puisse le discuter ici. En tout cas, il est certain qu'elles peuvent jouer des deux côtés. Cinquièmement, tant les entreprises de bonne réputation que des entreprises peu recommandables souhaitent se prémunir contre des mesures administratives, de régulation, ou compenser leurs effets négatifs sur leurs affaires. Sixièmement, de telles cibles ne peuvent utiliser de recours pénal (car elles ne tombent pas sous le coup de cette juridiction) au contraire des recours judiciaire, administratif ou civil. Enfin, les entreprises peu-

vent, si elles le souhaitent, mettre en place des actions préventives en réclamant aux collecteurs d'informations de valider l'information qu'ils détiennent.

#### IMPLICATIONS POUR LE RENSEIGNEMENT JUDICIAIRE

Sur le long terme, ces éléments ne sont probablement pas sans conséquences pour le type et la qualité des informations échangées par les différentes agences (qu'elles soient à destination pénale, administrative, ou à des fins de désorganisations ou de régulation). Puisque les systèmes d'information tendent à être de plus en plus intégrés, il sera de plus en plus difficile pour chaque système de continuer d'utiliser différents critères de sélection des données, des méthodes de développement de l'information variées, des critères diversifiés de qualité interne, d'examen externe, de récusation et de correction d'informations erronées, etc. Certains critères et certaines données standardisées vont devenir problématiques pour des raisons à la fois juridiques et pratiques. Ces dernières sont très simples : comment l'information peut-elle être échangée si elle n'est pas comparable ? Les systèmes de renseignement sont déjà configurés pour des catégories d'informations plus standardisées, et moins pour du texte libre <sup>1</sup>.

Les raisons juridiques sont plus discutables : le renseignement multiforme - qui est un produit hybride provenant tant des sphères commerciales qu'administratives, pénales, etc. - pourra peut-être un jour faire l'objet d'un examen attentif de la part de la Cour européenne de justice, malgré la réticence de certains États. En attendant, la Cour européenne des droits de l'Homme exerce déjà une juridiction sur les méthodes de surveillance et sera peut-être amenée à se prononcer sur certains aspects du renseignement, du fait de la constitution d'une jurisprudence faisant suite à des attentes légitimes en matière de respect de la vie privée. De plus, la problématique de la protection des données commence à prendre de l'épaisseur. On finira peut-être par trouver que les clauses dérogatoires aux lois concernant la protection des données - qui, de façon typique, exemptent du droit commun la collecte de données dans des motifs de

••••(1) C'est par exemple le cas du système AFIS, mentionné plus haut.



défense nationale ou de prévention des crimes graves - ne sont pas recevables dans les cas où des opérateurs économiques font l'objet d'un simple traitement administratif ou d'une mesure de désorganisation plutôt que d'un traitement pénal. Nous risquons d'attendre un certain temps que l'action publique réussisse à résoudre certains de ces problèmes.

En résumé, pour des raisons juridiques et pratiques, l'intégration progressive des systèmes d'information à laquelle nous assistons aujourd'hui - conjointement à la récolte et au traitement de l'information dans les domaines du pénal, de la désorganisation, de l'action administrative et de la régulation de marchés - conduit inévitablement à un débat sur les critères, les méthodes, la qualité, la légitimité, la transparence des systèmes. En d'autres termes, la gestion du renseignement d'ordre judiciaire sera affectée de façon croissante par l'empiètement croissant des formes d'informations non criminelles.

En conclusion, on peut affirmer qu'à la fois en termes pratiques et analytiques, le processus de constitution du renseignement ne relève plus seulement des agences répressives. Les deux camps font du renseignement, mais probablement de façon différente : les agences de contrôle ont plus de moyens pour structurer cette activité en élargissant le spectre qu'elles couvrent - traitement pénal, démantèlement, compensation administrative, régulation - et en augmentant le spectre global de leur saisine. Par contraste, le crime organisé est plus réactif et dispersé, recherchant les sanctuaires, les contradictions et les opportunités dans l'univers de l'information. Objectifs formels, contraintes, protection des données dans le cadre d'un contrôle et de pratiques légales... Autant de questions qu'il reste à poser aux niveaux national et européen, auxquelles on pourrait rajouter celle des ripostes adoptées par les dirigeants et les opérateurs des organisations économiques lorsqu'ils sont impliqués dans des affaires de délinquance économique et financière, celle des formes justement de cette délinquance et de ses conséquences, et enfin celle de la prospective à effectuer pour un contrôle effectif.

Cette dynamique est au cœur de la recherche européenne sur le crime organisé, et la façon dont celle-ci est conçue n'est pas sans conséquences. L'effondrement des frontières géographiques et sectorielles signifie que la vieille ligne de démarcation entre chercheurs et acteurs n'a plus raison d'être. Le phénomène qui nous intéresse a des implications trop larges pour que nous puissions réussir dans notre analyse, si nous nous enfermons dans nos frontières, que l'histoire a d'ailleurs fait volé en éclats. Nous ne pourrions plus longtemps compter sur notre expérience, dans quelque champ que ce soit - qu'il s'agisse d'une expérience pratique dans une agence ou dans un secteur de contrôle, d'une expertise universitaire dans telle ou telle discipline (criminologie, droit national et européen, économie et comptabilité appliquées, etc.). Il ne s'agit pas là d'une simple observation théorique : l'élaboration des politiques publiques pose de plus en plus de difficultés et des notes banales rédigées à partir d'approches hyper spécialisées deviennent de réels problèmes, à tel point que les différentes administrations sont elles-mêmes obligées de travailler en partenariat. Cette situation nous crée des opportunités théoriques mais aussi des problèmes de recherche pratiques : comment travailler en équipe quand celles-ci sont dispersées géographiquement et administrativement et que les expériences de vie, les modes de pensée et les langues sont différentes ?<sup>1</sup>.

Finalement, par l'émergence d'une catégorie intermédiaire d'analystes stratégiques, le développement de l'information efface de lui-même les frontières entre chercheurs et praticiens. Les analystes sont employés par les agences de contrôle non seulement pour passer au crible et analyser l'information (relative à des opérations particulières contre le crime organisé) mais aussi pour développer une capacité d'analyse stratégique (description de dynamiques générales de développement du crime organisé). Cette activité, dispendieuse en énergie, se situe à la croisée des chemins entre chercheurs universitaires et praticiens des agences de contrôle et de régulation du crime organisé, et empiète sur les deux perspectives. Lors d'un débat entre hauts fonctionnaires et représentants des États-membres de l'union européenne qui faisait suite à une réunion-débat

••••(1) Nous tenons à exprimer nos remerciements aux *Cahiers de la sécurité intérieure* qui ont pris en charge la traduction de ce texte.

de deux jours entre universitaires experts du crime organisé - auquel j'ai eu le privilège d'assister, la question suivante a été posée : que peuvent nous dire sur le crime organisé les chercheurs indépendants que les analystes stratégiques ne nous aient déjà dit ? Peut-être les derniers peuvent-ils nous en dire plus... C'est bien sûr une question intéressante qu'il serait stimulant d'explorer de façon systématique, mais son intérêt pour notre conclusion, c'est que l'information devient protéiforme : elle donne à repenser le monde du chercheur, celui du décideur public mais aussi celui du crime.

■ **Nicholas DORN**

*Directeur de recherche, (ISDD), Londres.  
Coordinateur du programme Eurocrime  
(Institute of Advanced Legal Studies).*

## BIBLIOGRAPHIE

BRANTS (C.), FIELDS (S), 1995, « Participating Rights and Proactive policing: convergence and drift in European criminal Process », *Nederlandse Vereniging voor Rechtsvergelijking*, number 51, Kluwer, 95 p.

COMMISSION EUROPÉENNE, Secrétariat général, 1998.

DORN (N.), OETTE (L.), WHITE (S), 1998, « Drug importation and the bifurcation of risk: capitalization, cut-outs and crime », *British Journal of Criminology*, vol. 38, n°4, p. 537-560.

DORN (N.) (Dir.), 1999, *Regulating European Drugs Problems : administrative measures and civil law in the control of drug trafficking, nuisance and use*, Kluwer, La Haye.

HOME OFFICE WORKING GROUP ON CONFISCATION, 1998, *Third Report: criminal assets*, Londres, Home Office Organised and International Crime Directorate, 51 p., document de consultation.

JOHNSTONE (P.), 1998, « Financial crimes in England and Wales: The criminal and civil interface », *European Financial services Law*, vol. 5, n°9, septembre, p. 196-203, Dordrech, Kluwer.

PAOLI (L.), 1999, *The pledge of secrecy: Culture, Structure, and Action of Mafia associations*, Thèse de l'Institut universitaire européen de Florence.

RIDER (B.), « Civilising the law: the use of civil and administrative proceedings to enforce financial services law », *Journal of financial crime*, vol.3, n°1, Juillet, Londres, Henry Stewart publications, p. 11 et suivantes.

UNION EUROPÉENNE, 1998, « Plan d'action du Conseil et de la Commission sur l'application optimale des décisions contenues dans le Traité d'Amsterdam en matière de liberté, de sécurité et de justice ». Texte adopté par le Conseil des affaires intérieures et de la justice le 3 décembre 1998, in *Official journal of the European Communities*, 23 January 1999, C 19/1,EN.

*Tackling drugs to Build a Better Britain*, Londres, HMSO, 1998.

VAN DEN WYNGAERT (C.), 1998, « The transformations of international criminal law as a response to the challenge of organised crime », rapport pour le colloque préparatoire d'Utrecht, 13-17 mai 1998, in *International association of Penal Law*, 94 p. À paraître in *Revue internationale de droit pénal*, (1999)

# INFORMATION ET SÉCURITÉ

## Les institutions françaises

Alain BELVEAU, Commissaire principal, bureau des projets de police opérationnelle (DTI/BPPO)

Richard BROUSSE, rédacteur en chef adjoint de la revue *Culture et conflits*

Jean-Pascal CODINE, Administrateur civil hors classe, chargé de mission auprès du Directeur des douanes et droits indirects

Yves GUILLOT, Inspecteur général de la police nationale (IGPN)

Jean GUISNEL, Journaliste au *Point*

Colonel HERNANDEZ, Adjoint au sous-directeur des télécommunications et de l'informatique (DGGN)

Jean-Claude KARSENTY, Inspecteur général de l'administration (IGA), président de la Commission de l'informatique et des télécommunications (COMIT)

Paul LAGIER, Commissaire divisionnaire, sous-direction de la police technique et scientifique

TABLE RONDE

109

**JEAN GUISNEL :** *Je souhaiterais que nous commencions par un tour de table permettant à chacun d'entre vous de présenter sous quelle(s) forme (s) l'informatisation et les technologies de l'information ont pénétré l'institution qu'il représente et dans quelle mesure elles ont modifié les rapports de travail.*

JEAN-CLAUDE KARSENTY

Si l'on pense sécurité au sens large, c'est-à-dire à la fois les outils techniques permettant à la police d'assurer ses fonctions, mais aussi la gestion de la police (ressources humaines, matérielles, logistiques), il y a effectivement un nombre extrêmement important d'applications informatisées permettant une mise à disposition de l'information de plus en plus étendue, puis-

qu'aujourd'hui elle est même accessible aux commissariats de province. À titre d'exemple, on pourrait citer les fichiers des personnes recherchées, ceux des véhicules volés, ou encore les logiciels de rédaction de procédure.

Mais paradoxalement, l'introduction de ces nouveaux outils, tout en produisant un bouleversement des méthodes de travail, n'a en pratique pas changé grand chose. On constatera simplement une référence de plus en plus fréquente à une information existante, centralisée à l'échelon national, avec bien sûr des degrés différents d'habilitation à la consultation, permettant à la majeure partie des policiers d'avoir accès à des bases de données, de les consulter mais aussi de les alimenter, par exemple par l'intermédiaire du Système de traitement des infractions

constatées<sup>1</sup> (STIC). Toutefois, sur le plan du fonctionnement, seuls certains services ont été touchés en profondeur. Ce qui n'est pas le cas de la sécurité publique, qui représente le gros des effectifs, même si les machines à écrire disparaissent et si l'enregistrement des plaintes a été facilité. Je n'en dirais pas autant de certains services, et en particulier de la police judiciaire. Il est vrai que dans ce contexte-là, le recours aux connaissances scientifiques et techniques, par exemple au FAED<sup>2</sup>, modifie dans un sens positif les modes de fonctionnement.

Dernier point, le Ministère de l'Intérieur est en train de développer une masse extrêmement importante d'applications informatisées, sans pour autant que l'on puisse parler d'un « système d'information » au sens général du terme, même si le STIC tend à les fédérer. Cet ensemble informatisé représentera à terme un bouleversement dans les méthodes de travail mais il est un peu tôt pour évaluer réellement le changement dans les mentalités : le cablage de l'ensemble n'est pas totalement effectif et le système Intranet, qui permettrait le partage de l'information sur l'ensemble des services, n'est pas encore opérationnel. Il faudra sans doute attendre deux à trois ans. Développer cette information partagée et apprendre aux policiers à l'utiliser au mieux, c'est, me semble-t-il, l'enjeu de la prochaine décennie.

YVES GUILLOT

Pour ma part, je situerai le débat à l'échelle de la Direction générale de la police nationale (120 000 policiers actifs, 10 000 administratifs, environ 2800 implantations immobilières). Étant donné la diversité de ses missions et de ses services, se posent alors des problèmes de spécificité des applications informatiques, dont la nécessité de pouvoir les consulter de n'importe quel service, à tout moment, et donc d'une organisation pyramidale de consultation avec des droits d'accès... Pour les opérationnels, le problème se situe essentiellement dans les différents niveaux de communication et de confidentialité à articuler et à préserver. À un premier niveau de communication ouverte sur le monde extérieur, il n'y a pas besoin de protection particulière. Internet est un support idéal à la documentation, l'information, et éventuellement à la facilitation des relations entre citoyens et administrations. Le deuxième niveau répond à un besoin d'information interne et nécessaire au bon fonctionnement des services. Il nécessite une limitation d'accès qui passe par un dispositif de type Intranet. Quant au troisième niveau, proprement opérationnel et prépondérant en police, il nécessite d'utiliser des réseaux qui sont spécifiques. L'évolution technologique a ceci de particulier qu'elle relie l'informatique et les radiotélécommunica-

•••(1) Et non plus de l'information criminelle, depuis l'intervention de la CNIL.

(2) Fichier automatique des empreintes digitales.

tions autrefois distinctes. Les nombreux avantages, dont le fait de disposer de ces applications informatiques dans les véhicules, ne doivent pas dissimuler le défi important en matière de protection des communications.

JEAN-PASCAL CODINE

Pour une bonne part, les préoccupations de sécurité de la douane ne sont pas fondamentalement différentes de celles de la police et de la gendarmerie. L'une de nos premières applications informatiques, développée il y a maintenant quinze ans, et ce sous le contrôle de la CNIL, le fichier national d'information douanière (FNID) - en fait, un fichier des infractions constatées, des fraudeurs suspectés ou identifiés - témoigne de notre exigence dès le départ de garder une mémoire de notre travail et de la mettre à disposition de l'ensemble des opérationnels sur le terrain, malgré des moyens à l'époque rudimentaires, il faut bien le reconnaître. On commençait tout juste à parler de réseaux avec des terminaux intelligents reliés à de grosses unités centrales, de la radiotélécommunication pour interroger des PC de transmission radio qui, eux, avaient accès au réseau informatique.

Ensuite, nous avons cherché à savoir ce que nous faisons, c'est-à-dire à maîtriser l'informatique, du moins pour le volet sécurité (très différent du volet de traitement des marchandises et des opérations juridiques). Il fallait faire en sorte que, sur le terrain, nos agents

aient des pratiques harmonisées et systématisées, d'où le développement d'outils de gestion automatisée des procès verbaux. Ces outils permettaient que, dans un domaine juridique extrêmement fluctuant - le droit communautaire - les procédures ne risquent pas d'être invalidées par les juges. Cette approche est actuellement complétée par un projet initié il y a huit mois : une somme de la connaissance douanière, réglementaire, doctrinale et procédurale, sous forme de Cédérom, bien entendu crypté, qui sera mis en ligne sur notre Intranet, dès que celui-ci sera opérationnel, c'est-à-dire d'ici deux ans. Enfin, il nous importe de savoir aussi ce que font les autres. Sur la base de nos préoccupations, la lutte contre la contrebande, contre les contrefaçons, le trafic de stupéfiants, nous sommes en train d'explorer tout ce qui se passe sur Internet. Depuis deux ans, nous avons formé une équipe d'internautes, en mettant en place des logiciels d'abord extrêmement standardisés, des moteurs, des méta-moteurs classiques. Mais le problème de l'Internet, c'est le trop plein, et désormais, nous franchissons cette étape qui consiste à mettre moins de gens derrière les écrans, et plus d'intelligence derrière la machine. Nous collaborons avec des organismes de pointe comme l'agence pour la diffusion de l'information technologique dont les outils permettent de rechercher sur Internet de grandes masses d'informations par rapport à des profils de sélection, et d'analyser des contenus de façon à qualifier cette information.

Ensuite seulement, cette information est soumise à l'intelligence humaine de nos analystes douaniers qui vont opérer des discriminations en son sein et enrichir les profils. Nous ne savons pas encore quelle est l'efficacité réelle de cette technique tout à fait nouvelle, mais c'est la seule manière que nous ayons trouvée pour ne pas avoir à vider l'océan avec une écumoire.

COLONEL HERNANDEZ

La Gendarmerie est une arme de personnels, aux unités extrêmement dispersées sur le terrain (3600 brigades territoriales et plus de 4000 unités de terrain en tout), par opposition aux autres armes du Ministère de la Défense, qui sont plutôt des armes techniques ou de matériel. La capacité de la gendarmerie à renseigner et à communiquer est primordiale, d'où l'importance que l'on a toujours accordée à l'information et aux réseaux de communication entre unités de gendarmerie. À l'image de la police, nos applications de recherche opérationnelle concernent les personnes recherchées et les véhicules volés - en version nationale ou Schengen. Nous pouvons consulter des fichiers administratifs tels que le fichier national des automobiles ou celui des permis de conduire, mais nous utilisons aussi des applications de rapprochement judiciaire qui permettent de décrire les modes opératoires puis de faire des analyses croisées. L'ensemble de ces applications, traitées au niveau central, est consultable par

toutes les unités de gendarmerie, y compris à partir des véhicules de ces unités grâce aux réseaux de communications propres à la gendarmerie, dénommés « saphir » et « rubis ». De ce fait, nos gendarmes ont pris depuis longtemps l'habitude de consulter et d'alimenter, à partir des véhicules, des bases centrales.

Ce dispositif national est complété par des bases départementales de la délinquance qui permettent de la même manière de décrire les affaires traitées, les personnes impliquées, mais cette fois-ci à un niveau local : seules les affaires les plus importantes viennent alimenter la base nationale.

Enfin, nous disposons d'applications spécifiques aux unités de recherche spécialisées dans le judiciaire, et d'applications de type bureautique pour l'aide à la rédaction des procédures au niveau des brigades territoriales. Il est prévu de faire migrer ces applications de type transactionnel vers des technologies Intranet ; un site est déjà disponible sur ce réseau, qui regroupe notamment l'ensemble de la documentation constituant le mémorial de base des unités de gendarmerie. Cette documentation est également disponible sur cédérom.

Cette évolution appelle à une réflexion en termes de métiers. Nous en distinguons trois types. Un premier niveau nécessaire est celui de l'expertise en nouvelles technologies qui sera normalement limité à l'Institut de recherche criminelle de la gendarmerie (IRCGN). Le domaine traité par ces experts recouvre



les investigations sur Internet - les possibilités de tracer les tentatives de connexions sur un certain nombre de serveurs - et également tout ce qui peut permettre de reconstituer des filières à partir de l'analyse de ces connexions.

Un deuxième domaine relève du traitement des écoutes judiciaires à partir des téléphones portables et du GSM, beaucoup plus difficiles à intercepter et à traduire en clair que les appels sur le réseau téléphonique classique. Nous comptons par ailleurs former des spécialistes en nouvelles technologies affectés dans nos vingt-six sections de recherche, qui correspondent au découpage des régions administratives. Pour l'instant, on trouve dans ces unités des techniciens en investigation criminelle, qui sont des spécialistes habituels de la scène du crime, mais on souhaite également former de véritables spécialistes en nouvelles technologies qui constitueraient donc le relais entre les experts de l'IRCGN et les unités de recherche sur le terrain.

Un troisième besoin est identifié en matière d'analyse stratégique : ces analystes stratégiques - qui d'ailleurs pourraient ne pas être des gendarmes - devraient avoir une forme de liberté et d'autonomie afin de nous aider à percevoir ce que pourraient être les nouvelles formes de délinquance et de criminalité dans les années à venir et mettre au point les parades qui conviennent. La difficulté principale réside là dans le fait qu'il n'existe pas de cursus, de profil déterminé de ce que devrait être un analyste stratégique.

PAUL LAGIER

Le souci que nous avons eu dès 1985, c'est-à-dire au moment où a été créée la sous-direction de la police technique et scientifique, n'était pas de mettre en place un vaste système « big brother », mais de revigorer un domaine de la police qui avait été laissé de côté depuis plusieurs décennies, en assurant une cohérence des traitements, une harmonisation des outils au moment où commençaient à se développer les moyens micro-informatiques. Nous percevions, déjà à cette époque-là, la puissance énorme de cette micro-informatique et nous ne voulions pas la laisser aux mains d'initiatives locales dispersées, dont on a parfois un peu sous-estimé les capacités. Mettre en place des applications parfois appelées « système » - comme c'est le cas pour le système de traitement des infractions constatées, STIC - participait d'une volonté de réguler.

Cette volonté de cohérence a entraîné un besoin de réorganisation et d'adaptation ; en effet, si l'intelligence humaine a la capacité extraordinaire de pallier les inconvénients du traitement papier, ce n'est pas le cas de l'informatisation, et l'un de nos plus grands problèmes reste celui de la prévision, pour faire en sorte que les dispositifs automatisés puissent trouver des parades aux impondérables. L'autre conséquence de l'automatisation est juridique : s'il existe bien des règles en matière d'information de police judiciaire, on n'a jamais véritablement éprouvé la nécessité de les approfondir de façon très

précise. Avec l'automatisation, il a fallu mettre au point de façon extrêmement précise toutes les règles procédurales permettant de conserver, de traiter et ensuite d'utiliser de l'information à des fins de police - ce que nous avons fait avec l'aide de la CNIL et d'autres instances telles que la Chancellerie.

Le problème posé par l'informatisation n'est pas sans conséquences : on informatise pour plus d'efficacité, mais en même temps cette efficacité est largement compensée par une diminution des prérogatives du policier, allant dans un sens démocratique. Il devient donc nécessaire de définir la notion de personne mise en cause dans une procédure, ainsi que, de façon plus précise, la durée de conservation des informations, c'est-à-dire le droit pour la police de les utiliser pendant deux, cinq, dix ans, ou plus, sans oublier les règles d'épurement (avec les fichiers manuels, à classement alphabétique, on ne pouvait pratiquer d'épurement de données, à la différence d'un fichier automatisé).

Efficacité et par là même gain de temps pour l'enquêteur, temps qu'il peut alors consacrer aux victimes, et à davantage de rigueur : voilà quelques-uns des avantages que présente l'informatisation. Certes, une informatisation bien coordonnée a aussi ses dangers tant techniques que de sécurité, de confidentialité, et d'intégrité des données. Avec la puissance que nous avons entre les mains, il ne s'agit pas de laisser faire n'importe quoi par n'importe qui ; ce en quoi l'outil informatique

nous aide aussi : à la différence d'une consultation de fichiers manuels, l'informatique, on le sait, permet de garder la trace des précédents utilisateurs. Aussi ce changement donne-t-il du grain à moudre en ce qui concerne la formation aux règles procédurales et déontologiques des utilisateurs de ces systèmes. Quoi qu'il en soit, tous ces moyens technologiques ne doivent jamais faire oublier qu'ils ne sont qu'une aide à l'enquête : et d'ailleurs lors de la consultation du STIC, un affichage écran rappelle que c'est l'homme qui est l'enquêteur et jamais la machine, bien entendu.

ALAIN BELVEAU

L'informatisation ouvre un potentiel important, mais, me semble-t-il, tant qu'elle fait office d'outil ou de moyen et qu'elle déleste les policiers des tâches matérielles auparavant effectuées manuellement au profit d'une plus grande implication personnelle, notamment en direction des victimes. Voilà, à mon sens, le grand défi qui s'ouvre avec l'informatique quant à l'évolution, non pas des métiers de police, mais du métier de la police.

JEAN GUISNEL : *De ce premier état de la situation, il ressort globalement que l'informatique doit permettre de ramener les policiers à leur métier de base, à une pratique quotidienne, traditionnelle du contact humain. Ce qui est loin d'être encore évident. L'outil informatique ne reste-t-il pas étranger à la grande masse des policiers, en*

***tout cas dans ses possibilités ou dans ses devenirs. Qu'en pensez-vous ?***

PAUL LAGIER

En réalité, rejoignant ce que disait M. Karsenty, nos outils n'ont pas encore pénétré suffisamment nos services de police, c'est vrai. Mais il faut rappeler que notre métier est particulier et que la transformation des traitements manuels en processus automatisés n'a rien à voir avec ce qu'on a pu connaître dans la banque, les assurances, ou la gestion où il n'y a pas la même problématique des informations nominatives, du traitement des identités approximatives. Depuis 1985, l'un des plus grands problèmes réside dans la numérisation et le traitement de l'existant qui représente des millions et des millions de données, qu'il s'agisse des empreintes digitales, des antécédents des personnes ou des infractions, etc. Par exemple, en une année ce sont environ deux millions quatre cent mille infractions que la police enregistre. Il a fallu aussi élaborer de petits outils informatiques préparatoires à la mise en place d'un système plus cohérent. Après dix ans de travail, ce système a le mérite d'exister et d'avoir pénétré les services de base. Par exemple, le logiciel de rédaction des procédures du STIC touche aujourd'hui quelque 38 000 enquêteurs, et le logiciel CANONGE, qui permet le rapprochement criminel à partir des photographies des personnes mises en cause, est également très connu des utilisateurs de base. Globalement, l'informatique a

pénétré, mais des efforts restent à effectuer, notamment en matière de formation, de dotation en micro-ordinateurs, mais aussi en termes de communication externe et d'information dans les services.

YVES GUILLOT

L'exemple du réseau acropol est assez significatif des difficultés que peuvent poser de telles mutations. Lorsqu'il a fallu mettre en place ce réseau, des problèmes nouveaux se sont posés à l'État qui, par l'intermédiaire de la Direction des transmissions et de l'informatique du ministère de l'Intérieur, est devenu opérateur : celui-ci a dû passer des marchés, mettre en place une infrastructure de commutateurs de gestion, donc un réseau intelligent, et négocier des sites ; toutes choses qui, pour le ministère de l'Intérieur, s'avéraient totalement nouvelles par rapport à la situation antérieure de réseaux analogiques indépendants et généralement non cryptés. Il s'agit véritablement d'une culture nouvelle qui est celle des industriels, et qui maintenant vient rencontrer les besoins des opérationnels. Cette capacité d'adaptation est essentielle.

COLONEL HERNANDEZ

Pour ma part, je n'ai pas du tout le sentiment que l'informatique soit étrangère au personnel de la gendarmerie. En 1999, le ratio d'équipement de la gendarmerie nationale est d'un micro pour quatre personnels à peu près, et notre

objectif en 2002 est d'arriver à un micro pour deux. Compte tenu des rotations de personnels, on pourra estimer le ratio à un ordinateur par personnel disponible pour le service. Deuxième point, sur les 3600 à 4000 unités de gendarmerie, il n'y a qu'un seul service situé à Rosny sous Bois, qui développe les applications. Ce qui veut dire que la mise en service d'une application informatique au niveau des brigades de gendarmerie suppose la distribution de quatre à cinq milles supports-disquettes d'applications, puisque nos gendarmeries ne sont pas reliées par un réseau télématique. La procédure d'installation et le logiciel en lui-même ont un niveau de facilité en terme d'utilisation et de convivialité, sans lequel on ne pourrait travailler de la sorte. Les personnels ne se sentent donc pas étrangers à l'informatique en tant qu'utilisateurs.

JEAN-CLAUDE KARSENTY

Il est vrai que l'informatique doit être appréciée différemment selon les services de police auxquels on s'adresse. En PJ, dans certains services comme la Direction centrale du contrôle de l'immigration et de la lutte contre l'emploi des clandestins (DICCILEC), dans des services spécialisés, le recours à l'informatique est un élément prégnant. Cet accès à l'information jouera un rôle de plus en plus important avec tous les nouveaux systèmes qui vont se développer, à partir de Cheops, architecture qui permettra une mise en réseau complète des services entre eux.

En revanche, je répète que l'informatique représente une aide bien sûr au fonctionnement des directions départementales de sécurité publique, mais ne constitue pas en soi un bouleversement: des fichiers comme le Fichier des personnes recherchées (FPR) ou le Fichier des véhicules volés (FVV) ont toujours existé ; de manuels, ils ont été numérisés, leur consultation est bien sûr plus aisée, plus rapide, et permet des recherches multicritères, ce qui n'était pas le cas avant. Mais la fonction essentielle de ces polices reste malgré tout la police de proximité, le maintien de l'ordre. Certes, la police de proximité peut avoir besoin d'amasser des informations sur des individus, mais l'essentiel de son travail consiste à être présente, vigilante, à désamorcer des conflits, et éventuellement à arrêter les auteurs en flagrant délit. Il en va de même pour le maintien de l'ordre.

JEAN-PASCAL CODINE

Je voudrais rebondir sur les propos de M. Karsenty et M. Lagier, parce que nos services peuvent avoir des approches totalement divergentes. Par exemple, dans le cas de la douane, qui n'a pas de mission de « maintien de l'ordre » mais qui est plutôt une administration de contrôle et d'anticipation, l'informatique sert à devenir le plus invisible possible, au contraire des administrations sœurs, qui, elles, doivent se montrer sur le terrain dans une optique de dissuasion. Depuis des années, et particulièrement depuis

L'ouverture du grand marché intérieur en 1993, l'objectif est de contrôler sans que le bout du képi dépasse le sommet de la haie.

De ce fait, l'informatique est très ancrée dans la culture douanière pour diminuer les contrôles physiques, les interventions visibles sur le terrain, tout en ciblant et en faisant de l'analyse de risques au maximum. Pour le trafic de marchandises, on est passé de 50% de taux de contrôle physique il y a 25 ans, à moins de 3% aujourd'hui, avec des constatations qui ont considérablement augmenté, ce qui veut dire que le ciblage résultant de toutes nos bases statistiques a été très performant.

Grâce aux techniques de ciblage, nous avons pu abandonner le contrôle statique aux frontières, préjudiciable pour la liberté des flux de communication. Nous intervenons de manière plus mobile, sur beaucoup moins de cas, mais sur des cas permettant de faire des constatations, notamment en matière de stupéfiants, qui sont en augmentation constante.

RICHARD BROUSSE

Il me paraît tout à fait intéressant de revenir sur l'intérêt que représente pour les agences de sécurité cette sorte de liberté nouvelle.

À ce titre, M. Codine soulignait que la disparition des contrôles physiques aux douanes a permis *a contrario* et grâce à l'informatique une invisibilisation des contrôles.

JEAN-PASCAL CODINE

On peut sans causer d'entrave ou d'inconvénient à la population de référence que l'on traite, effectuer une qualification des risques, non pas sans que cette population le sache, mais plutôt sans qu'elle en soit incommodée. Les entreprises savent que dans les flux d'informations éventuellement échangés par voie d'échanges de données informatisées, une partie des informations sont déviées pour alimenter un processus de sélection qui ne touche en aval que certaines d'entre elles.

JEAN Guisnel : *Dans cette société où les informations s'échangent beaucoup plus qu'avant, je voudrais savoir quelles sont les répercussions de ce phénomène sur vos propres pratiques et les échanges d'informations que vous êtes amenés à effectuer entre vous...*

NICOLAS DUPEYRON :

...ou avec d'autres administrations, qui ne sont pas forcément dédiées directement au contrôle ou à la sécurité, telles que les administrations de la sphère fiscale ou sociale.

JEAN-CLAUDE KARSENTY

Ces échanges vont déjà bon train entre gendarmerie et police nationale : il y a, par exemple, mise en commun des fichiers automatiques, des empreintes digitales, échanges et mises à jour en temps réel des informations concer-

nant les fichiers véhicules volés et personnes recherchées. De la même manière, des échanges se font avec les pays Schengen, ou avec les assurances, sur un mode informatisé.

Auparavant, il était hors de question que ces informations puissent être échangées si facilement. Il est évident aussi que l'on n'aurait jamais pu imaginer que l'on puisse, dans un service de police, non seulement consulter un nombre important d'empreintes digitales pour identifier quelqu'un, mais partager également ces informations avec la gendarmerie. On voit naître une sorte d'imbrication des systèmes d'information de ces deux services avec une utilisation partagée des données. L'idéal serait qu'on puisse mettre en commun non seulement des informations, mais également les moyens de communication. Reste le problème de l'interface entre RUBIS et ACROPOL.

COLONEL HERNANDEZ

Ce problème d'interface est déjà réglé en partie.

JEAN GUISEL : ***Mais le plus simple n'est-il pas que gendarme et policier s'appellent sur leurs GSM respectifs ?***

YVES GUILLOT

Au moindre événement, le taux d'utilisation des GSM est tel que le réseau sature : l'expérience de la coupe du monde de football nous a montré qu'au Stade de France, on ne pouvait plus

passer de communications pendant les mi-temps. Le GSM n'a pas le profil idéal pour asseoir les communications des forces de sécurité en cas de crise. Qui plus est, celles-ci sont tout au plus numérisées mais non pas chiffrées. Enfin, cette technologie ne permet ni la téléphonie en conférence ni les groupes fermés d'abonnés, qui reproduisent en organisation informatique l'organisation opérationnelle des services. Il me semble que la combinaison de la confidentialité, d'un niveau suffisant de ressources et d'une fonctionnalité adaptée à un moment t, pose un problème qui n'est pas simple à régler, parce que c'est un croisement de capacités systèmes, de profils opérationnels et de ressources.

COLONEL HERNANDEZ

Sur ces questions-là, la gendarmerie a en quelque sorte été trop en avance : dès 1985-1986, nos ingénieurs avaient fait le pari, à l'époque relativement osé, du tout numérique. La longueur et le coût de ces programmes sont tels que nous avons commencé à mettre en place notre réseau de radio communication numérique, en même temps que ces technologies se sont déployées dans le civil. Nous utiliserons ce réseau jusqu'en 2015-2020. Mais si nous trouvons à cette échéance pour le renouvellement de notre réseau actuel un opérateur capable de fournir un réseau radio numérique pour forces de sécurité, qui remplisse le cahier des charges spécifique, il

n'est pas dit que nous ne nous tournions pas vers lui.

JEAN-CLAUDE KARSENTY

Il est difficile de projeter dans l'avenir les limites actuelles des systèmes. Les saturations du GSM aujourd'hui et l'absence des cryptages des réseaux satellitaires sont des données actuelles mais qu'en sera-t-il dans dix ans ? Le ministère de l'Intérieur a, pour le moment en tout cas, une philosophie tout à fait inverse. Même en ce qui concerne la transmission de données, le ministère a développé depuis très longtemps son réseau général de transport. Toutes les données, mais aussi la voix, passent par le RGT et le ministère est en train de multiplier sa capacité par dix afin de n'utiliser que cette liaison spécialisée, qui passe certes par des liaisons France Télécom, mais dont les nœuds de communication nous appartiennent puisque nous les avons achetés et mis en place. Par là, nous privilégions la sécurité, notamment du fait que ce réseau est privatif et donc plus difficilement attaquable que les autres. D'ici deux ans, une étude sera effectuée afin de savoir si nous pouvons externaliser une partie des transmissions de données, et, à ce moment là, revenir au plus offrant, mais en gardant malgré tout le RGT dans sa configuration actuelle pour toutes les transmissions confidentielles.

NICOLAS DUPEYRON

À propos d'anticipation, je tenais à signaler une recherche de deux cana-

diens, Ericson et Haggerty, qui ont travaillé sur ce thème de la police et de l'information. Ils montrent que l'information ne résout pas tout : les policiers qui, auparavant, étaient débordés de paperasserie et de procédures écrites dans leur travail quotidien, le sont aujourd'hui autant par l'information, par ce travail de tri et d'entrée des données dans les systèmes. Même si on rationalise davantage, le même genre de problèmes subsiste. La question de la formation se pose également telle que l'a souligné le colonel Hernandez à travers cette nécessité de devoir faire appel à ce que l'on a appelé des analystes stratégiques, ou en tout cas de savoir choisir entre les compétences que l'on a en interne dans les institutions de sécurité et des compétences qui relèvent d'un savoir d'expertise, d'un savoir technologique externe. Par ailleurs, dans ce même travail de recherche, les auteurs développent l'hypothèse selon laquelle le *Community Policing* nord-américain, proche de notre police de proximité, est essentiellement une police de l'information, et des communications. La proximité dans cet ordre d'idées serait, non pas de savoir ce qui se passe chez chacun de vous, mais d'avoir en tout cas des capacités de ciblage, de profilage d'une population beaucoup plus serrées que ce qui peut se faire actuellement.

PAUL LAGIER

Concernant ce risque de saturation par l'information, lorsque nous avons lancé

les projets de traitement informatisé, nous avons eu ce souci fondamental - que l'on a exprimé de façon un peu simpliste par la notion d'unicité de la saisie de l'information alors que les fichiers manuels obligeaient à autant de saisies qu'il y avait de traitements nécessaires. Je ne dis pas que nous atteindrons ce but aisément, mais une partie du chemin est déjà faite.

YVES GUILLOT

Pour revenir à la question de police de proximité, grâce à un réseau comme acropol, par voie hertzienne, on prolonge la transmission de données jusque dans les véhicules. Bientôt, à l'aide de la main courante informatisée, les fonctionnaires n'auront plus besoin de rentrer au service pour faire leur compte rendu d'intervention au chef de poste. Celui-ci sera effectué du véhicule par l'intermédiaire d'un terminal embarqué sur Acropol (TESA), et transmis directement en salle de commandement. Le ministère de l'Intérieur avait, dans un premier temps, initialisé, le réseau Siter, une technologie analogique avec la même fonctionnalité, mais qui nécessitait une infrastructure différente de l'infrastructure radio. Ce projet a été abandonné au profit d'Acropol et de TESA, qui présentent l'avantage d'utiliser une infrastructure unique. Autre gain en terme de proximité, l'informatique permet un recueil et une transmission d'informations plus précises entre les différentes équipes qui se succèdent sur le terrain.

FRÉDÉRIC OCQUETEAU

Je voudrais revenir sur les propos de Nicolas Dupeyron et les croiser avec les observations de M. Codine ; ce dernier faisait état d'une rencontre heureuse de la technologie et des douaniers dont le métier était en voie de redéfinition. Avec le ciblage et l'analyse des risques rendus possible par l'informatique, les douaniers seraient désormais plus efficaces. La maîtrise intelligente du renseignement permettrait de maximaliser la performance douanière. En même temps, il s'agit d'un processus différent de celui de la police, où la micro-informatique permettrait seulement et de façon plus classique de gagner du temps. Ma question est la suivante : ce processus d'informatisation est-il sans réelle conséquence sur l'identité professionnelle des policiers ou rend-il, comme c'est le cas pour les douaniers, l'agent de régulation plus dépendant de l'outil qui lui fournit des connaissances sur les situations à risques plutôt que des renseignements sur la personne ?

JEAN-PASCAL CODINE

Nous sommes effectivement plus dépendants dans la mesure où nous avons axé notre organisation sur ce type de gestion des flux d'information. Nous pourrions certes revenir à la seule vieille méthode du flair douanier mais nous perdriions alors tout ce bénéfice d'une connaissance cumulative. Dans la mesure où les règles sont harmonisées au niveau européen, nous



pouvons procéder à des échanges de spécialistes. Des analystes de risque tournent chaque année sur les pays de l'Union européenne, et un premier échange de spécialistes de la recherche de l'information sur l'Internet est envisagé, ce qui permettrait de bénéficier de l'expérience d'analystes douaniers de pays où les liens avec l'université sont sur ces questions très étroits.

JEAN-CLAUDE KARSENTY

En police, les conditions ne sont pas les mêmes. Nous ne sommes pas en mesure d'intervenir tant que l'infraction n'est pas commise, sauf en matière de stupéfiants où l'action policière est proactive, même si l'on peut penser que des gens qui ont des casiers judiciaires chargés sont plus enclins à commettre de nouveaux actes de délinquance. De même, dans les banlieues, des cellules de veille permettent de prévoir une situation explosive mais nous ne sommes pas arrivés à un tel système d'analyse de risque. Les policiers sont tout à fait capables de savoir quels sont les individus qui posent problème, quels sont les leaders, les chefs de bande, etc. Et après ? Le fait de savoir que des méfaits se préparent ne donne pas pour autant la clef de l'intervention. La douane est proactive tandis que la police attend l'infraction pour réagir. L'analyse de risque devra donc être complétée par des méthodologies très élaborées que nous ne maîtrisons pas encore.

COLONEL HERNANDEZ

La situation des douanes est assez particulière puisque les individus déclarent préalablement les marchandises qu'ils vont passer d'un pays à l'autre.

JEAN-PASCAL CODINE

Pas exactement, puisque nous faisons porter également l'analyse de risque sur tout ce qui est ciblage de trafic non-commercial. Les constatations effectuées et autorisées par la CNIL sont engrangées et permettent de définir des profils de types de véhicules, de comportements, des trafics à risque. Il s'agit de repérer des types de trafic commercial inoffensifs en soi, mais ayant de fortes probabilités de cacher une cargaison illicite complémentaire.

FRÉDÉRIC OCQUETEAU

Vous nourrissez-vous pour établir ces profils de vos propres données concernant les flux des personnes et de biens ou allez-vous chercher ces informations ailleurs dans d'autres administrations ?

JEAN-PASCAL CODINE

Jusqu'à présent, nous nous sommes contentés de notre information, mais nous explorons en profondeur le Net pour tenter d'obtenir des informations complémentaires, et nous recourons fortement à l'assistance administrative mutuelle internationale entre administrations douanières.

PAUL LAGIER

Au-delà du traitement de masse relatif à la sécurité publique et à la police de proximité, nous avons des traitements spécifiques pour la répression de la criminalité organisée, les stupéfiants, le blanchiment d'argent, le proxénétisme, le vol de biens culturels. Mais la priorité reste le citoyen...

COLONEL HERNANDEZ

Nous n'avons pas encore développé la capacité d'analyse de renseignement d'ordre public pour en dégager des grilles d'analyse du risque.

Jean GUISEL : *Internet et l'univers informationnel qu'il instaure marquent l'émergence d'un nouvel espace social que certains qualifient d'espace stratégique global mondialisé. Comment vos services peuvent-ils répondre à la criminalité que génère cet espace virtuel ?*

YVES GUILLOT

Il nous faut d'abord bien cibler l'impact des nouvelles technologies et les objectifs à protéger : le patrimoine, l'intelligence économique, la lutte contre les attaques aux intérêts fondamentaux de la nation, etc., pour pouvoir ensuite penser une riposte tant au plan juridique que physique et mettre en place des structures de veille, de façon préventive ou répressive, avec cette complication évidente des lieux d'agissements qui peuvent se situer hors de l'Hexagone.

Jean Guisnel : *D'autant plus que ce qui est qualifié d'infraction d'un point de vue juridique français peut ne pas l'être du point de vue d'une juridiction étrangère, par exemple sur des questions relatives à la pédophilie ou au racisme.*

PAUL LAGIER

De nouveaux défis sont créés par les nouvelles technologies. Les enquêtes portent à la fois sur les infractions informatiques, sur les infractions déjà connues mais commises à l'aide de l'informatique et leur corollaire de complexité et de puissance, sur les affaires économiques et financières, le terrorisme. Les compétences à déployer sont sans commune mesure avec le passé et posent un problème en terme de formation des enquêteurs. De plus, pour l'exploration de ces mémoires de masse, les moyens doivent suivre.

JEAN-CLAUDE KARSENTY

Certes, il faut des moyens supplémentaires, mais mon opinion personnelle, largement à contre courant, est que nous ne sommes qu'au début d'un processus actuellement totalement libéralisé. Il est en effet impossible pour le moment d'interdire quoi que ce soit sur Internet. Par ailleurs, la situation n'est pas préoccupante au point de déployer des mesures d'exception, dont d'ailleurs nous n'avons pas encore les moyens. Enfin, il ne semble pas que ce soit la priorité essentielle du ministère de l'Intérieur, ni du gouvernement qui

préfère accentuer ses efforts dans le sens d'un développement fort de la société de l'information. Dans quelques années, quand des excès importants auront été commis en France et en Europe, des moyens de contrôle se mettront probablement en place. Des cellules de veille existent, en effet, dans les différentes administrations de sécurité, mais le contrôle relève encore pour l'instant du bricolage.

**JEAN GUISNEL : *Les récents événements américains ne semblent pas vous donner raison. Le Communication Licency Act a été rejeté par la Cour suprême par deux fois au motif du principe de la protection des libertés individuelles contenu dans le premier amendement.***

JEAN-CLAUDE KARSENTY

Inversement, le fait que deux tentatives successives de contrôle d'Internet aient eu lieu en si peu de temps est déjà significatif d'un problème de fond. Et ce n'est pas la première fois que la Cour suprême finit par avaliser une modification constitutionnelle. Le tout, me semble-t-il, est une question de temps. Pour prendre un exemple récent qui nous concerne : sur des problèmes de racisme sur le minitel, la cour de cassation renvoie, après quinze ans d'hésitation, à la responsabilité des serveurs qui doivent se mettre en capacité de contrôler.

**JEAN GUISNEL : *Si la communauté Internet a su s'organiser d'un point de vue technique,***

***on constate par contre une l'absence de régulation éditoriale. Cette absence de règle ne représente-t-elle pas pour vous aussi, forcés de contrôle, une forme de liberté d'action ?***

ALAIN BELVEAU

La législation exige des preuves matériellement constituées. Il peut exister un monde virtuel mais non pas des infractions virtuelles, improbables par rapport à des procédures précises et qui, à la moindre erreur, sont cassées. C'est à mon sens un véritable problème : s'agirait-il de la mort annoncée des États au profit d'une communauté mondiale dominée par des organisations supra-nationales, économiques, qui maîtriseront les réseaux ?

JEAN-PASCAL CODINE

J'adopterai pour ma part un point de vue différent de celui de M. Karsenty. Concernant ce problème de la régulation, voici en substance le raisonnement de mes collègues douaniers américains : puisqu'il n'y a pas de droit et que nous pouvons techniquement faire des contrôles, ne nous en privons pas et le droit évoluera. L'approche libertaire des internautes trouve un contrepoint dans les pratiques administratives américaines. D'ici trois à cinq ans, avec les réseaux de communications SS7 qui permettront de fondre les transferts vocaux et de données, qui auront des serveurs de sécurité pour la gestion des réseaux eux-mêmes, il existera des

moyens pour contrôler tout ce qui passe. Avec la diffusion technologique, la planète entière se trouvera rapidement équipée de ce genre de protocoles de sécurité. Enfin, sans tomber dans la paranoïa, on peut noter que le gouvernement américain et plus particulièrement le *Department of Defence*, dit-on, aura en charge à 40% du développement d'Internet II. Cet effort pourrait ne pas être dénué de tout lien avec un souci de contrôle. Pendant que les libertés individuelles triomphent dans la bataille du *Communication Licency Act*, des techniciens travaillent pour développer de véritables moyens de contrôle. C'est une étape à ne pas rater.

YVES GUILLOT

Des groupes de travail de formation de policiers européens ont été institués. On y apprend à identifier et localiser des fichiers délictueux dans un serveur pour remonter à leur origine, à per-

quisitionner également dans les disques durs d'ordinateurs pour repérer les transactions informatiques incriminées et enfin à intercepter les flux de données échangées entre plusieurs ordinateurs. Des outils sont fournis, dont des traceurs de messages et des scanners. Enfin, on réfléchit actuellement au niveau européen à un statut juridique des fournisseurs d'accès.

NICOLAS DUPEYRON

Plus précisément, cette réflexion est le fait d'une proposition de directive à l'initiative conjointe de la Direction générale XIII-Télécommunications, marché de l'information et valorisation de la recherche - et de la direction générale XV-Marché intérieur et services financiers. de la Commission européenne ; elle est en cours puisqu'une première proposition de directive a été déposée. <sup>1</sup>

•••(1) NDLR : cf dans ce même numéro, internet et le droit à la sécurité, p. 62-67

# LE BOGUE DE L'AN 2000, UN RÉVÉLATEUR DE LA VULNÉRABILITÉ DE NOS LIBERTÉS.

par Daniel NAULLEAU

Le bogue de l'an 2000 sensibilise à la vulnérabilité des systèmes informatiques mais au delà des pertes financières, une dégradation des libertés est à craindre. Une « nouvelle vulnérabilité » s'installe qui découle de la complexité des systèmes, de leur incohérence, des réseaux et de facteurs humains. On devrait systématiser des évaluations globales des systèmes informatisés et développer une éducation à la vulnérabilité. Ce sont là les passages nécessaires pour ne pas vivre dans l'illusion de la sécurité propre aux nouvelles technologies de l'information.

**P**sychose collective ou risque majeur, la réelle difficulté pour certains ordinateurs et logiciels de passer le cap de dates fatidiques - dont l'entrée dans les années 2000 - a tout de même un effet positif. Les décideurs et l'opinion publique prennent enfin conscience de l'extrême dépendance de la « société de l'information » vis-à-vis des puces informatiques. Pourtant, dès 1979, le rapport suédois SARK (SARK, 1979) pointait déjà cette dépendance, mais il prêchait alors quasiment dans le vide (LAGADEC, 1988).

••••(1) Annuels depuis 1982 appelés Securicom puis intégrés au salon Infosec depuis quelques années, ces conférences sont de bons indicateurs des préoccupations en terme de sécurité informatique.

Au fil des colloques Securicom-Infosec<sup>1</sup>, il est devenu clair que la vulnérabilité n'était qu'affaire de spécialistes, sans qu'une réelle inquiétude touche ceux qui devaient s'en préoccuper, et leur fasse prendre conscience que leur entreprise, la société dans son ensemble acquérait *via* l'informatique un type de vulnérabilité inconnu jusqu'à présent.

Au-delà des aspects financiers généralement mis en avant, ce sont nos modes de vie, nos libertés qui sont de plus en plus tributaires des nouvelles technologies. Les

exemples, nombreux, permettent de retenir quatre causes principales à cette « nouvelle vulnérabilité ». Développer les quelques solutions qui se dessinent semble nécessaire si l'on veut en réduire les risques.

## REMISES EN CAUSE DE NOS LIBERTÉS

L'homme a toujours cherché à se protéger des aléas de la vie, des dangers de la nature, grâce à des dispositifs de plus en plus sophistiqués. L'automatisation, et en particulier l'informatisation essentiellement par la numérisation et les réseaux, lui fournit depuis quelques années d'indiscutables moyens de se sentir moins vulnérable, plus libre par rapport aux contraintes naturelles. Mais les accidents, incidents, cybercrimes et autres catastrophes plus ou moins directement liées à l'informatique et aux automatismes, sont trop fréquents pour n'être que des épiphénomènes.

Nos machines sont à la merci d'un embargo commercial sur les pièces de rechange, de sanctions économiques<sup>1</sup>. Elles dépendent bien trop de quelques individus sur lesquels reposent tout le savoir faire, ce qui leur confère un rôle clef excessif. Sans même parler des risques en temps de guerre ou d'invasion, l'espionnage industriel est facilité par nos négligences et notre insouciance.

Les logiciels sont devenus tellement complexes, constitués d'une superposition de couches aux interfaces incertaines qu'il devient totalement impossible d'en certifier le bon fonctionnement, même s'il reste bien quelques domaines où l'on peut s'approcher d'une certaine certitude, comme dans la conquête spatiale. La décision de lancer l'arme atomique repose sur une multitude de détecteurs et de décisions automatisées et humaines dont la fiabilité globale n'est pas avérée.

L'État-Nation, traditionnellement souverain, doit faire face à des décisions prises ailleurs, par des groupes transnationaux qui font un grand usage des réseaux (flux financiers, délocalisations des entreprises facilitées par les réseaux). Son libre arbitre s'est réduit comme une peau de chagrin et il lui est difficile d'influer sur son propre avenir.

•••• (1) On se préoccupe seulement depuis peu de créer une alternative européenne au réseau de satellites de positionnement américain GPS.

••••(1) Voir les commentaires des médias sur les difficultés de mise au point du porte-avions Charles de Gaulle.

Relatés par les médias, les incidents quasi quotidiens liés à l'informatique, sont souvent vus d'un œil goguenard par l'opinion publique, comme une incapacité de la technique et des techniciens à maîtriser l'informatique<sup>1</sup>. Les aspects financiers sont principalement mis en avant et parfois l'on souligne que le dispositif est particulièrement dépendant de quelques millimètres carrés de silicium. Mais les causes et les conséquences d'une telle fragilité sont rarement analysées. On ne fait surtout pas le lien avec les libertés individuelles et publiques mises à mal et cette nouvelle situation.

L'exercice des libertés individuelles et publiques est de fait de plus en plus indissolublement lié à des systèmes informatisés : communiquer (pannes téléphoniques), se déplacer (écroulement du système informatique de l'aéroport de Hong Kong lors de son lancement), se nourrir, se soigner (accident de scanners), s'informer (difficultés de l'informatique à la Bibliothèque nationale de France), voter (la fiabilité des logiciels de vote électronique est fortement critiquée aux États-Unis), travailler, s'éduquer, avoir une vie privée (abus de la vidéo surveillance ou du fichage), etc.

Qui plus est, les nouvelles libertés «viennent» de plus en plus avec un nouveau fichage, et les risques qui vont avec. Les horaires «libres» vont de pair avec le badge et le fichier qui lui correspond. La faculté d'obtenir de l'argent aux quatre coins du monde avec une carte bancaire nécessite un fichage précis. Cette traçabilité est évidente avec le développement de l'usage des téléphones portables cellulaires. La libre circulation entre certains pays européens de l'espace de Schengen s'appuie sur le fichier SIS (Système d'Information Schengen). Le commerce électronique à distance par Internet entraîne, en général à notre insu, le développement de bases de données comportementales par les *cookies* et autres dispositifs de flicage informatique<sup>2</sup>.

••••(2) Voir le site de la CNIL et ses pages sur les «traces» informatiques : [www.cnil.fr](http://www.cnil.fr).

Toute perturbation des systèmes informatiques interfère avec nos vies et nos libertés ; on peut légitimement se demander si toutes nos libertés, «informatico-dépendantes», n'en pâtissent pas.

## CARACTÉRISTIQUES DE LA NOUVELLE VULNÉRABILITÉ

Dans cette « société du risque » dont parle Ulrich Beck (BECK, 1997), l'informatisation à outrance avec d'évidentes et fantastiques possibilités, est celle d'une invulnérabilité illusoire. Pour ma part, je pense depuis longtemps qu'une « nouvelle vulnérabilité », sournoise, est apparue, liée aux fragilités de l'informatisation (NAULLEAU, 1990). L'exemple récent de l'hôpital de Lyon nous rappelle opportunément que notre confiance aveugle en la technologie peut avoir des effets pervers. La surveillance humaine des groupes électrogènes de secours y avait été remplacée par de la télésurveillance qui n'a pas correctement fonctionné. Une panne électrique et la situation bascule dans l'incontrôlé.

Les causes de cette « nouvelle vulnérabilité » sont à rechercher dans quatre directions.

La complexité croissante des systèmes pour le plaisir du technicien, pour répondre à la pression de l'opinion publique qui confond sécurité et sécuritaire et qui veut toujours plus d'informatique après l'accident de train, ou des décideurs qui sont friands de méga-statistiques toujours plus inquisitoriales. C'est la fuite en avant. Or la panne est consubstantielle de la complexité. Comment tester les dizaines de millions d'instructions de Windows ou des puces hyper-intégrées ? Comment mémoriser tous les codes secrets, si ce n'est sur des post-it au coin de l'écran ? Un *bit* erroné, un bogue et tout s'arrête. La disproportion entre la cause et ses conséquences est caractéristique.

L'incohérence des systèmes informatiques a des origines diverses, mais toutes préjudiciables. Souvent ce sont des raisons économiques ou de propriété industrielle, qui conduisent à construire des systèmes incohérents (versions incompatibles des logiciels sur et entre PC). Les normes-constructeurs sont par définition incompatibles. Les chiffrement par DES très utilisés sont certes plus économiques que ceux avec RSA mais de loin moins performants. L'organisation largement informatisée du « *just in time* » destinée à réduire les coûts des immobilisations conduit fréquemment à immobiliser l'entreprise à court



de pièces. Il n'y a plus de marge d'erreur, de place pour gérer l'incident.

Dans les vastes réseaux d'entreprise incluant des milliers de postes de travail, en terme de niveaux de protections l'incohérence prévaut. Or, l'on sait que la valeur d'une chaîne ne peut être déduite que de son maillon le plus faible. La stratification des informatisations mélange le travail de nombreux informaticiens, depuis parfois des décennies, dans des langages différents aux interfaces approximatives.

À la base de l'enseignement de l'informatique le concept de la «boîte noire», s'il permet de fournir des schémas conceptuels simples, est pervers car il véhicule l'idée que l'on peut concevoir des dispositifs où les composants pourraient être indépendants et sans autres interférences que celles prévues par le concepteur.

La dépendance vis-à-vis des réseaux est fondamentalement la cause de la nouvelle vulnérabilité car malgré le développement du maillage - à la base de l'Internet - les réseaux restent toujours à la limite du *collapsus*, prêt à s'écrouler comme châteaux de cartes (voir les récents arrêts de serveurs aux États-Unis). Or l'échange de données qu'il soit lié à la centralisation des décisions <sup>1</sup> ou à la décentralisation des organisations, pose alors problème. Deux situations opposées, la concentration géographique<sup>2</sup> ou la délocalisation des fichiers, des centres de décision ou d'élaboration des logiciels (voir la politique de la Swissair en Inde et en Asie), sont tout aussi problématiques.

Le maillage, qui plus est, a l'inconvénient paradoxal que pour les échanges sécurisés, il est quasiment impossible de connaître le trajet des informations et d'être certain que le niveau de sécurité est homogène sur l'ensemble du parcours, ce dernier étant susceptible de varier d'une transaction à l'autre. Or l'usage des EDJ est croissant. De même, je peux me demander où sont mes fichiers, où se cachent mes données personnelles sur Internet ?

Les facteurs humains restent déterminants. Les explications sont à rechercher du côté des défauts ergonomiques, des interfaces déficientes ou indigentes et ambiguës, de l'excès de confiance dans la technique, des relâchements

••••(1) Le métro Météor sans conducteur nécessite de la vidéo surveillance et une centralisation des systèmes de commande.

••••(2) Le site de Paris-La Défense offre une très forte densité d'ordinateurs. Qu'est-il prévu en cas de panne électrique ?

d'attention, de la routine, de la déresponsabilisation, de la perte du savoir-faire, du stress, de la disparition de la maîtrise des solutions manuelles en mode dégradé (LEPLAT, 1990). Sans oublier les erreurs de programmation (bogues), les logiques mal maîtrisées des systèmes experts (ou des « *program trading* » en bourse), les cybercriminels. Et il y a de la place pour toutes les variétés de cybercriminels : pirate, espion, fraudeur, hacker, maître-chanteur ou informaticien en mal de vengeance (ROSÉ, 1991). Le développement de l'alphabétisation informatique augmente mathématiquement le nombre de cybercriminels potentiels.

Même si la maîtrise de l'informatique s'appuie sur une documentation, ce qui est rarement le cas, elle n'est pas aisément transmissible. Elle relève de la connaissance d'un groupe d'individus autour du service informatique. Quelles situations ingérables risqueraient alors de se produire en cas de mobilisation générale des réservistes ?

## DES SOLUTIONS

Les spécialistes de la sécurité informatique s'évertuent à améliorer le niveau de fiabilité des systèmes, à mettre en place des plans de secours et des solutions de repli, mais sans arriver à impliquer vraiment les utilisateurs. Il faut aller plus loin : une bonne sécurité, là comme ailleurs, doit être l'affaire de tous. La réflexion n'est pas nouvelle mais est plus que jamais d'actualité (BERLEUR, 1993). Je pense qu'elle peut se résumer en deux axes : évaluer et éduquer.

### ÉVALUATION DES SYSTÈMES INFORMATIQUES (*TECHNOLOGY ASSESSMENT*)

L'évaluation des systèmes informatiques, ou plus généralement informatisés, s'appuie sur des méthodes classiques comme *Marion* ou *Melisa* ou encore ITSEC<sup>1</sup> qui servent à repérer les faiblesses et tenter d'améliorer la protection. Mais il faut prolonger ces démarches en analysant les conséquences de l'informatisation en situation normale et en cas de dysfonctionnement : disponibilité des dispositifs, nature des solutions de repli, fonctionnement réel des solu-

••••(1) *Information Technology Security Evaluation Criteria*, ensemble de critères définis au niveau européen par la DG XIII.

tions dégradées, dangers nouveaux ou persistants, atteintes aux libertés, risques économiques. Il faut, loin de l'arrogance des techniciens, une approche globale, «écologique» lors d'enquêtes globales et contradictoires, en s'inspirant probablement de procédures qui se mettent en place dans les problèmes d'environnement.

Les décideurs, les politiques n'ont pas toujours une vision précise des risques liés à l'informatisation, et les solutions qui leur sont fournies ne sont souvent qu'une couche d'informatique de plus. Pourquoi tendre toujours vers le tout informatique ? Faut-il connecter toutes les machines aux réseaux ? ou faut-il préférer des dispositifs à sécurité positive qui, en cas de panne, «retombent» naturellement du bon côté de la sécurité et qui, de plus, ne soient pas liberticides ? Ainsi, le paiement avec un porte monnaie électronique ne laisse pas de traces comme le paiement avec une carte bancaire, il est donc intrinsèquement moins liberticide.

Mais rien n'est simple : la cryptographie protège nos échanges privés mais favorise les mafias. Les sites miroirs échappent à la censure mais peuvent être les refuges d'extrémistes. Faire simple ne veut pas nécessairement dire qu'il faut privilégier les PC plutôt que les centres informatiques car les PC sont très difficiles à protéger. Quand on demande plus d'informatique après un accident de transport, plus de vidéo-surveillance face à la délinquance, est-ce la bonne démarche ? Plus on s'éloigne de la situation à gérer, plus le contrôle devient froid, déshumanisé, décontextualisé. Et si on ajoute un dispositif de protection il ne doit pas être testé seul mais en situation <sup>1</sup>.

•••(1) Voir précédemment les risques liés au concept des boîtes noires.

•••(2) Il est tout de même parfois fait état de la possibilité de détruire des fichiers en situation de crise.

•••(3) Voir le vote en Décembre 98 sur l'introduction du numéro de sécurité sociale dans les fichiers fiscaux.

Avec les grands fichiers de population : casier judiciaire centralisé à Nantes, RNIPP (Registre national d'identification des personnes physiques, RIAM (Registre national inter-régimes de l'assurance maladie), SIS de l'espace Schengen, nous mettons tous nos «œufs dans le même panier». Le bilan coût/bénéfice est certes réalisé par la CNIL mais si la sécurité n'est pas oubliée, le risque de vulnérabilité éventuellement induit est peu présent dans ses analyses <sup>2</sup>. Des interconnexions sont lancées sans qu'une étude des risques informatiques générés soit menée <sup>3</sup>.

Où sont les plans d'urgence de nos administrations ? Où sont les plans ORSEC-informatiques qui, s'ils existent, restent bien discrets ?

## ÉDUCATION À LA VULNÉRABILITÉ

Petit à petit, la confiance s'installant, nous négligeons la mise en place de dispositifs palliatifs. Peu d'entreprises, en particulier de PME et PMI, se sont vraiment posées le problème de leur survie en cas de panne informatique majeure. Seules de grosses entreprises, les militaires, les marins ou encore les aviateurs par tradition, par culture, cherchent à se mettre à l'abri des conséquences des pannes. Il s'agit de former informaticiens, techniciens, décideurs, à la panne et à ses conséquences. Mais aussi former le citoyen à ne pas dépendre entièrement de dispositifs fragiles. Selon les assureurs allemands, le système de freinage ABS n'a pas fait baisser le taux d'accident. Le système de positionnement par satellites GPS n'empêche pas les naufrages et on peut même observer que la vigilance des plaisanciers s'est amoindrie. Moitessier ou Slocum ont réalisé des circumnavigations sans dommages dans des mers où, lors des courses autour du monde, les naufrages se succèdent, cinquante ou cent ans de développement technologique plus tard. Actuellement, les nouvelles technologies endorment nos réflexes de protection, créent des illusions de sécurité, un peu comme les assurances ou l'État providence. On s'évertue à demander aux seuls techniciens de résoudre nos problèmes. Et on s'étonne de voir la nature nous résister en montagne (avalanches) ou en plaine avec les inondations par exemple <sup>1</sup>. « *De la société de peine à celle de la panne* » dit Yves Lasfargue (LASFARGUE, 1987). Où est la culture de la panne, la grande inconnue des ingénieurs, demande-t-il ? On continue de confondre prouesses techniques et sécurité. Il convient pourtant d'apprendre à vivre avec les pannes. Il en va de la survie de nos libertés.

•••(1) On continue de construire des usines automatisées dans des zones inondables.

## CONCLUSION

Effectivement rien n'est simple car, par exemple, si la documentation des systèmes et des logiciels souvent

••••(1) C'est l'excuse mise en avant dans certaines intrusions de systèmes informatiques. La tentation est trop forte, disent les *hackers*.

••••(2) Peut-être ne faut-il plus s'étonner d'avoir des difficultés à trouver des édiles quand on sait qu'une grande part de leurs responsabilités légales sont partiellement prises par des systèmes sur lesquels ils n'ont pas prise.

embryonnaire, est trop précise, et comme cela est parfois le cas, accessible en ligne, elle offre alors les plans du coffre à ceux qui veulent attaquer une installation. La normalisation des solutions sécurité, si elle permet d'estimer le niveau de sécurité d'une installation permet paradoxalement aux cyberterroristes ou criminels de mieux connaître leur cible<sup>1</sup>. Mais évaluer globalement les conséquences des risques informatiques sur tous les plans, y compris en terme d'impact sur nos libertés, et développer en cohérence une éducation à la sécurité, sont deux enjeux majeurs.

On peut se demander quelle part il reste à l'homme dans les processus décisionnels. Saurait-il encore agir en cas de panne de ses aides à la décision ? La prolifération des aides à la décision est irresponsabilisante<sup>2</sup>, et c'est une irresponsabilité machinique qui s'instaure tranquillement.

Il faudrait aussi s'intéresser, bien au-delà des impacts économiques des risques informatiques, aux conséquences quotidiennes sur le stress des utilisateurs. Stress engendré par les micro-incidents quotidiens ou inquiétude pouvant advenir chez ceux qui ont déjà perdu des données, subi les aléas des réseaux, vu leurs responsabilités diluées dans des logiciels plus ou moins experts, dû se battre au quotidien avec des logiciels toujours plus incompatibles avec les anciennes versions et des fonctionnalités nouvelles mais inconnues, ou enfin géré une dégradation de l'image de marque du service rendu pour cause d'incident-machine (LASFARGUES, 1993).

La vulnérabilité de l'informatique est claire, celle de l'informatisation l'est moins. Et dans l'opinion publique la vulnérabilité de la société informatisée et de l'homme pas encore, malgré les nombreux articles sur le bogue de l'an 2000. Il en va pourtant de nos droits et libertés.

#### ■ Daniel NAULLEAU

*Université de Pierre et Marie Curie-CREIS*

## BIBLIOGRAPHIE

- BECK (U.), 1997, «Le concept de Société du Risque», *Risques*, N° 32.
- BERLEUR (J.), BEARDON (C.), LAUFER (R.), 1993, *Facing the challenge of risk and Vulnerability in an Information Society*, IFIP Transactions A-33, North Holland, Amsterdam.
- LACROIX (G.), NAULLEAU (D.), 1995, «Maîtriser l'informatisation», *Manière de voir, Le Monde Diplomatique*, N°27.
- LAGADEC (P.), 1988, *États d'urgence, Défaillances technologiques et déstabilisation sociales*, Seuil, Paris.
- LASFARGUES (Y.), 1987, «De la peine à la panne», in *Le Monde*, Paris, 22 août.
- LASFARGUES (Y.), 1993, *Robotisés, Rebelles, Rejetés ? Maîtriser les changements technologiques*, Les éditions de l'Atelier, Paris.
- LEPLAT (J.), de TERSAC (G.), 1990, *Les facteurs humains de la fiabilité dans les systèmes complexes*, Octares, Marseille.
- NAULLEAU (D.), 1990, «Vulnérabilité et Libertés», in *Journal de Réflexion sur l'Informatique*, N° 17, Namur, Juillet.
- NAULLEAU (D.), 1993, «The new vulnerability: some ideas to face it», in BERLEUR (J.), et al., *Facing the challenge of risk and vulnerability in an information society*, IFIP, North-Holland, Amsterdam.
- NAULLEAU (D.), 1995, «Vulnérabilité : où vas-tu ?», *Journal de Réflexion sur l'Informatique*, Belgique, Namur, Mars.
- NAULLEAU (D.), 1995, «Information society and the New Vulnerability», *Summer School, ISAT'95*, Biblioteka Informatyki, Wrocław, Pologne.
- Richard (C.), NAULLEAU (D.), 1996, «La sécurité sur les réseaux», *Terminal* N°71/72.
- ROSÉ (P.), 1991, *La criminalité informatique à l'horizon 2005, analyse prospective*, FORS-IHESI, Paris.
- SARK, 1979, *The vulnerability of the Computerized Society, considerations and proposals*, (dit rapport SARK), Swedish Ministry of Defense, Stockholm.

# INTERCONNEXIONS ET FICHIERS POLICIERS

## deux débats de notre temps

par Joël BOYER

Face à l'avènement de la société de l'information, les modes de contrôle et d'intervention de la CNIL doivent évoluer afin que l'informatique ne permette pas ce que le législateur a entendu proscrire. L'interconnexion de fichiers doit rester l'exception, de même qu'une vigilance particulière quant à l'utilisation et la diffusion du NIR est nécessaire. Concernant l'action de la police judiciaire, le tiers autorisé, la CNIL prône une plus grande transparence, notamment en garantissant un droit d'accès indirect. Enfin, la multiplication des traces informatiques qui touchent à nos activités privées pousse l'auteur à s'interroger sur le droit à l'oubli, nécessaire à l'équilibre d'une démocratie.

La loi « informatique et libertés » a un peu plus de vingt ans et une directive européenne du 24 octobre 1995 impose de la réformer. En vingt ans le paysage a considérablement changé : les fichiers les plus considérables ne sont plus forcément ceux de l'État ou des administrations. A l'heure du « *data mining* » et d'Internet, l'information nominative a acquis une valeur marchande, les « profils » s'achètent et se vendent, un marché est né, suscitant de nouvelles inquiétudes et appelant sans doute à une vigilance d'une autre nature que celle à laquelle le législateur de 78 avait songé. Pourtant, la fin de l'année 1998 aura été marquée par deux débats publics, autant que passionnés : l'un concernait les interconnexions de fichiers, l'autre un fichier de police, dénommé STIC, pour système de traitement des infractions constatées. Comme il y a vingt ans.

La CNIL se trouve à la croisée de ces chemins, participant à ces débats en même temps qu'elle en est l'objet.

Impatiente de connaître les grandes orientations de la prochaine transposition de la directive, elle est sollicitée pour évoquer ces deux thèmes, ce que le rédacteur de ces lignes fait de bonne grâce, à peine fâché de passer pour archaïque à l'heure où l'entrée de la France dans la société de l'information offre tant d'occasions de se découvrir «branché». A peine osera-t-il préciser, en manière d'excuse, qu'il n'a choisi ni le thème de cette contribution à la revue, ni l'actualité de ces deux débats.

### LES INTERCONNEXIONS DE FICHIERS

La loi du 6 janvier 1978 puise ses origines dans la crainte que l'informatisation de l'administration et les interconnexions entre fichiers publics portent atteinte à la liberté des citoyens. Il est vrai que la dénomination d'un projet, imaginé par l'administration en 1974, consistant à interconnecter l'ensemble des fichiers publics grâce au numéro de sécurité sociale, pouvait faire craindre le pire : «SAFARI ou la chasse aux Français» avait malicieusement titré Philippe Bouchet dans un article paru dans le journal *Le Monde*. C'est la révélation de ce projet qui a conduit le Gouvernement de l'époque à confier à une commission de réflexion, présidée par le vice-président du Conseil d'État, M. Bernard Tricot, le soin de définir les garanties qui devaient être offertes aux citoyens face à l'informatisation de la société. Un projet de loi, ensuite déposé devant le Parlement, devait aboutir à la loi du 6 janvier 1978, dite «loi informatique et libertés».

Cette loi porte trace de cette histoire : elle traduit une vigilance particulière à l'égard des fichiers publics, une méfiance marquée à l'égard des interconnexions de fichiers et la conviction que l'usage du numéro de sécurité sociale, autrement appelé numéro d'inscription au répertoire (NIR), devait être étroitement encadré.

La loi de 1978 est incontestablement rigoureuse à l'égard des fichiers publics : ils ne peuvent être mis en œuvre qu'après avis favorable de la Commission tandis que les fichiers du secteur privé obéissent à une simple procédure de déclaration.



Les interconnexions de fichiers sont assimilées à de véritables traitements qui doivent, en tant que tels, être subordonnés à l'avis de la CNIL. L'utilisation du répertoire national d'identification des personnes physiques, tenu par l'INSEE, et qui associe à chaque personne un numéro d'identification spécifique, ne peut être autorisée que par décret en Conseil d'État pris après avis de la CNIL.

Cette histoire, mais aussi ces dispositions légales, expliquent que, saisie d'un projet d'interconnexion entre fichiers, la CNIL s'assure en premier lieu que l'échange d'informations peut légalement avoir lieu. Or, tel n'est pas toujours le cas. Ainsi, si des informations sont protégées par le secret professionnel ou par un secret particulier (médical, bancaire, fiscal, statistique), l'échange d'informations, c'est à dire leur divulgation à un organisme tiers, ne peut intervenir que si ce secret est préalablement levé par la loi. Il s'agit là d'un principe fondamental : l'informatique ne doit pas permettre de faire ce que le législateur a entendu proscrire.

A ce stade, il ne s'agit pas pour la CNIL de procéder à un contrôle d'opportunité, comme on le croit encore trop souvent et comme on en fait quelquefois le grief à la Commission, il s'agit pour la Commission, comme pour toute autorité publique, de s'assurer qu'un projet dont elle est saisie n'est pas contraire à la loi. Quel serait le crédit d'un État qui assurerait que certaines informations sont protégées par le secret, si ce secret était en pratique et automatiquement éventé par le biais d'interconnexions entre organismes différents ? Quel serait d'ailleurs le crédit des dépositaires de ces secrets - médecins, banquiers, institut national de la statistique - si, hormis les cas prévus par la loi, des liaisons informatiques permettaient de révéler ce que la loi a entendu garantir du sceau du secret ?

C'est cette raison qui a conduit la CNIL, à titre d'exemple, à interdire aux maires, à l'occasion du recensement général de la population organisé par l'INSEE, d'utiliser pour leur propre compte - et fut-ce à des fins exclusivement statistiques - les données collectées, couvertes par le secret statistique. La sincérité des réponses et donc l'exactitude du recensement exige que les personnes aient l'assurance

qu'aucune autorité autre que l'INSEE ne puisse disposer de ces données. Le secret statistique est pour l'État la condition absolue de la fiabilité du recensement et, pour les citoyens, la garantie que leurs réponses ne seront pas exploitées à des fins étrangères à celles pour lesquelles elles sont collectées.

De même, lorsqu'elle a été saisie de la généralisation d'une expérimentation tendant à rapprocher les fichiers de la redevance de l'audiovisuel avec ceux de la taxe d'habitation pour identifier les personnes n'ayant pas déclaré la possession d'un poste, la Commission a demandé que la loi soit préalablement modifiée pour autoriser une telle utilisation, par le service de la redevance, d'informations couvertes par le secret fiscal.

Ce préalable levé, la CNIL a pour mission première de s'assurer que les personnes concernées ne seront pas tenues dans l'ignorance de l'interconnexion. Il s'agit là d'un principe commun à toutes les législations de protection des données : les personnes doivent être informées du sort des données collectées et tout particulièrement des organismes ou autorités qui en seront destinataires. Ainsi, en matière de contrôle des conditions de ressources auxquelles est subordonné le versement de bon nombre d'allocations, la Commission demande que les allocataires de prestations sociales soient informés, lorsqu'ils remplissent leur déclaration, du caractère systématique et automatisé des vérifications qui seront opérées. Il s'agit là pour l'État d'une obligation de loyauté à l'égard des citoyens et, au demeurant, de la plus efficace des mesures pour prévenir toute tentative de fraude.

Et le NIR ? Fidèle à la genèse de la loi, la CNIL a toujours manifesté des réticences à ce que, au seul motif de faciliter des interconnexions, une administration puisse disposer du numéro d'identification au répertoire si elle n'a pas été préalablement autorisée à l'utiliser pour la tenue de ses propres fichiers. Il s'agit là d'une réserve réfléchie qui a conduit la Commission à limiter l'extension de l'usage de cet identifiant à la sphère « médico-sociale ». Dans ce dernier domaine, en effet, la CNIL a, dès l'origine, pris acte que le NIR avait été utilisé comme identifiant par la plupart des

organismes de sécurité sociale et autorisé l'enregistrement de ce numéro dans tous les traitements concernant les opérations en lien avec la sécurité sociale.

#### UNE UTILISATION INCONSCIENTE DU NIR

Rapportée à la problématique des interconnexions, cette position de la Commission signifie que si deux administrations sont autorisées à utiliser le NIR, chacune pour ses propres fichiers, et à procéder, entre elles, à des échanges d'informations, sous les garanties précédemment définies, le NIR peut évidemment être utilisé dans le cadre de ces échanges : l'efficacité de l'interconnexion, autorisée et transparente, pourra alors - peut-être - s'en trouver accrue sans qu'aucune des deux administrations qui se communiquent des informations ait connaissance d'une information dont jusqu'alors elle n'aurait pas disposé.

En revanche, la CNIL a toujours considéré que la seule nécessité d'établir une interconnexion entre fichiers ne justifiait pas, à elle seule, qu'une administration qui ne dispose pas du NIR puisse s'en doter. Cette position est incontestablement mal comprise, et parfois mal acceptée, par les administrations. Elle a été exposée, une dernière fois, dans une importante délibération de la Commission du 25 mars 1997 portant avis sur un projet de loi destiné à compléter le code de la sécurité sociale pour autoriser l'administration fiscale à utiliser le NIR.

Le risque, dès lors que les interconnexions se multiplient, d'une diffusion du NIR, par capillarité, d'un organisme à un autre, a alors été souligné par la Commission, de même que celui qu'engendrerait le fait qu'un très grand nombre de fichiers administratifs ou privés puissent, en étant interrogés sur la base de ce même numéro, « sur cette seule information, les révéler toutes ».

A ces arguments, s'ajoutaient deux motifs de préoccupation. D'abord le fait que peu à peu un numéro se substitue à l'état-civil des personnes. Le président Guy Braibant a rappelé, dans son rapport sur la transposition de la directive européenne, la grande sensibilité de l'opinion à ce sujet. Ensuite, que l'utilisation du numéro de sécurité sociale ne

transforme, sans que nul ne s'en aperçoive, les fichiers de la sécurité sociale en fichiers de domiciliation, à inscription obligatoire, et à la disposition de toutes les administrations. Sur ce dernier point, la Commission s'est toujours bornée à souligner qu'il n'appartenait pas à une autorité administrative, fût-elle indépendante, de porter un tel projet et qu'il revenait au seul législateur d'en décider.

La récente Loi de finances pour 1999 a en partie tranché le problème. Elle autorise les administrations financières à utiliser le NIR, mais non sans précaution. Il doit à cet égard être souligné que dans sa décision du 29 décembre 1998, le Conseil Constitutionnel précise que les seuls échanges d'informations pouvant comporter le NIR concernent d'une part, les échanges entre les administrations financières elles-mêmes (direction générale de la comptabilité publique, direction générale des impôts, direction générale des douanes) et, d'autre part, les échanges entre ces directions et les organismes et services chargés de la sécurité sociale. Le risque d'une diffusion du NIR, hors la sphère nouvelle où il vient d'être introduit, paraît dès lors, en l'état, être encadré, comme la Haute-Juridiction l'a fait savoir par un communiqué de presse précisant que «l'utilisation du numéro de sécurité sociale par l'administration fiscale [...] n'a été admise qu'au prix de réserves d'interprétation, la portée [de la disposition critiquée] devant rester restreinte.»

140

#### TROIS DOGMES DE LA CNIL CONCERNANT LE NIR

Le débat ouvert sur les interconnexions de fichiers et les libertés publiques ne serait pas tout à fait complet si l'on taisait trois réflexions dont la CNIL s'est souvent fait l'écho.

La première de ces réflexions est d'ordre technique : contrairement à ce qui est souvent prétendu ou espéré, le NIR ne constitue pas la «solution miracle» aux interconnexions. Les bilans des interconnexions autorisées entre fichiers publics dont la CNIL a connaissance attestent que les échanges d'informations, même sur la base du NIR, entre deux administrations ou organismes qui en disposent, connaissent un «taux d'échec» de l'ordre de 5 %. On peut

alors, selon sa philosophie personnelle, regretter que l'informatique ne puisse pas rendre de meilleurs services à l'État gestionnaire ou au contraire voir un espace de liberté, là où la technique ne peut plus rien. En tout état de cause, la CNIL n'est pas comptable d'un tel taux d'échec.

La deuxième réflexion est d'ordre politique : une interconnexion n'est pas d'abord une procédure informatique, c'est aussi un mode de gestion par une administration de ses relations avec ses administrés. La loi du 24 août 1993 relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France a autorisé des échanges d'informations entre les organismes de sécurité sociale et les préfetures afin qu'il puisse être vérifié que les assurés étrangers sont en situation régulière, condition à laquelle sont depuis lors subordonnés leur affiliation à la sécurité sociale et les versements de prestations. La presse a relaté, peu de temps après l'entrée en vigueur de cette loi, qu'une caisse de sécurité sociale, soucieuse de procéder à une telle vérification légale, avait exigé de tous les Français portant un nom à consonance étrangère ou nés à l'étranger la présentation d'une carte nationale d'identité, voire d'un certificat de nationalité française afin de limiter le contrôle administratif par interconnexion de son fichier avec le fichier des étrangers aux seules personnes ne pouvant pas rapporter la preuve de leur nationalité française. Las, cette caisse était située dans une région à tradition d'immigration millénaire : le tollé fut général. Où l'on voit qu'une interconnexion ne vise pas forcément ceux qui devaient en faire l'objet et que la procédure de contrôle envisagée a pu avoir des effets qui ont largement excédé le champ de l'informatique.

La troisième réflexion nous vient des pratiques comparées. Dans plusieurs États dotés d'une législation de protection des données, tels le Québec ou l'Australie et la Nouvelle Zélande, un bilan coût/avantage est établi pour chaque interconnexion d'envergure faisant apparaître le rapport entre le financement public nécessaire à la mise en place de l'opération et l'avantage financier qui en résulte (c'est-à-dire, le plus souvent, la récupération de sommes indûment versées). Ce rapport est ensuite présenté à l'au-

---

Interconnexions et fichiers policiers : deux débats de notre temps

torité nationale de protection des données ou au Parlement qui décide, au vu des résultats, de renouveler ou non l'autorisation précédemment accordée. Une telle méthode, pragmatique, présente incontestablement l'avantage d'éviter les débats dogmatiques à l'issue desquels, immanquablement, les gestionnaires passent peu ou prou pour liberticides et les défenseurs des libertés pour complices de la fraude...

#### LE PRINCIPE DE FINALITÉ

Ces réflexions manifestent que les interconnexions doivent, en tout état de cause, être étroitement encadrées si l'on souhaite que soit respecté le point d'équilibre défini par toutes les législations de protection des données et qui tient en un mot : le principe de finalité. Un fichier doit avoir une finalité déterminée : c'est au regard de cette finalité, et d'elle seule, que doivent être appréciées les catégories d'informations qu'il est utile d'enregistrer et les personnes ou organismes qui pourront avoir accès à ces informations. Les interconnexions de fichiers ne sont pas interdites par nos législations mais elles constituent incontestablement des exceptions. Et, dans un État de droit, l'exception doit s'interpréter strictement : l'exception n'est pas la règle.

#### LES FICHIERS DE POLICE

Les fichiers de police ont toujours existé, comme nous le savons depuis que nous regardons des téléfilms : « fiché au grand banditisme », dit l'officier de police judiciaire, et voilà notre attention plus soutenue ; « inconnu des services de police », nous pouvons aller à la cuisine préparer un plateau-repas. Les fichiers de police ne sont pas nés avec l'informatique ni même, dit-on, avec la télévision. L'adoption de la loi « informatique et libertés » a cependant marqué une date dans leur histoire : celle de leur apparition dans le débat public. En effet, le législateur français de 1978 a fait le choix de l'application de la nouvelle loi aux fichiers de police. Il en est résulté trois conséquences qui sont autant de garanties pour les citoyens.

La première garantie est qu'aucun fichier de police ne peut être mis en œuvre sans avoir été examiné par une autorité indépendante (la CNIL) et avoir recueilli un avis favorable.

La deuxième garantie consiste à n'autoriser les administrations policières à enregistrer des données sensibles qu'avec l'aval de deux institutions : la CNIL d'une part, le Conseil d'État d'autre part.

La troisième garantie est celle du droit d'accès. La loi «informatique et libertés» prévoit, s'agissant des traitements qui intéressent la sûreté de l'État, la défense et la sécurité publique, que le droit d'accès s'exerce par l'intermédiaire d'un membre de la CNIL, magistrat ou ancien magistrat. C'est ce magistrat qui opère aux lieu et place de la personne concernée les vérifications nécessaires après quoi il est notifié à la personne, selon les termes mêmes de la loi, que les «vérifications ont été faites». Cette formule, qui ne fait pas mention des résultats obtenus à la suite de l'exercice du droit d'accès indirect, laisse certes les requérants souvent insatisfaits. Mais il faut y insister, cette procédure offre une garantie essentielle : il n'y a pas en France de fichier qui ne soit soumis au contrôle direct de la personne concernée ou au regard extérieur d'un membre de la CNIL. En un mot, aucun responsable de fichier n'est seul juge de l'opportunité de fichier quelqu'un, du choix des informations qu'il enregistre et de la durée pendant laquelle elles seront conservées. Ce droit est exercé : la CNIL a mené plus de six mille missions d'investigation dans les fichiers relevant de la sûreté de l'État, de la défense ou de la sécurité publique.

CONSERVATION ET CONSULTATION :  
LE CHANGEMENT DE DONNE

Sans doute les développements de l'informatique en vingt ans ont, dans ce domaine comme dans d'autres, changé la donne. La micro-informatique, comme les architectures en réseau, permettent aisément de conserver trace d'une information, de la consulter à distance, de la rapatrier. La machine à écrire « à l'ancienne » n'a peut-être pas encore

---

Interconnexions et fichiers policiers : deux débats de notre temps

déserté tous les commissariats, et cet archaïsme peut rassurer : le procès-verbal, une fois tapé, est signé puis adressé au procureur, « Nous voilà sauvés, nulle trace ! ». On peut cependant préférer, à l'heure de la délinquance sans frontière et des réseaux internationaux de blanchiment d'argent, une police modernisée, efficace, dotée d'outils performants... et au moins de micro-ordinateurs ! Mais c'est précisément là que le problème commence : désormais, le procès-verbal une fois tapé, signé, adressé au procureur, est toujours dans le micro du policier, enregistré sur le disque dur, prêt à resservir, à être consulté en cas de besoin depuis l'autre bout de la France. Tout le débat public suscité par le fichier STIC du ministère de l'Intérieur tient à cette différence qui fonde la loi « informatique et libertés » : ce n'est pas l'information, en soi, qui est dangereuse - un procès-verbal de police est un procès-verbal de police - ce sont les modalités nouvelles d'organisation, de conservation et de sélection de l'information qui rendent indispensable la reconnaissance de nouvelles garanties. En matière de police, plus qu'en toute autre.

144

Le paradoxe du récent débat sur le STIC tient à ce que le caractère ambitieux du projet du ministère de l'Intérieur a conduit la CNIL, pendant l'instruction de ce dossier, à préciser des règles qui méritaient, certes, de l'être mais qui représentaient autant d'avancées de l'État de droit. La première d'entre elles est qu'un fichier de police ne peut pas être utilisé à des fins d'enquête de moralité, sauf à devenir un « casier judiciaire bis ». La deuxième règle est qu'un fichier de police judiciaire doit être placé sous le contrôle du procureur de la République, toute décision judiciaire de mise hors de cause, de non-lieu, de relaxe ou d'acquiescement devant provoquer une mise à jour ou un effacement des informations. L'informatique, et les architectures en réseaux, permettent précisément de rendre systématique ce qui, à l'époque des « fichiers-papier », n'était qu'aléatoire. La troisième règle consiste à prévoir des durées de conservation adaptées à la gravité de l'infraction et à l'âge des personnes mises en cause dans une procédure. La CNIL a ainsi obtenu que les mineurs ne demeurent pas fichés si dans un délai de cinq ans ils n'avaient pas réitéré.



Le débat n'est sans doute pas terminé, mais il est déjà riche d'enseignements. M. Guy Braibant, dans le rapport qu'il a remis au Premier ministre sur la transposition de la directive européenne fait, en la matière, deux propositions qui méritent d'être rappelées.

La première consiste à préconiser que les avis de la CNIL sur les fichiers de police judiciaire soient rendus publics. Aujourd'hui, ils ne le deviennent que lorsque les actes réglementaires créant les fichiers sont eux-mêmes publiés. La CNIL a approuvé cette suggestion. Une plus grande transparence serait sans doute de nature à éviter, tout à la fois, quiproquos dans une matière qui s'en accommode mal et fantasmes sur un terrain qui leur est naturellement propice.

La deuxième proposition vise à modifier la procédure du droit d'accès aux fichiers de police judiciaire. La CNIL soutient cette proposition, comme elle l'a signalé dans son rapport annuel d'activité pour 1997. Le code de procédure pénale prévoit des règles précises en matière de droit d'accès des parties aux pièces de la procédure. Une fois la procédure achevée, rien ne paraît s'opposer à ce que la personne concernée puisse disposer d'un droit d'accès direct aux informations qui la concernent et dont elle n'ignore rien. Au demeurant la personne concernée paraît la mieux à même, le cas échéant, d'en demander la rectification, la mise à jour ou l'effacement. Ce droit pourrait s'exercer au tribunal de grande instance, le procureur de la République en étant le garant

Le propos ne serait pas complet sans une ultime observation. La CNIL a suggéré, dans son dernier rapport d'activité, que le dispositif particulier prévu pour les renseignements généraux soit étendu et prolongé. Ainsi, s'agissant du système Schengen, lorsque, à l'issue des vérifications, une fiche dont l'intéressé avait eu connaissance (à l'occasion d'un contrôle d'identité ou d'une formalité administrative) a été supprimée, il devrait pouvoir en être informé.

Par ailleurs, le code de procédure pénale prévoit des règles précises en matière de droit d'accès des parties aux pièces de la procédure. Une fois la procédure achevée, rien ne paraît s'opposer à ce que la personne concernée puisse disposer d'un droit d'accès direct aux informations qui la

concernent et dont elle n'ignore rien. Au demeurant la personne concernée paraît la mieux à même, le cas échéant, d'en demander la rectification, la mise à jour ou l'effacement. Ce droit pourrait s'exercer au tribunal de grande instance, le procureur de la République en devenant le garant. La CNIL a souligné qu'à ses yeux, une plus grande transparence dans ce domaine paraissait tout à la fois compatible avec la sauvegarde de l'intérêt public et de nature à renforcer les droits des personnes.

#### LA FIN DU DROIT À L'OUBLI ?

A l'heure des réseaux et des échanges de données dans le cadre de la coopération policière internationale - Schengen, Europol - il ne faudrait cependant pas imaginer que les moyens de l'action policière se limitent, comme jadis, à un fichier et à un aveu. Il convient de rappeler que la police judiciaire tient du code de procédure pénale des pouvoirs à l'égard de tous les fichiers détenus en France par d'autres administrations ou par des entreprises. La police est, aux termes de la loi, lorsqu'elle agit en flagrant délit ou sur commission rogatoire d'un juge d'instruction, un « tiers autorisé » à consulter des fichiers qui ne lui appartiennent pas, mais qui peuvent intéresser de près ou de loin l'enquête dont elle est saisie. Dans ce cas, nul ne peut s'opposer à son intervention, ni le responsable du fichier, ni la personne fichée, ni la CNIL bien évidemment. Ainsi, la police peut rechercher des renseignements en consultant l'ordinateur d'un hôtel, les fichiers d'un opérateur de télécommunications (pour savoir quel numéro a été appelé), ceux d'une société d'autoroute (pour vérifier à quel moment tel véhicule est passé au péage) ou encore ceux d'un fournisseur d'accès à Internet (pour savoir quel internaute est connecté à tel site).

Révéler cet élément, c'est souligner qu'au fur et à mesure que la société s'informatise et que se généralise l'utilisation des moyens informatiques « nomades » (une carte bancaire, un téléphone mobile) ou les architectures en réseau, les gisements de données ou les « traces informatiques » qui touchent à nos activités privées se multiplient. Ces gise-

ments de données constituent, pour la police, autant de preuves aisément accessibles... et difficilement contestables.

La CNIL le dit souvent : jusqu'à l'informatisation d'une société, l'oubli était une contrainte de la mémoire humaine. Avec l'informatisation, l'oubli relève désormais du seul choix social. Le droit à l'oubli n'est pas nouveau ; il n'est pas né avec la loi du 6 janvier 1978, qui d'ailleurs ne le consacre pas, même s'il inspire toute notre législation. Ce droit est sans doute né avec l'idée même d'équilibre. Qu'on y songe : même le code pénal ou le code de procédure pénale qui déterminent les règles de l'ordre public, le prévoient en plusieurs de leurs dispositions : l'amnistie efface l'infraction ; la grâce relève de la condamnation ; la réhabilitation est une manière d'oubli collectif lorsque le condamné n'a pas récidivé ; certaines condamnations peuvent être automatiquement effacées après un temps d'épreuve ; l'action publique contre les auteurs d'infractions se prescrit : la société se prive volontairement du droit de rechercher un criminel passé un long délai ; la condamnation elle-même se prescrit : on ne peut plus faire exécuter une condamnation correctionnelle plus de cinq ans après son prononcé. Il s'agit là d'équilibres anciens, les uns datent des rois, les autres de la République. Et cet équilibre ancien n'a jamais signifié qu'on préfère l'impunité au civisme.

C'est cet équilibre qu'une démocratie doit sans cesse rechercher. L'entrée de la France dans la société de l'information, c'est-à-dire aussi dans un monde de traces informatisées que nous laissons à l'occasion de nos actes les plus quotidiens et qui sont enregistrés dans des puces, des fichiers «logs», des «proxys», des bornes interactives, nécessite plus que jamais la vigilance, si nous souhaitons, ensemble, échapper à une société de surveillance.

■ **Joël BOYER**

*Chargé des affaires juridiques de la CNIL*



# LA SURVEILLANCE ÉLECTRONIQUE À DOMICILE : UNE NOUVELLE ÉCONOMIE DU POUVOIR DE PUNIR ?

par Jean-Charles FROMENT

Plus qu'un simple gadget technologique, l'utilisation du bracelet électronique modifie l'économie et le sens de la peine : dans un sens positif, tout d'abord, en reléguant la prison synonyme de privation de liberté, à un moment circonscrit de l'histoire de la peine, mais aussi en réinscrivant la peine comme marquage du corps. Idéal vite battu en brèche puisque, là où cette nouvelle modalité de sanction est effective, la population carcérale n'est pourtant pas en diminution. Plus généralement, cette mutation marquerait l'avènement d'une société de contrôle aux dépens d'une société disciplinaire, dans laquelle le pouvoir politique se diffuserait, se socialiserait et se civiliserait.

•••• (1) FROMENT, 1996.

•••• (2) Si les États-Unis et le Canada, notamment la province d'Ontario, font ici figure de précurseurs, ils ont progressivement été rejoints, à titre expérimental ou non, par de nombreux pays européens, comme la Grande-Bretagne, la Suède, les Pays-Bas. L'Allemagne, l'Italie, la Suisse, la Belgique ont elles aussi engagé une réflexion ou des expériences dans cette direction. Cf. KUHN, MADIGNIER, 1998, p. 671 et suivantes.

•••• (3) Cf. pour une présentation du dispositif, l'article de COUVRAT, 1998, et celui de PRADEL, 1998, p. 15 et suivantes. Ainsi que, pour une analyse critique, KUHN, MADIGNIER, *Op. cit.*

•••• (4) BONNEMAISON, 1990.

•••• (5) CABANEL, 1995, p. 115-139.

Deux ans ont suffi pour qu'en France, le mécanisme pénal du « bracelet électronique », que j'étudiais encore sous un angle virtuel en 1996, soit devenu réalité<sup>1</sup>. Ainsi, la France a-t-elle rejoint le cercle, de plus en plus important<sup>2</sup>, des pays qui ont décidé de recourir au système du placement sous surveillance électronique (PSE) ou de l'assignation à domicile sous surveillance électronique (ADSE). Le parlement a, à cette fin, adopté le 19 décembre 1997 une loi instaurant ce procédé au titre des nouvelles modalités d'exécution des peines<sup>3</sup>. Les propositions faites en ce sens par Gilbert Bonnemaïson en 1990, dans son rapport sur la modernisation du service public pénitentiaire<sup>4</sup> et par le sénateur Guy Cabanel en 1995, dans son rapport sur les moyens de prévenir la récidive<sup>5</sup>, ont donc été suivies d'effets, ce dernier étant directement à l'origine de la loi du 19 décembre 1997. Difficile cependant de se prononcer encore de façon définitive sur ce texte dès lors que ses décrets d'application n'ont toujours pas été publiés plus

d'un an après l'adoption de la loi <sup>1</sup>. D'autant plus difficile qu'au-delà des incertitudes juridiques qui la caractérisent encore, cette technique nous place régulièrement face à des sentiments et des interrogations contradictoires. Ne voit-on pas, en effet, adversaires et partisans de ce procédé se rejoindre sur le même terrain de la protection de la dignité de la personne humaine pour développer leur argumentation ?<sup>2</sup> N'observe-t-on pas régulièrement abolitionnistes et non abolitionnistes se retrouver paradoxalement dans une même critique ou encore une même défense de ce type de placement ?<sup>3</sup> Ne doit-on pas enfin s'étonner de la diversité des arguments invoqués pour ou contre ce mécanisme qui nous conduit des approches les plus pratiques aux considérations les plus philosophiques ? Cette technique ne laisse donc pas de surprendre, et surtout de susciter des interrogations. Et cela s'explique sans doute par le fait que le débat sur l'adse se situe au cœur du procès général de surveillance (vidéo-surveillance, écoutes téléphoniques, empreintes génétiques, etc.), que l'on peut observer dans notre société<sup>4</sup>. C'est précisément au moment où les dispositifs de surveillance se diffusent dans l'ensemble de la société et ne demeurent plus confinés au sein d'établissements disciplinaires fermés que les détenus sont autorisés à effectuer leur peine en dehors de murs étrangers, au sein même de leur propre domicile. C'est pourquoi il me semble que ce double mouvement de déterritorialisation et de désinstitutionnalisation de la peine, ou de son exécution<sup>5</sup> doit en réalité s'interpréter comme un déplacement ou une mutation des formes dans lesquelles la puissance publique exerce sa fonction de punir. L'adse révèle plus fondamentalement une recomposition des formes dans lesquelles le pouvoir incarne sa souveraineté, sa puissance. En effet, la peine et son exécution en tant qu'expression du « droit et du pouvoir de punir »<sup>6</sup> marquent la présence de l'État, seul détenteur du « monopole de la violence physique légitime »<sup>7</sup>. La localisation et l'analyse des formes pénales constituent fondamentalement une localisation et une analyse des formes d'exercice du pouvoir souverain par l'État. Or précisément, de ce point de vue, l'adse traduit une réorganisation des formes d'expression de la

••••(1) Révélant par là même les hésitations du nouveau gouvernement sur ce dispositif.

••••(2) FROMENT, 1996, p. 121 et suivantes.

••••(3) CUSSON, 1998, p. 34 et suivantes.

••••(4) *Les Cahiers de la sécurité intérieure*, n°21, 1995.

••••(5) Sur ces deux concepts de déterritorialisation et de désinstitutionnalisation, cf. mes précédents articles sur l'assignation à domicile sous surveillance électronique.

•••• (6) PONCELA, 1983, p. 123 et suivantes.

••••(7) WEBER, 1963, p. 100.

••••(1) SFEZ, 1993.

••••(2) GLUCKSMANN, 1967, p. 75.

puissance publique qui, plutôt que de s'incarner, comme elle l'a longtemps fait, dans des institutions et des hommes sur un territoire public donné, semble peu à peu s'inscrire et se diffuser dans la société. Ainsi, l'adse dévoile le processus de dissémination d'un pouvoir qui se diffuse socialement par éclats. Ce sont ces « éclats de pouvoir », que Lucien Sfez a analysés, qui partent et se projettent et notamment sur chacun d'entre nous. Chacun, en effet, représente le pouvoir dans la configuration présente d'une politique éclatée qui caractérise une société de type ordinaire<sup>1</sup>. Et la disparition des « centres de gravité »<sup>2</sup>, à partir desquels le pouvoir s'incarne, (cœur même de ce qui demeure son espace stratégique) est aussi un moyen d'auto-protection dans un temps où il se sent exposé.

#### DE LA SOCIÉTÉ DISCIPLINAIRE À LA SOCIÉTÉ DE CONTRÔLE

Le problème, en effet, est bien là, à savoir celui de la légitimation de la puissance publique. Rendre compte de ce processus de dissémination sociale du pouvoir, ce n'est pas seulement céder aux fantasmes de *Big brother*, comme semble le penser Maurice Cusson<sup>3</sup>, mais plutôt s'interroger sur les conséquences, dans un temps de contestation de son autorité et de sa légitimité, d'une recherche par la puissance publique d'une nouvelle efficacité et légitimité qui la conduit à s'ancrer de plus en plus dans la société elle-même. Ici, il ne s'agit pas d'évoquer une volonté consciemment déterminée du pouvoir qui chercherait à s'immiscer toujours plus dans la société et la vie privée de chacun, mais d'identifier les répercussions possibles, en termes de construction d'un nouveau modèle social, d'un pouvoir en quête de légitimité. C'est sans doute de cette manière qu'il convient de comprendre cet encouragement de Pierre Landreville à « surveiller et prévenir » l'assignation à domicile sous surveillance électronique<sup>4</sup>. C'est en tout cas ainsi qu'il faut interpréter les analyses de Gilles Deleuze sur la naissance d'une « société de contrôle »<sup>5</sup>, laquelle se substitue au modèle foucauldien de « société disciplinaire »<sup>6</sup>. L'ADSE révèle la dilution progressive de la distance sépa-

••••(3) CUSSON, op. cit.

••••(4) LANDREVILLE, 1987, p. 251 et suivantes.

••••(5) DELEUZE, 1990.

••••(6) FOUCAULT, 1975.

rant le pouvoir de la société civile, dans le sens où le pouvoir s'incarne désormais dans la société civile elle-même et se diffuse de plus en plus en elle en s'ancrant directement sur les citoyens. Elle incarne *a priori* une évolution de l'inscription sociale de la peine, qui, en fait, révèle plus fondamentalement encore une nouvelle inscription sociale du pouvoir lui-même.

#### UNE NOUVELLE INSCRIPTION SOCIALE DE LA PEINE

La prison, « *manifestation extérieure de la puissance de l'État* » <sup>1</sup> représente symboliquement un territoire sur lequel le pouvoir exerce publiquement et exclusivement sa souveraineté. Elle est finalement la forme essentielle aujourd'hui, sinon exclusive, de projection spatiale de la puissance de punir. Or, l'ADSE s'inscrit dans un mouvement qui tend à effacer progressivement cette idée d'un « *lieu de pénalité* » à proprement parler. À travers elle, on assiste à une nouvelle manifestation d'une peine investissant de plus en plus le champ social, traduisant un double procès de pénalisation de la société civile et de socialisation de la peine.

#### LA PÉNALISATION DE LA SOCIÉTÉ CIVILE

N'en déplaise à M. Cusson <sup>2</sup>, s'interroger sur l'élargissement du « *filet pénal* » susceptible de résulter de l'ADSE, est nécessaire. Comme l'expriment en effet A. Kuhn et B. Madignier, « *lorsque la surveillance électronique est utilisée pour remplacer de courtes peines privatives de liberté, il est indispensable de se demander comment il sera possible d'éviter le net widening, à savoir l'application de cette mesure de contrôle à des personnes qui, autrement, auraient pu profiter d'un mode d'exécution de peine plus « clément » (sursis, peine pécuniaire, classement, etc.)* » <sup>3</sup>. Difficile pour l'instant d'apprécier avec précision la réalité de ce phénomène, mais cette préoccupation doit demeurer présente. C'est notamment ce que démontrent P. Landreville <sup>4</sup> et A. Normandeau <sup>5</sup> à travers les exemples respectifs du Canada et des États-Unis qui constituent les

••••(1) KELSEN, 1988, p. 174.

••••(2) CUSSON, *Op. cit.*

••••(3) KUHN, MADIGNIER, *op. cit.*

••••(4) LANDREVILLE, *op. cit.*

••••(5) NORMANDEAU, 1996, p. 333 et suivantes.



••••(1) Les premières expériences de surveillance électronique ont été engagées aux États-Unis en Floride et au Nouveau-Mexique en 1984. Le Canada a retenu ce système à partir de 1987 dans la province de l'Ontario.

••••(2) NORMANDEAU, op. cit., p. 342-343.

••••(3) de MONTVALLON, 1996, p. 9. La loi du 19 décembre 1997 ne remet pas en cause cette opposition en confirmant que le PSE n'est ni un substitut à la détention provisoire, ni une modalité de contrôle judiciaire avant jugement.

expériences les plus anciennes en ce domaine <sup>1</sup>. Aux États-Unis, le recours à l'EM (*Electronic monitoring*) accompagne l'obligation pour un criminel de ne pas quitter son domicile durant certaines heures de la journée ou de la nuit, ordinairement, en dehors de ses heures de travail (s'il travaille ou cherche un emploi). La surveillance électronique est imposée par le juge comme une condition lors de la remise en liberté avant procès, lors d'une probation ou lors d'une libération conditionnelle. Dès lors, le PSE ne peut que se traduire par une extension du dispositif de contraintes pénal. Dans ce cadre, écrit A. Normandeau, « on emprisonne de façon habituelle, autant et même plus de monde, mais l'on ajoute dans certains cas à la probation ou à la libération conditionnelle ordinaire ou intensive une surveillance additionnelle de type électronique. Cette surveillance est également un « ajout punitif » et une mesure communautaire de « contrôle plus strict » plutôt qu'une solution de rechange à l'emprisonnement, comme c'est le cas de la surveillance intensive »<sup>2</sup>. Dans ces deux pays, en tout cas, l'adoption de la surveillance électronique ne s'est pas traduite par une substantielle baisse de la population carcérale. De même, les catégories de personnes principalement concernées par ce dispositif peuvent aussi laisser entendre le risque d'une extension du « filet pénal ». Ainsi, en Suède (58 % des condamnés pour conduite en état d'ivresse, 19 % pour violences, 33 % pour vols, stupéfiants et divers) et aux États-Unis (25,6 % des condamnés pour circulation routière, 18,2 % pour atteinte à la propriété, 13,5 % pour infractions aux stupéfiants), on constate que ce sont essentiellement les délinquants routiers et ceux qui commettent des infractions aux stupéfiants qui sont soumis à de telles mesures, catégories qui n'auraient pas nécessairement fait l'objet d'une mesure d'incarcération.

C'est encore cette crainte qui avait poussé les organisations professionnelles des magistrats et des avocats, en France, à s'opposer à la volonté des sénateurs d'insérer dans la loi relative à la détention provisoire adoptée le 30 décembre 1996, la possibilité pour le juge de recourir au PSE à titre d'alternative à la détention provisoire <sup>3</sup>. Le légis-

lateur de 1997 a pris, à cet effet, des précautions n'instituant le PSE qu'à titre de modalité d'exécution des peines, et non de peine prononçable directement par une juridiction de jugement. Mais cela ne dissipe pas toutes les inquiétudes. Rien n'empêche en effet les juges d'anticiper sur un recours ultérieur à ce procédé. D'autant qu'en vertu du décret du 22 juillet 1996 (art. D. 49-1, CPC), le parquet communique au juge de l'application des peines un extrait de toute décision de condamnation à une peine ne dépassant pas un an concernant une personne non incarcérée afin que ce juge puisse « déterminer les modalités d'exécution de la peine en considération de la situation du condamné ». Or, c'est précisément le juge de l'application des peines, soit de sa propre initiative, soit sur demande du procureur de la République<sup>1</sup>, qui pourra justement décider que la peine s'exécutera selon la formule de l'ADSE si le condamné n'a à subir qu'une peine maximale d'un an.

Au-delà du seul cas de l'ADSE, la question semble se poser avec d'autant plus d'acuité que celle-ci n'est pas un cas isolé parmi ces formes pénales qui traduisent cette possible extension. Ainsi, au nom d'une nécessaire adaptation<sup>2</sup> des réponses pénales face aux mutations de la délinquance, se développent les formes alternatives de justice et de peine. Rien de contestable en soi dans cette évolution<sup>3</sup>. Si ce n'est que cette dernière ne semble jamais se traduire par une diminution du recours aux formes pénales « traditionnelles » et notamment à la prison, laquelle ne souffre manifestement pas de cette concurrence. C'est ainsi, par exemple, que doit s'analyser le développement de la médiation pénale. Anne Wyvekens, à partir de l'exemple lyonnais des maisons de justice et du droit, a bien montré comment cette médiation, loin de correspondre à une réponse communautarisée aux conflits de voisinage telle qu'elle est souvent présentée, participe d'une restauration du droit pénal dans les quartiers où celui-ci a « disparu » en fonctionnant fondamentalement selon une logique du « classement sous condition »<sup>4</sup>. Elle permet à ce titre à la justice pénale de se ressaisir d'un ensemble d'actes délictuels jusque-là classés. Les analyses de Philippe Mary témoignent d'une même logique<sup>5</sup>. En soi, là encore l'évolution peut paraître logique

••••(1) Soit encore à la demande du condamné. Dans tous les cas, le consentement du condamné est obligatoire. Il doit être donné en présence de son avocat ou, à défaut, d'un avocat désigné par le bâtonnier. En revanche, il n'y a pas d'exigence du consentement du Procureur de la République, lequel peut exercer un recours dans les 24 heures devant le tribunal correctionnel (art. 733-1 CPP). Enfin, un médecin peut être désigné (de droit si le condamné le demande) pour vérifier que ce procédé ne présente pas d'inconvénient pour la santé du condamné.

••••(2) COLLET, 27 janvier 1999.

••••(3) Et l'on ne peut ici que rejoindre les analyses de M. Cusson lorsqu'il considère que l'évolution des formes de la délinquance suppose une adaptation des réponses pénales dans le sens d'une adaptation, d'une proportionnalité retrouvée, entre l'acte et la réponse fournie. cf. CUSSON, *op. cit.*

••••(4) WYVEKENS, 1997.

••••(5) MARY, 1997 et 1997.

••••(1) FROMENT, à paraître en 1999.

••••(2) WYVEKENS, 1997, p. 73.

••••(3) Ce problème concerne d'ailleurs l'ensemble des nouvelles technologies de sécurité, de la vidéosurveillance aux techniques d'identification vocale, qui se traduisent toutes, de façon différente, par une pénétration de l'espace privé individuel. cf. pour une approche globale de ces problèmes, 4e Université d'automne de la Ligue des droits de l'homme, 1998.

••••(4) NORMANDEAU, *Op. cit.*, p. 343.

••••(5) KAYSER, 1990.

dès lors qu'elle entend mettre fin à des actes délictueux auxquels il n'était plus répondu, mais elle devient problématique si elle se traduit par la pénalisation d'actes qui jusqu'alors n'étaient pas volontairement traités dans les termes du droit pénal, car ne nécessitant ni ne méritant une telle qualification. C'est ainsi que l'hypothèse d'une pénalisation, voire d'une sur-pénalisation <sup>1</sup>, de la société civile, peut être légitimement émise. Il devient urgent de poser cette question : « *Où s'arrête le champ d'intervention du pénal ?* » <sup>2</sup>.

#### LA SOCIALISATION DE LA PEINE ET DE SON EXÉCUTION

Mais ce mouvement de pénalisation du social se double d'une autre évolution que semble sous-tendre l'ADSE, à savoir un mouvement de déterritorialisation de la peine et de son exécution se traduisant par leur socialisation. Avec l'ADSE, il n'y a en effet plus d'identification possible des lieux d'exécution de la peine, il n'y a plus de territoire propre pour la peine qui se déplace désormais avec soi. Ainsi, l'ADSE pose la question de l'inscription sociale de la peine. À l'exclusion institutionnelle et disciplinaire du condamné succède une socialisation de la peine. S'il y avait jusqu'à présent dans notre société des lieux identifiables et socio-historiquement justifiés où la liberté individuelle pouvait être limitée selon certaines procédures et garanties, avec l'ADSE, c'est directement dans et sur le corps du condamné que la peine s'inscrit désormais ; elle n'est plus ce que l'on vit dans un lieu précis, désigné spécifiquement à cette fin et dont on peut finalement s'échapper, ou du moins avoir l'espoir de s'évader. En la circonstance, cette idée de lieux liberticides clairement identifiés disparaît, il y a diffusion, capillarisation de l'atteinte à la liberté puisque l'on peut porter atteinte à cette liberté dans le lieu même où elle était jusqu'alors protégée de façon ultime, le foyer, le domicile, l'espace privé <sup>3</sup>. Comme le souligne A. Normandeau, « *en démocratie, le concept de résidence personnelle, de logement, de maison est le symbole de cette sphère privée : un refuge, un sanctuaire* » <sup>4</sup>. Que reste-t-il, dès lors, du droit au respect de la vie privée <sup>5</sup>,

énoncé explicitement en France par le Conseil constitutionnel dans sa décision du 18 janvier 1995 (« *la méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* ») <sup>1</sup> ? Ou encore du droit à l'inviolabilité du domicile dont P. Hagser et M. Frangi ont montré - à la suite de leur analyse de la décision du Conseil constitutionnel du 29 décembre 1983 <sup>2</sup> et surtout de celle du 12 janvier 1977 <sup>3</sup> par laquelle il s'était opposé à une loi permettant la fouille des voitures en raison de son étendue et de l'imprécision des contrôles possibles - qu'il avait une valeur constitutionnelle <sup>4</sup> ? Sans compter que la surveillance électronique peut aussi entraîner une violation de la sphère privée de la famille de l'individu sous surveillance. En effet, selon les modalités de surveillance retenues (par exemple si on décidait de surveiller par l'intermédiaire d'une caméra placée au domicile du condamné), la sphère privée de ses proches pourrait être violée <sup>5</sup>. Dans ce cas, ne pourrait-on évoquer une atteinte au « *droit à mener une vie familiale normale* », là encore reconnu par le Conseil constitutionnel ? <sup>6</sup>

Aux États-Unis, la question a, en grande partie, été réglée. Ainsi, la Cour suprême affirme-t-elle depuis un arrêt *Katz c/ États-Unis* (1967), qu'un moyen tiré de la violation du quatrième amendement de la Constitution, lequel tend à la préservation de l'intimité de la vie privée, n'est pas recevable dès lors que l'individu n'est pas en mesure de prétendre raisonnablement au bénéfice d'une quelconque intimité. C'est ainsi par exemple qu'un détenu n'est pas fondé à invoquer l'inconstitutionnalité de l'utilisation d'un procédé électronique ayant permis d'intercepter l'une de ses conversations avec d'autres détenus (*Lanza c/ New York*, 1962). Quant aux probationnaires qui sont éligibles à l'ADSE, leur situation ne change rien dans la mesure où la Cour suprême estime, depuis un arrêt *États-Unis c/ Manfredonia* de 1972, que les atteintes portées à leur intimité ne sont pas entachées d'inconstitutionnalité dès lors qu'elles contribuent à assurer le contrôle auquel ils sont soumis <sup>7</sup>. Mais quand l'exécution de la peine a lieu non plus dans une résidence publique, mais dans la résidence privée de l'individu sous surveillance, peut-on toujours raisonner

••••(1) LUCHAIRE, p. 590 ; BARLOY, 1995, p. 483 et suivantes.

••••(2) C.C., 1983, p. 67.

••••(3) C.C., 1977, p. 33.

•••• (4) HAGSER, 1992.

••••(5) KUHN ; MADIGNIER, *op. cit.*, p. 675.

••••(6) C.C., N°93-325 DC, 12-13 août 1993, relative à la maîtrise de l'immigration, G.D.C.C., N°47.

••••(7) BENGHOZI, 1990, p. 59 et suivantes.

ainsi ? De surcroît, l'état de la jurisprudence de la Cour européenne de sauvegarde des droits de l'homme rend possible une autre lecture juridique. Ainsi l'article 8 de la CESDH qui stipule que « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* » a permis à la Cour de préciser la façon dont il fallait interpréter les conséquences de cet article, notamment pour des condamnés. Elle a en effet posé le principe qu'une restriction ne doit jamais porter atteinte à la « *substance même* » d'un droit, se mettant par là même en position d'apprécier le contenu concret des droits proclamés. Elle a pu, par exemple, procéder ainsi en ce qui concerne le droit au respect de la correspondance, lequel est un élément constitutif du droit, et plus généralement, au secret de la vie privée, qui revêt une importance toute particulière pour les détenus : la Cour a pu estimer que la saisie de la correspondance des détenus <sup>1</sup>, la non-transmission d'une lettre à un détenu <sup>2</sup>, la limitation de la possibilité de correspondre aux seuls amis et parents <sup>3</sup> ou des obstacles à la possibilité même de correspondre <sup>4</sup>, constituaient des ingérences qui, bien que visant un but légitime (défense de l'ordre, prévention des infractions pénales), n'étaient pas nécessaires dans une société démocratique et vidaient le droit au secret de la correspondance de toute réalité <sup>5</sup>. On peut dès lors se demander si ce raisonnement ne pourrait pas être retenu à propos de différents aspects de l'ADSE. Car c'est bien le caractère de « *lieu privilégié de la vie privée* » <sup>6</sup> du domicile et le sens même de ce que certains spécialistes des libertés publiques ont appelé le « *territoire de la personnalité* » <sup>7</sup> qui semble disparaître avec elle.

En remettant en cause le principe d'une séparation entre l'espace privé et l'espace public, c'est plus fondamentalement le problème de la limitation du champ d'action du pouvoir politique que l'ADSE soulève. En effet, l'apport principal de la Déclaration des droits de l'homme et du citoyen du 26 août 1789, comme l'expose Luc Ferry, a sûrement été, moins que de proclamer le triomphe absolu des droits subjectifs, de poser le principe de l'existence d'une frontière nécessaire entre la sphère de l'action publique et celle de l'action privée, entre le pouvoir politique et la société

••••(1) C.E.D.H, 1983.

••••(2) C.E.D.H, 1988.

••••(3) C.E.D.H, 1984.

••••(4) C.E.D.H, 1975.

••••(5) SUDRE, 1998.

••••(6) HAGSER, *op. cit.* ;  
FRANGI, *op. cit.*

••••(7) ROBERT, DUFFAR,  
1994, p. 369 et suivantes.

civile<sup>1</sup>. À partir du moment où l'État pénètre la sphère privée et la société civile pénètre l'espace public, ces deux notions perdent de leur sens. Dès lors, l'action du pouvoir peut se porter en des lieux qui lui étaient interdits jusqu'alors puisque relevant précisément de la sphère des relations privées. À partir du moment où, en effet, il n'y a plus de séparation entre les espaces public et privé, les limites « territoriales » imposées aux interventions du pouvoir disparaissent<sup>2</sup>. Sans doute convient-il ici de se méfier des pièges de la « modestie étatique » qu'encourage la pensée néo-libérale : elle ne conduit en rien à un abandon par l'État de ses prérogatives, elle ne conduit qu'à éviter qu'il ne se montre justement dans l'exercice de ses dites prérogatives. Dans le cadre de l'ADSE précisément, le pouvoir continue à exercer de la même façon son pouvoir de punir, mais ce qu'il faisait jusqu'alors à travers un dispositif visible, il le réalise maintenant sans se donner à voir. Ainsi, la société civile pouvait jusqu'alors se prémunir en se distanciant de qui symbolisait le pouvoir. La notion de « *périmètre sensible* », analysée par Philippe Combessie, et traduisant une forme de répulsion sociale et physique à l'égard des établissements pénitentiaires dans les villes où ils sont implantés, symbolisait cette nécessaire et possible opération de distanciation de la société civile vis-à-vis du pouvoir<sup>3</sup>. En est-il de même avec cet État-régulateur que nous livre la crise de l'État-providence, un État modeste qui pour surmonter la crise de légitimité à laquelle il est confronté ne se donne plus à voir dans l'exercice de certaines fonctions, risquant finalement de profiter de cette absence de visibilité pour s'insinuer dans des territoires qui lui étaient jusqu'alors interdits ? Comme le rappelle Luc Rouban, « *c'est dans cette perspective qu'il faut bien comprendre que l'adoption d'une économie néo-libérale ne s'accompagne pas des limites politiques posées par la théorie libérale classique. Les possibilités multiples d'une recomposition de l'espace public sur lui-même élargissent le champ du politique dont rien, a priori, ne peut plus être soustrait* »<sup>4</sup>. On peut certes s'en remettre à la démocratie pour concevoir des garanties face à cette évolution<sup>5</sup>. Mais ce n'est précisément que par la conscience

••••(1) FERRY, 1991, p. 43 et suivantes.

••••(2) Cette analyse interroge, d'une façon générale, tout l'avènement du droit social qui par essence remet en cause la distinction entre Etat et société civile. Et c'est précisément ce problème que l'on trouve au cœur des ouvrages d' HABERMAS, 1978, et de DONZELOT, 1984.

••••(3) COMBESSIE, 1996.

••••(4) ROUBAN, 1994, p. 41.

••••(5) CUSSON, *Op. cit.*, p. 44.

de ces effets et leur mise en évidence que celle-ci sera à même de jouer ce rôle.

#### UNE NOUVELLE INSCRIPTION SOCIALE DU POUVOIR

La modification du rapport de la peine à la société qu'organise la surveillance électronique révèle plus fondamentalement l'émergence d'une nouvelle économie sociale du pouvoir. En effet, c'est bien, dans un temps de contestation de la légitimité des appareils d'autorité <sup>1</sup>, à la recherche d'une nouvelle insertion sociale de la puissance publique à laquelle nous fait assister le PSE. Ainsi, semble peu à peu se dessiner sous nos yeux l'image d'un pouvoir qui ne s'incarnerait plus à travers ses appareils institutionnels traditionnels que sont la prison et les professionnels de la puissance publique, remettant peu à peu en cause son statut d'extériorité par rapport à la société.

•••(1) SENNETT, 1981.

#### LA FIN DES PRISONS ?

Reconnaissons ce mérite à la surveillance électronique d'intervenir précisément dans une période où les thèses abolitionnistes perdent de leur vigueur ou du moins ne trouvent plus de relais médiatiques de nature à leur donner une certaine force sociale. Dans cette perspective, l'ADSE est peut-être propre à relancer un débat qui n'aurait jamais dû être abandonné, celui de l'historicité de la peine carcérale. La prison n'est pas éternelle, elle n'est pas la seule fin possible en matière pénale. Elle n'est qu'un moment historique de la pensée sur la peine et la surveillance électronique tend à le démontrer. Ainsi, ceux qui parlaient de la fin de la prison n'étaient peut-être pas aussi utopiques que l'on voulait bien le dire. Le débat sur la peine est toujours à réinventer, il est du moins toujours à interroger <sup>2</sup>. Avec l'ADSE, il est de nouveau légitime d'imaginer un démantèlement progressif des prisons en tant qu'organisations spécialisées dans la punition, il devient de nouveau possible d'évoquer la disparition d'une architecture disciplinaire de la société. Décidément, comme l'écrit symboliquement Christian

•••(2) Il ne s'agit pas nécessairement ici de défendre un propos abolitionniste, mais de mettre en garde contre tout historicisme qui nous conduirait à penser que nous avons atteint la « fin de l'histoire » de la peine le jour où la prison a été « inventée ».

Demonchy, « *l'architecture carcérale n'est plus ce qu'elle était* ». <sup>1</sup>

••••(1) DEMONCHY, 1998, p. 79.

Bien entendu, la réalité nous situe encore bien loin d'une telle perspective. Les chiffres en témoignent, même s'ils traduisent des situations très variables. Ainsi, si aux États-Unis, la surveillance électronique est utilisée depuis 1990 dans les cinquante États, et si elle ne concerne pour A. Kuhn et B. Madignier que de 50 000 à 70 000 personnes<sup>2</sup>, et, au mieux, pour A. Normandeau, environ 100 000<sup>3</sup>, le nombre de personnes incarcérées n'a dans le même temps pas cessé d'augmenter, dépassant le million aujourd'hui. Quant au Canada, où ce système existe dans les provinces de la Colombie britannique, du Saskatchewan, de Terre-Neuve et de l'Ontario, il ne s'est pas traduit non plus par une baisse du nombre des incarcérations. L'expérience européenne est encore trop récente pour apprécier ses effets réels, mais il semble que parier sur une très forte diminution de la population carcérale serait en grande partie illusoire. En Angleterre, le *Home Détenition Curfew programme* prévoit cependant que dès la première année, 4 000 détenus pourront bénéficier de ce système, puis 30 000 chaque année suivante. En Suède, la population carcérale a baissé de 10 % ; l'objectif était d'atteindre une baisse d'un tiers. Quoi qu'il en soit, dans tous les cas, seules certaines catégories de condamnés sont concernés par la surveillance électronique, généralement ceux qui n'ont à subir que des courtes peines : en Angleterre, le dispositif existe désormais comme modalité d'exécution des peines pouvant s'appliquer à ceux qui ont été condamnés à une peine comprise entre trois mois et quatre ans d'incarcération<sup>4</sup>. Aux Pays-Bas, la surveillance électronique peut être utilisée en remplacement de certaines peines de durée moyenne (six mois) et pour les libérés sous conditions. De même en Suède pour les peines de moins de deux mois de privation de liberté<sup>5</sup>.

••••(2) KUHN, MADIGNIER, *Op. cit.*, p. 673.

••••(3) NORMANDEAU, *Op. cit.*, p. 340.

••••(4) L'Angleterre a expérimenté ce système pour la détention provisoire en 1994, mais ne l'a finalement pas retenu dans ce cadre.

••••(5) BISHOP, 1995, p. 8 et suivantes.

Le dispositif retenu en France par la loi du 19 décembre 1997 prévoit que le juge de l'application des peines pourra décider du recours au PSE dans trois cas : *ab initio*, pour les condamnés à une peine inférieure ou égale à un an, en fin de peine, pour les condamnés à une ou plusieurs peines



•••(1) Il est aussi à noter que l'article 13 de l'ordonnance du 2 février 1945 a été modifié par la loi du 19 décembre 1997 pour rendre applicable ce type de placement aux mineurs condamnés.

•••(2) Dans son rapport au nom de la commission sénatoriale des lois, G. Othily indique ainsi que sur les 52 658 personnes incarcérées en France au 1er janvier 1996, 17 600 auraient pu être concernées par le PSE, Sénat, N°3, 2 octobre 1996, p. 8.

•••(3) PRADEL, *op. cit.*, p. 20..

•••(4) TRAVIS, 27 janvier 1999.

•••(5) NORMANDEAU, *Op. cit.*, p. 343.

auxquels il ne reste plus à purger que moins d'un an, et enfin en prélude à la libération conditionnelle<sup>1</sup>. Dans tous les cas, le PSE ne pourra jamais excéder une période d'un an. Théoriquement, c'est ainsi plus d'un tiers des peines prononcées qui pourraient être exécutées selon ce système<sup>2</sup>. Mais ce chiffre doit, bien entendu, être revu à la baisse dans la mesure où les condamnés qui en bénéficieront feront nécessairement l'objet d'une sélection, même si les termes de celle-ci ne sont pas déterminés par la loi<sup>64</sup>. Ce qui n'est pas toujours le cas à l'étranger. En Angleterre, par exemple, sont exclus du dispositif les délinquants sexuels en vertu du Sex offender Act de 1997 et les prisonniers de catégorie A<sup>3</sup>. Quant aux États-Unis, la pratique est variable, mais comme le rappelle A. Normandeau, plusieurs programmes opèrent une sélection des « *meilleurs risques* »<sup>4</sup>. Même si, comme on le constate, les chiffres invitent à la prudence, l'ADSE ne témoigne pas moins d'une évolution dans les formes d'intervention du pénal, et donc du pouvoir, susceptible de relancer le débat sur le dispositif carcéral et peut-être de mettre en cause ce constat d'une prison, « *détestable solution dont on ne saurait faire l'économie* ». <sup>5</sup>

#### LA FIN DES PROFESSIONNELS DE LA PUISSANCE PUBLIQUE

Cette première, et encore timide, mise en cause des murs de la puissance publique s'accompagne aussi de celle - et sans doute est-elle mieux observable - des professionnels qui l'incarnaient humainement. En effet, l'ADSE illustre un triple mouvement qui semble s'engager de déprofessionnalisation, de privatisation et de socialisation des personnels de la puissance publique.

Si l'on prend en effet pour exemple le cas des surveillants de prison, on s'aperçoit qu'avec l'ADSE, le rapport détenu/surveillants/administration n'a plus de sens institutionnellement. Il lui est substitué une autre relation triangulaire au sein de laquelle le surveillant perd sa place au profit de l'ordinateur qui joue le nouveau rôle de médiation entre le détenu et l'administration. Les réactions des organisations syndicales pénitentiaires témoignent d'ailleurs

des interrogations que suscite cette technique quant à la fonction même du surveillant. Alors même que ces dernières années, on cherche absolument à légitimer et à justifier socialement celle-ci de façon à lutter contre le malaise lancinant et constant de ce personnel, l'ADSE peut au contraire se traduire par sa déprofessionnalisation. Le surveillant peut en effet légitimement avoir le sentiment de perdre, dans un tel contexte, l'exclusivité de son savoir-faire. Ainsi, par la négative, resurgit le débat sur le rôle social du surveillant vis-à-vis du détenu et les organisations syndicales peuvent apprendre à se saisir d'arguments, notamment celui du risque d'une déshumanisation de la peine, qu'elles refoulaient jusqu'alors <sup>1</sup>. De surcroît, ce sont généralement les agents de probation qui se voient confier la responsabilité du suivi de la surveillance électronique. En France, la question est ouverte, la loi du 19 décembre 1997 ayant renvoyé aux décrets d'application le soin de préciser qui, des surveillants ou des agents d'insertion et de probation, seront chargés du suivi de l'assignation à résidence. On a là, de toute évidence, une nouvelle expression du rapprochement entre milieu ouvert et milieu fermé qui mérite d'être relevée, en raison notamment des interrogations qu'elle peut susciter sur le sens des missions respectives de leurs agents respectifs.

Mais les conséquences de cette évolution sont plus profondes encore. En effet, dans bien des expériences, ce ne sont plus les surveillants qui sont chargés du suivi de cette surveillance électronique. Ainsi, sont retenus à l'occasion de ces dispositifs, différents systèmes qui traduisent bien un mouvement de privatisation ou de socialisation de la puissance publique. En Angleterre, par exemple, ces missions échoient au secteur privé. Ainsi, ce sont trois grandes entreprises privées, *Premier UK*, *Securicor* et *American Company GSSC*, qui sont chargées d'installer l'équipement de surveillance électronique dans la résidence du condamné, de lui apposer le bracelet et de suivre le respect par ce dernier de ses obligations en signalant au service pénitentiaire toute rupture du signal électronique de présence <sup>2</sup>. Il en est de même aux Pays-Bas, où la possibilité a été ouverte d'une délégation de ces missions à des entre-

••••(1) FROMENT, 1998.

••••(2) BROADHEAD, 1998, p. 1800.

••••(1) MAC MAHON, 1996, p. 103 et suivantes.

••••(2) On peut ainsi concevoir qu'indirectement cette mesure est susceptible de rompre le principe de l'égalité face au logement que le conseil constitutionnel a doublement consacré dans ses décisions N°90-274 DC, 29 mai 1990, Rec., p. 61 et s, et N°94-359 DC du 19 janvier 1995, Rec., p. 176 et suivantes.

••••(3) BONNEMAISON, op. cit., p. 29.

••••(4) CABANEL, op. cit., p. 124.

••••(5) GLEIZAL, FROMENT, 1998.

prises privées. Cette possibilité a, en revanche, été exclue en France par la loi du 19 décembre 1997. Mais ce mouvement de privatisation de la justice pénale <sup>1</sup>, peut aussi prendre la forme, plus riche encore à analyser, d'une socialisation. Ainsi, dans le cadre de certaines expériences menées actuellement, notamment en Suède, un référent familial et professionnel doit se porter garant de l'ADSE du condamné. En France, le débat engagé dans les rapports Bonnemaïson et Cabanel a pu, à sa façon, témoigner de cette logique d'association de la société à l'œuvre de justice. Est, en effet, révélatrice la position des deux rapports sur le risque de rupture du principe d'égalité que cette mesure pourrait faire naître. Celle-ci étant en effet susceptible d'être appliquée de façon inégalitaire du fait qu'elle ne s'avère appropriée que pour les personnes dont l'existence comporte déjà des éléments de stabilité (domicile, foyer, travail, etc.) <sup>2</sup>, les deux rapports évoquent des mesures susceptibles de pallier ce problème. Le rapport Bonnemaïson prévoyait « *de développer une coopération étroite entre l'Administration pénitentiaire et les partenaires extérieurs pour offrir des hébergements permettant l'application de la mesure à tous les individus. Ce devra être une tâche prioritaire pour le conseil national des villes, les conseils départementaux et communaux de prévention de la délinquance* » <sup>3</sup>. Quant au rapport Cabanel, il écartait ce risque en évoquant une collaboration possible avec les structures associatives <sup>4</sup>. Mais, dans les deux cas, il s'agit d'une prise en charge sociale de l'exécution de la peine sur laquelle les auteurs s'appuyaient pour remédier à ce risque ; cette prise en charge est déjà bien engagée à travers la coopération renforcée de l'Administration pénitentiaire avec des associations para-administratives.

Cette évolution dépasse le cadre du seul dispositif de l'ADSE. D'une façon générale en effet, les nouvelles technologies de sécurité et les orientations des politiques de sécurité <sup>5</sup> semblent mettre en cause le principe de l'existence de « professionnels de la discipline ». Qu'il s'agisse des surveillants de prison, de la police ou encore des gendarmes, les corps de la fonction publique dépositaires de l'autorité publique, perdent leur exclusivité en matière de sécurité.

Les politiques de la ville et de sécurité, en encourageant une approche horizontale des problèmes de délinquance et de sécurité, favorisent le procès de dilution et d'interpénétration des rôles entre acteurs sociaux et de sécurité. Un mouvement que l'on observe aussi à travers le développement des polices municipales, du secteur de la sécurité privée, ou encore l'émergence des médiateurs, pénaux et sociétaux <sup>1</sup>. Les adjoints de sécurité fournissent à ce titre une évolution exemplaire. Ici, le mouvement de privatisation de ces fonctions ne renvoient pas exclusivement à une logique du marché, à une logique managériale, mais plus fondamentalement à un processus de socialisation qui témoigne d'une recomposition des formes dans lesquelles tente de s'incarner et de s'exercer aujourd'hui la puissance publique. C'est bien à la fin de l'idée d'un personnel spécialisé dans les fonctions de sécurité, c'est aussi à la perte de visibilité de l'État dans sa fonction souveraine à laquelle on assiste peu à peu aujourd'hui. Ainsi l'évolution, annoncée par G. Deleuze, vers une « *société de contrôle* » <sup>2</sup> semble de plus en plus avérée. Et le droit pénal en témoigne avec force, les rôles se dissolvant peu à peu dans la responsabilité de l'action criminelle. <sup>3</sup> L'ADSE n'en donne à ce titre qu'un nouvel exemple.

## CONCLUSION

Mais pour autant, cette analyse ne doit pas évacuer la question de la visibilité du pouvoir. Ce dernier, en effet, a besoin d'être mis en scène, d'être re-présenté. Il ne peut se passer d'une théâtralisation qui est constitutive de sa puissance même. C'est pourquoi on doit aussi émettre l'hypothèse selon laquelle l'ADSE, plutôt qu'une dilution de la visibilité de la puissance publique, illustre une recomposition de celle-ci. On pourra notamment l'identifier en observant le mouvement de re-corporisation ou de réincorporation de la peine qu'elle implique. Nous pensons en effet que ce retour de la peine dans le corps doit fondamentalement s'analyser comme une forme actuelle de recomposition du politique. Pendant longtemps en effet, c'est dans l'éclat des supplices corporels que le pouvoir souverain s'est mis en

••••(1) Cf., notamment sur cette évolution, *Les cahiers de la sécurité intérieure*, n°33, 1998.

••••(2) DELEUZE, 1990.

••••(3) PONCELA, *Op. cit.*

••••(1) FOUCAULT, *Op. cit.*

••••(2) DELMAS SAINT-HILAIRE, 1994, p. 34.

••••(3) BECCARIA (1764), 1991, p. 87.

••••(4) de TOCQUEVILLE, 1984, p. 107.

••••(5) Sur cette dimension, essentielle, de la surveillance électronique, se reporter à notre article paru à la *Revue interdisciplinaire d'études juridiques*, *Op. cit.*

scène. Il suffit de se rappeler la description faite par M. Foucault du supplice de Damien pour comprendre comment la peine théâtralisait le pouvoir <sup>1</sup>. Or, l'émergence de la prison pour peine, à la fin du XVIII<sup>e</sup> siècle, a traduit une nouvelle économie de la visibilité du pouvoir. Il est alors décidé que « *la cible de la répression pénale ne serait plus le corps du condamné, elle serait désormais la liberté du condamné* » <sup>2</sup>. Et sans que ce déplacement de la peine du corps vers l'esprit ne soit pensé comme son adoucissement, ainsi que l'écrit Beccaria <sup>3</sup> et le confirme Alexis de Tocqueville : « *Ici la peine est en même temps la plus douce et la plus terrible qui ait jamais été inventée. Elle ne s'adresse qu'à l'esprit de l'homme, mais elle exerce sur lui une incroyable emprise* » <sup>4</sup>. L'ADSE semble révéler aujourd'hui un mouvement qui s'exerce dans la direction inverse ; elle permet le retour de la peine dans le corps. Dès lors, il nous apparaît que re-corporation ou réincorporation de la peine n'est pas neutre du point de vue de la visibilité du pouvoir. La pénalisation du corps traduit et permet en réalité une nouvelle mise en scène du pouvoir. Mais cela est une autre histoire <sup>5</sup>.

#### ■ Jean-Charles FROMENT

*Université P. Mendès France de Grenoble, CERDAP.*

## BIBLIOGRAPHIE

- BARLOY (F.), « Le Conseil constitutionnel, la liberté individuelle et l'ordre public », *RA*, n°287, Sept-oct. 1995, p. 483 et suivantes.
- BECCARIA (C.), 1764, *Des délits et des peines*, GF-Flammarion, 1991, p. 87.
- BENGHOZI (M.), 1990, « L'assignation à domicile sous surveillance électronique », *Déviance et société*, vol. 14, n°1, p. 59 et suivantes.
- BONNEMAISON (G.), 1990, *La modernisation du service public pénitentiaire*, Rapport au garde des Sceaux et au premier Ministre.
- BISHOP (N.), 1995, « Le contrôle intensif par surveillance électronique : un substitut suédois à l'emprisonnement », *Bulletin d'information pénologique*, n°19-20, p. 8 et suivantes.
- BROADHEAD (J.), 1998, « Tagging », *New Law Journal*, 4 décembre, p. 1800.
- C.C, N° 89-164 DC du 29 décembre 1983, Rec., p. 67.
- C.C, N° 76-75 DC du 12 janvier 1977 « Fouille des véhicules », Rec., p. 33.
- C.C, N°93-325 DC, 12-13 août 1993, relative à la maîtrise de l'immigration, G.D.C.C, N°47.
- C.E.D.H, Silver, 25 mars 1983, Série A, Vol. 61.
- C.E.D.H, Schönenberg et Durmaz, 20 juin 1988, Série A, Vol. 137.
- C.E.D.H, Campbell et Fell, 28 juin 1984, Série A, Vol. 80.
- C.E.D.H, Golder, 21 janvier 1975, Série A, Vol. 18.
- CABANEL (G.), 1995, *Pour une meilleure prévention de la récidive*, Rapport d'orientation au premier Ministre, p. 115-139.
- « Les technologies de sécurité », 1995, *Les cahiers de la sécurité intérieure*, N°21.
- « Les partages de la sécurité », *Les cahiers de la sécurité intérieure*, N°33, 1998.
- COLLETT (S.), 1999, « Checking out », *The Guardian*, 27 janvier.
- COMBESSIE (P.), 1996, *Prisons des villes et des campagnes. Etude d'écologie sociale*, Paris, éditions de l'Atelier éditions Ouvrières.
- COUVRAT (P.), 1998, « Une première approche de la loi du 19 décembre 1997 relative au placement sous surveillance électronique », *RSCDPC*, n°2, avril-juin, p. 374 et suivantes.
- CUSSON (M.), 1998, « Peines intermédiaires, surveillance électronique et abolitionnisme », *RICPT*, n°1, p. 34 et suivantes.
- DC, N°90-274, 29 mai 1990, Rec., p. 61 et suivantes.
- DC, N°94-359 du 19 janvier 1995, Rec., p. 176 et suivantes.
- DELMAS SAINT-HILAIRE (J-P.), 1994, *La prison, pourquoi faire ? Problèmes actuels de science criminelle*, T. VII, P.U d'Aix-Marseille, p. 34.
- DELEUZE (G.), 1990, *Pourparlers*, éditions de Minuit.
- DEMONCHY (C.), 1998, « Architecture et évolution du système pénitentiaire », *Les cahiers de la sécurité intérieure*, n°31, 1998, p. 79.
- DONZELOT (J.), 1984, *L'invention du social. Essai sur le déclin des passions politiques*, Paris, Fayard.

## BIBLIOGRAPHIE

- FERRY (L.), 1991, « L'humanisme juridique en question. Réponse à B. Edelman », *Droits*, n°13, p. 43 et suivantes.
- FOUCAULT (M.), 1975, *Surveiller et punir. Naissance de la prison*, Gallimard, Paris.
- FRANGI (M.), *Constitution et droit privé*, Economica, 1992.
- FROMENT (J.-C.), 1996, « Le pouvoir souverain, la peine et le corps : éléments pour une philosophie pénale de la surveillance électronique », *RIEJ*, n°37, p. 1 et suivantes.
- FROMENT (J.-C.), 1996, « L'assignation à domicile sous surveillance électronique et les libertés publiques », *RDP*, p. 121 et suivantes.
- FROMENT (J.-C.), 1999, *Médiation pénale et ajustement du droit*, in *Les mécanismes de régulation de la sécurité*, L'Harmattan, à paraître.
- FROMENT (J.-C.), « La République des surveillants de prison (1958-1998) », Paris, *LGDJ*, 1998.
- GLEIZAL (J.-J.), FROMENT (J.-C.), *Les politiques locales de sécurité*, éditions La lettre du cadre territorial, 2e éd., 1998.
- GLUCKSMAN (A.), 1967, *Le discours de la guerre*, Union Générale d'Éditions, Coll. 10/18, p. 75.
- HABERMAS (J.), 1978, *L'Espace public. Archéologie de la publicité comme dimension constitutive d'une société bourgeoise*, Paris, Payot.
- HAGSER (P.), 1990, *La protection de la vie privée*, Paris, Economica, 2e éd..
- KAYSER (P.), *La protection de la vie privée*, Economica, P.U.d'Aix-Marseille, 1990.
- KELSEN (H.), 1988, *Théorie pure du droit*, éditions de la Baconnière, deuxième édition, p. 174.
- KUHN (A.), MADIGNIER (B.), 1998, « Surveillance électronique : la France dans une perspective internationale », *RSCDPC*, n°4, Oct-Déc., p. 671 et suivantes.
- LANDREVILLE (P.), 1987, « Surveiller et prévenir ; l'assignation à domicile sous surveillance électronique », *Déviante et société*, vol. 11, n°3, p. 251 et suivantes.
- LIGUE DES DROITS DE L'HOMME, *Des puces, des souris et des hommes. Sciences, techniques et droits de l'homme*, 4e université d'automne, Novembre 1998.
- LUCHAIRE (F.), « La vidéosurveillance et la fouille des voitures devant le Conseil constitutionnel », *RDP*, p. 590.
- MAC MAHON (M.), 1996, « La répression comme entreprise : quelques tendances récentes en matière de privatisation et de justice criminelle », *Déviante et société*, vol. 20, n°2, p. 103 et suivantes.
- MARY (P.), 1998, *Délinquant, délinquance et insécurité. Un demi-siècle de traitement en Belgique (1944-1997)*, Bruylant, 1998
- MARY (P.), (dir.), 1997, *Travail d'intérêt général et médiation pénale. Socialisation du pénal ou pénalisation du social ?*, Bruylant.
- de MONTVALLON (J.-B.), 1996, « Les sénateurs introduisent le « bracelet électronique » dans la réforme de la détention provisoire », *Le monde*, 31 mai, p. 9.

## BIBLIOGRAPHIE

NORMANDEAU (A.), 1996, « Bilan criminologique de quatre politiques et pratiques pénales américaines contemporaines », RSCDPC, n°2, avril-juin, p. 333 et suivantes.

PONCELA (P.), 1983, « Droit de punir et Pouvoir de punir : une problématique de l'État », *Archives de philosophie du droit*, tome 28, p. 123 et suivantes.

PRADEL (J.), 1998, « La prison à domicile sous surveillance électronique. Nouvelle modalité d'exécution de la peine privative de liberté. Premier aperçu de la loi du 19 décembre 1997 », *RPDP*, n°1-2, p. 15 et suivantes.

ROUBAN (L.), 1994, *Le pouvoir anonyme. Les mutations de l'Etat à la française*, Presses de la Fondation Nationale des Sciences Politiques, p. 41.

ROBERT (J.), DUFFAR (J.), 1994, *Droits de l'homme et libertés fondamentales*, PUF, Montchrestien, p. 369 et suivantes.

SENNETT (R.), 1981, *Autorité*, Paris, Fayard.

SFEZ (L.), 1993, *La politique symbolique*, Quadrige/Presses Universitaires de France.

SUDRE (F.), 1998, *Droit international et européen des droits de l'homme*, PUF, Droit fondamental.

TOCQUEVILLE (A.) de , cité par M. Perrot, « Alexis de Tocqueville et les prisons », *Médecine et hygiène*, in PETIT (J.G.) (Sous la dir.), *La prison, le bague et l'histoire*, Méridiens, 1984, p. 107.

TRAVIS (A.), First inmates to go free in new tagging system, *The guardian*, 27 janvier 1999.

WEBER (M.), 1963, *Le savant et le politique*, Union générale Générale d'édition, Coll. 10/18, p. 100.

WYVEKENS (A.), 1997, *L'insertion locale de la justice pénale*, L'Harmattan.

WYVEKENS (A.), 1997, « Entre médiation et justice pénale, l'activité judiciaire des maisons de justice du Rhône », *Archives de politique criminelle*, n°19, p. 73.



# LA POLICE DANS LA SOCIÉTÉ DU RISQUE ET DE L'INFORMATION<sup>1</sup>

Un texte de Richard V. Ericson et de Kevin D. Haggerty

Les Fondamentaux de la sécurité

169

Dans sa critique publiée dans la dernière livraison des *Cahiers de la sécurité intérieure*, Maurice Punch tient en substance ces propos : « Cette somme considérable que représente le livre de R. V. Ericson et K. Haggerty contribuera sans nul doute à la redéfinition des recherches sur la police. Policing the Risk Society mérite non seulement les éloges de toute recherche soigneusement et amplement documentée, solidement argumentée et audacieuse dans ses prises de position, mais ne propose rien moins qu'un nouveau paradigme situant la police au cœur de la société du risque (...). En substance, on peut tenter de présenter le propos de Haggerty et d'Ericson autour des points suivants : à la suite de Beck, Foucault, Ciddens et quelques autres, ils perçoivent la police comme un intermédiaire informationnel situé au cœur

de la société du risque, destiné à la surveillance, l'échange d'informations, l'audit, la communication et la classification ». Élogieux mais lointain, ce compte rendu ne pouvait que nous donner envie d'aller plus loin dans la découverte de l'ouvrage des deux canadiens. Traditionnellement, les textes logés à l'enseigne des *fondamentaux* sont patinés par l'épreuve du temps qui leur confère lettres de noblesse et légitimité, mais il nous paraissait normal que dans un numéro consacré à l'information, et en quelque sorte prospectif, cette règle est inversée. Qui plus est, si cette traduction abrégée de *Policing the risk society* est la première en français, l'ouvrage existe depuis 1997 de l'autre côté de l'Atlantique.

Commençons par les auteurs, tous deux canadiens. Si Kevin Haggerty est peu connu - il a

•••(1) La rédaction des *Cahiers* remercie tout particulièrement les auteurs et les presses de l'Université de Toronto pour leur avoir donné gracieusement le droit de traduire puis de reproduire plusieurs passages importants de l'ouvrage de: ERICSON (Richard V.), HAGGERTY (Kevin D.), 1997, *Policing the Risk Society*, Toronto, University of Toronto Press, 487p.

récemment soutenu sa thèse sur « les comptes du crime » - Richard V. Ericson est pour sa part un habitué de l'univers de la recherche sur la police, qu'il anime régulièrement de ses travaux depuis 1975. Pourtant - est-ce le simple effet de la nouveauté ? - le présent ouvrage ne semble pas résonner exactement du même son de cloche que les précédents, comme s'il représentait une forme d'aboutissement. Quelle est sa force évidente et si particulière ?

L'une des principales difficultés que pose la police constituée en objet de recherche réside dans son articulation à la société : quelle est la bonne focale pour l'appréhender ? À trop vouloir aborder la police du dehors, on risque d'en livrer une vision stéréotypée et inexacte. Inversement, la monographie du monde policier, malgré la précision de ses détails, confinant parfois au folklore, conduit à saisir les interactions et les conflits dans l'ordre statique du vase clos et à privilégier une forme d'inertie. Cette difficulté épistémologique est significative d'une tension essentielle de l'objet, toujours pris en tenailles entre isolationnisme et ouverture concédée et nécessaire à la société. Quelle doit être la valeur d'interaction entre les deux dimensions, et comment la prendre en compte ? Comme Maurice Punch le soulignait, comme eux-mêmes l'indiquent dans leur introduction, R. Ericson et K. Haggerty n'ignorent pas cette difficulté et la dépassent en replaçant leur objet dans le cadre plus large du changement social. Ce n'est pas la police qui insuffle les changements mais bien elle qui se transforme, dans un processus d'adaptation plus ou moins heurté, sans que ses cadres en prennent toujours conscience. Les auteurs font figure de révélateurs de ce changement en nous présentant une police nouvelle de part en part, même si leur propension à la généralisation reste l'ob-

jection majeure qu'on pourrait leur adresser. La police a évolué au contact de deux éléments qui, eux, qualifient le changement général : le risque et les nouvelles technologies.

C'est la richesse essentielle de ce travail que d'avoir articulé les deux notions, autrement dit les paradigmes informationnel et assurantiel. En bref, l'analyse actuarielle du risque qui caractérise la rationalité du monde des assurances colonise la compréhension du monde par le biais de la généralisation de technologies qui permettent un calcul systématique et instantané des probabilités de risques tels que la survenance de fraudes ou d'infractions de masse. Comment justifier une telle évolution au regard d'un critère d'efficacité, quel intérêt, sinon quel désavantage, y aurait-il à calculer systématiquement, à rendre toute action plus complexe ? La question devient dès lors celle de la causalité d'une telle évolution et s'avère plus difficile à résoudre. Parmi d'autres explications, on peut attribuer ce passage à l'ère du risque comme une conséquence de la fiscalisation de l'État : avec la crise de l'État-providence, on cherche à rationaliser et optimiser toute rentrée fiscale en évitant au maximum les pertes (l'évasion) générées par les contentieux de masse. La capacité de calcul et du tri des informations actuelle permet le ciblage de populations à risque jusqu'à individualiser la probabilité des risques de passage à l'acte là où, auparavant, il était illusoire de rechercher l'aiguille dans la botte de foin. L'aléa finit par se transformer en quasi certitude.

Certes ces outils et cette posture de travail peuvent être reproduits dans le monde policier, et les auteurs montrent qu'au Canada, tout du moins, cette évolution devient réalité. Mais appliquée aux méthodes de travail policier, elle a des conséquences non négligeables : elle

tend à modifier plus fondamentalement la nature du contrôle social. D'une économie de la dissuasion-prévention-répression, on passe à un mode de conformité-conformation. Idéalement, chaque citoyen sait qu'il devient difficile de jouer avec la norme, que ses écarts sont repérables, repérés et potentiellement sanctionnés. La caractérisation de cette évolution est encore largement prospective et malaisée à mettre en évidence ; d'autres auteurs évoquent l'émergence d'un véritable pouvoir de stimulation. Fonctionnellement, cette évolution serait de nature à régler les problèmes très actuels de perte de légitimité et d'efficacité de l'autorité, l'engorgement de la réponse judiciaire. Dans ce modèle, le règlement du conflit est possible en amont de la justice, ce que Nicholas Dorn cherche à démontrer en employant le terme de police post-pénale <sup>2</sup>.

L'ouvrage est dense et dresse un panorama relativement exhaustif des questions inhérentes à la police entendue comme « *policing* ». Pour en donner une vue générale et didactique, nous avons choisi d'en traduire l'introduction, et des éléments de la première partie qui synthétisent les thèmes principaux : les policiers comme travailleurs du savoir (*knowledge workers*) ; la théorie et le rôle du risque par rapport à la loi ; l'importance de la notion de régulation ; le passage d'un mode social de dissuasion à un mode de conformation.

Des éléments importants ont cependant été laissés de côté, que nous souhaiterions rapidement aborder ici. Tout particulièrement la conception que développent les auteurs à propos du *Community policing*, notion voisine de notre police de proximité (p. 67-80).

Pour en traiter, les auteurs retracent l'importan-

te discussion opposant les chercheurs anglosaxons sur la question depuis quinze ans. Trois conceptions s'opposent en effet : pour les uns, la police de proximité ne serait que pure rhétorique visant à masquer le besoin d'une ressource de coercition forte et rapidement mobilisable (BAYLEY, MURPHY, MANNING, WADDINGTON) ; pour d'autres, il s'agirait plutôt d'une philosophie ou d'un état d'esprit qui structurerait par la suite des pratiques (GIDDENS, DANDEKER) ; pour d'autres, enfin, ce serait une pratique effective, ancrée dans la notion de communauté (GOLDSTEIN, MOORE). Les auteurs s'inscrivent plutôt dans la perspective de Giddens, qui récusé l'opposition binaire entre le symbolique et la réalité, tout en précisant par quel moyen réel la « proximité » est envisagée. La proximité serait un ajustement et une médiation rendus possible par un travail important de communication et de traitement de l'information de la part de la police, permettant de cibler les populations au plus près et de répondre aux demandes des institutions du « risque administré ». La police agirait alors au plan local comme une sorte d'intermédiaire informationnel, de même que la possession d'informations lui permettrait de trier dans ses interventions, d'agir dans une posture de résolution des problèmes de façon plutôt proactive.

D'autres aspects longuement abordés dans l'ouvrage sont ici laissés de côté notamment les conséquences de l'informatisation au sein de l'institution elle-même, sur les relations hiérarchiques, et la capacité de contrôle des agents de la force publique. Comme toute innovation, celle que procure la révolution informationnelle se présente pour les policiers sous un aspect dual : si l'utilisation de l'informatique tend à cas-

•••(2) « Les nouvelles formes de renseignement policier », *Les Cahiers de la sécurité intérieure* n°32, deuxième trimestre 1998, p. 137-150.

ser la relation hiérarchique de verticalité classique entre un supérieur et un subordonné au profit d'une relation de collaboration et d'interdépendance, l'informatique est relativement mal vécue par les policiers de la base. Elle présente pour eux un potentiel fortement liberticide en permettant de consigner et de vérifier chacune de leur démarche et opérations. Ce phénomène classique d'appréhension de l'innovation conduit les agents à adopter des tactiques d'évitement. Dans le cas du contrôle par voie informatique, étant donné sa puissance et sa précision, ces tactiques semblent se radicaliser d'autant : par exemple, les policiers censés intervenir sur des violences domestiques graves sont conduits à interroger « victime et auteur » pour les besoins d'un questionnaire à destination du ministère du Bien-être Social au Québec. En pratique, ce questionnaire étant difficile à remplir, les agents préfèrent ne pas déclarer l'affaire ou affirmer qu'il n'y a pas eu de violence. Par ailleurs, chaque fois qu'un dossier est rempli de façon inexacte, incomplète ou incorrecte, l'agent est rappelé à l'ordre par voie informatique. C'est ainsi que la confiance s'étiole et que le travail s'effectue dans une atmosphère de suspicion réciproque.

Les critiques les plus importantes adressées à cet ouvrage concernent essentiellement sa portée paradigmatique : Jean-Paul Brodeur a fait observer qu'un travail de recherche qui prétend

fonder un nouveau paradigme doit offrir un protocole et les moyens de sa reproduction à l'identique en d'autres occasions pour d'autres objets<sup>3</sup>. Or, Ericson et Haggerty auraient omis de qualifier en annexe les entretiens étayant leurs conclusions. L'ouvrage fait en réalité état de très peu d'indications temporelles, de précisions géographiques, bref d'éléments d'enquête systématique, permettant d'asseoir la thèse. Du coup, cela le rangerait dans la catégorie des essais. Selon Brodeur, l'ouvrage correspondrait à la réalité de certains services spécifiques - comme le service de renseignement canadien, CSIS - mais resterait éloigné de la réalité de certains autres. Par ailleurs, l'ouvrage ne serait pas exempt de confusions entre information et connaissance - autrement dit entre savoir spéculatif et savoir confirmé. Surtout, alors que la notion de risque est omniprésente dans l'ouvrage, de façon surprenante, elle reste très insuffisamment théorisée ou problématisée, ce qui nuit à la force de la démonstration. Quoi qu'il en soit de ces réserves, il faut reconnaître aux auteurs le talent d'avoir fourni un travail dont le caractère heuristique ne fait pas de doute. Surtout, en élargissant la notion de police à celle de « *policing* », ils montrent les mutations de l'institution et de la société, et posent le caractère absolument indissociable des deux. Gageons que d'autres sauront emprunter la voie tracée.

■ Nicolas DUPEYRON

•••(3) *Revue canadienne de criminologie*, octobre 1998, *Revue des livres, Policing the Risk Society*, p.455-465.

## *Policing the Risk Society*<sup>1</sup> : introduction

La police est partout présente dans la vie sociale contemporaine. Elle est présente dans la rue. Sa présence se fait encore plus lourdement sentir à travers les émissions de télévision mettant en scène, dans des scénarios trépidants, des héros policiers et leurs hauts faits. C'est vers elle que l'on se tourne lorsque l'on est en butte à des problèmes personnels, des accidents et des agressions. Elle est présente lors des cérémonies officielles, à l'occasion des événements sportifs, des défilés et des manifestations. Des cartes postales et des souvenirs sont vendus qui représentent des agents de police en tenue, dignes représentants de la noblesse de la communauté et de l'État nation. À travers toutes ces formes de présence, la police reproduit et représente tout à la fois l'ordre. Elle incarne l'autorité centrale sous les espèces de la paix, de l'ordre et du bon gouvernement.

Ce livre se propose de repenser de manière fondamentale notre conception de la police. Si la recherche sur la police est proliférante, elle est aussi incroyablement redondante et stagnante. Il est donc nécessaire de revenir de manière critique sur cette littérature existante, afin de produire une théorie compréhensive de la police qui permette une analyse fouillée des buts et des conséquences de la police de l'ordre. Nous faisons l'hypothèse dans cet

ouvrage que le travail de la police, tout comme la société dans laquelle il s'exerce, doivent être compris à travers un modèle de la communication de risque. Dans ce livre, on s'attache à comprendre comment la police identifie et gère les risques en tenant également compte de ce qui se fait dans d'autres institutions. Notre hypothèse est que le travail de la police consiste en une coordination d'activités en interaction avec d'autres agents placés dans d'autres institutions, tous formant une large base sociétale pour le *management des risques* (gouvernance) et de la sécurité (garanties contre les pertes).

La notion de risque renvoie à l'idée de danger extérieur, comme les désastres naturels, les catastrophes technologiques, ou toute forme de réalité menaçante pour le genre humain. Le système de communication sur la question des risques - ses règles, son cadrage et ses technologies - contribue à la définition sociale du risque. Il constitue donc une pierre d'angle de notre analyse. La recherche se concentre sur les systèmes de communication que les institutions développent pour identifier et gérer les risques, et sur la manière dont la police est impliquée dans ces systèmes. La signification du risque varie en fonction du système de communication utilisé par les institutions responsables de

•••(1) Des extraits du livre de ERICSON (Richard. V.), HAGGERTY (Kevin. D.), p.3-14 (introduction) ; p.17-19 ; p.21-23 ; p.25-27 ; p.36-38 (partie 1, chap.1) ; p.39-42 ; p. 48-52 (partie 1, chap.2).

leur gestion, et de ce point de vue l'institution policière se trouve prise dans un champ complexe de relations ambiguës, mouvantes et contradictoires.

Les systèmes de communication ne sont pas de simples véhicules de la circulation du savoir. Bien au contraire, ils ont leur propre logique et renvoient à des processus autonomes. Ils déterminent à la fois les relations institutionnelles et ce que les individus et leurs organisations sont capables d'accomplir. Il n'y a pas d'un côté des événements qui surviennent dans le monde et à propos desquels on communique. L'événement est construit, rendu visible et traité au travers le filtre de règles, de cadrages et de technologies disponibles dans le système de communication. Le système de communication fait exister l'événement. Aussi pour comprendre la manière dont la police travaille est-il nécessaire d'analyser les logiques et les processus du système de communication auquel elle participe et qui dictent la manière dont elle est organisée et évaluée.

Ce livre repose sur une enquête ethnographique qui entend rendre compte de la manière dont la police est organisée au sein des systèmes de communication sur les risques. Des entretiens approfondis ont été réalisés auprès de 155 personnes de la tenue et des services administratifs de la police ; nous avons observé leurs activités et analysé leurs documents. Si la recherche empirique porte sur la police canadienne, les liens établis avec les sources secondaires de la littérature sur la police et la

théorie sociale suggèrent que les spécificités identifiées ici sont généralisables au cas d'autres États-nations.

Les données font l'objet d'une analyse dans le cadre d'un modèle qui inclut les récentes avancées en théorie sociale concernant le risque, la gouvernance et la communication. Si l'accent est principalement mis sur les voies par lesquelles les règles de communication, les cadrages et les technologies structurent les organisations de police en relation avec d'autres institutions, nous aborderons aussi la question de savoir comment les communications au sein de la police expriment de manière générale des traits propres de nos sociétés. De ce point de vue, le livre ne fournit pas seulement une base empirique pour comprendre le travail de la police selon une approche radicalement nouvelle mais il contribue également aux théories de la société du risque, de la gouvernabilité et de la communication organisationnelle.

Dans le développement de notre propos, nous avons suivi un mode d'exposition quelque peu hérétique au regard des canons académiques. Au lieu d'ouvrir par les aspects les plus théoriques qui informent notre analyse, nous commençons par une analyse critique de la littérature existante sur le travail de la police. Cette analyse démontre que d'autres chercheurs ont presque totalement laissé de côté les systèmes policiers de communication sur les risques. Pourtant, on verra que la littérature existante souligne à tout le moins leur importance dans les modes opéra-

toires. La théorie abstraite de la société du risque prendra un sens beaucoup plus concret après que les problèmes pratiques dont la littérature traite en matière de risque auront été exposés. Théoriser la société du risque à l'issue de cette revue de la littérature offre non seulement des armes à la critique des travaux antérieurs mais permet également un cadre explicatif pour les analyses empiriques présentées ensuite.

Dans la première partie, notre analyse de la littérature existante sur le travail de la police nous amène à défendre l'idée selon laquelle la mobilisation de la police n'est pas seulement affaire d'intervention dans la vie individuelle des citoyens mais renvoie aussi aux demandes institutionnelles pour une meilleure connaissance des risques. Du coup, le premier lieu d'exercice des activités policières se situe au niveau des systèmes de communication sur les risques mis en place par d'autres institutions. À travers ces systèmes de communication, celles-ci ont accès de manière routinière à la police pour obtenir des connaissances utiles à la gestion des risques qu'elles ont à connaître. Cet accès routinier rend le travail de la police hautement visible et circonscrit à la fois l'autonomie des organisations policières et l'arbitraire des fonctionnaires.

Le système judiciaire est l'une de ces institutions parmi d'autres qui s'organisent au travers des systèmes de communication sur les risques et la justice est sans aucun doute la plus centrale et la plus influente en terme de police de

l'ordre. Avant que de servir à la poursuite et au jugement des activités criminelles, la plupart des connaissances ayant trait au crime, produites par la police sont disséminées en direction d'autres institutions (par exemple, dans le domaine de la santé, de l'assurance, de l'assistance sociale, de la finance et de l'éducation) pour satisfaire leurs besoins de *management des risques*. Si la police a tous les moyens coercitifs pour produire cette connaissance en matière de crime, il se trouve qu'elle en fait d'abord profiter des institutions dont le principe d'action ne doit rien à la coercition. Le contrôle coercitif donne lieu à des catégorisations contingentes. Le maintien de l'ordre public s'effectue à la fois à travers la surveillance du territoire et à un niveau extra-territorial de connaissance abstraite des risques en matière de sécurité (moyens d'échange économiques), de carrières (*management des cycles de vie*) et d'identité de la personne.

La police communautaire est ici analysée comme un discours visant à rationaliser, après coup, la gestion des risques sociaux. La police communautaire est en fait une police de gestion des risques. Cela s'explique par le fait que nos communautés reposent sur une communication des risques, qui laisse bien peu de place à tout ce qui se situerait en dehors des classifications institutionnalisées de ces risques.

La seconde partie du livre se compose d'une discussion théorique élargie du contexte de la société de risque dans lequel se développe le travail de la poli-

ce. En vertu d'une sorte de logique négative, la société du risque focalise sur la peur et la distribution sociale des «maux» plutôt que sur le progrès et la distribution sociale du «bien». La peur collective et les appréhensions étayent le système de valeurs d'une société insécure, d'une insécurité perpétuelle et viennent nourrir d'incessantes demandes pour plus de connaissance du risque. La peur finit par créer ses propres démons, au fur et à mesure que prolifèrent de nouveaux systèmes de gestion et d'information sur les risques. Les mécanismes de surveillance de ces systèmes définissent des profils humains types, en fonction des menaces qu'ils sont censés provoquer et des risques qu'ils peuvent encourir. Les individus sont construits par les normes institutionnellement établies : le risque est toujours quelque part sur le *continuum* d'une imprécise normalité.

La communication de risques mêle les deux dimensions de la confiance et du privé. Plus l'appréhension et la peur conduisent les individus à se retirer d'un engagement public, plus ces derniers valorisent la sphère privée et s'enferment dans un mode de vie très cloisonné. Plus ce retrait vers le privé se développe, plus se fait sentir le besoin de mécanismes de surveillance propres à assurer une connaissance nécessaire pour permettre la confiance dans des transactions institutionnelles anonymes. Paradoxalement, ces mécanismes viennent interférer avec la sphère privée et fonctionnent comme un constant rappel des incertitudes de la confiance.

Pourtant, ce n'est que dans un cadre de confiance que des conceptions du risque peuvent s'institutionnaliser correctement pour former la base des décisions. La préservation du privé, la confiance, la surveillance et la gestion du risque marchent main dans la main dans la gestion des probabilités et des possibilités de l'action.

Dans la société du risque, la gouvernance est privatisée et dispersée en une myriade d'institutions fragmentées. Les organisations et les individus sont censés être auto-suffisants et s'occuper de la gestion de leurs propres risques. Le thème de la gouvernance individuelle est renforcé dans sa prééminence par les discours imbriqués du droit, de la morale, de la responsabilité politique et financière.

Dans le cadre de la morale utilitariste de la gestion des risques, la norme, le standard du risque acceptable est toujours à la fois de nature factuelle et morale. Cela signifie que l'on a recours aux standards typiques ou usuels, mais assortis de contraintes éthiques. Les classifications des risques distillent une certitude morale et une certaine légitimité dans les faits qu'elles produisent, autorisant les individus à les considérer comme des obligations normatives et donc comme des schèmes d'action. La légitimité d'une morale utilitariste dans le discours sur le risque est épaulée par un discours sur les droits. Le discours sur les droits s'est développé avec la décentralisation du politique en nombre d'institutions dotées de moyens propres de justice distributive.



Il fournit une éthique du possible et du probable enchâssée dans les règles légales du droit. Il participe d'une politique de la différence, laquelle conteste la moralité des classifications du point de vue de la sécurité que ces règles légales du droit offrent ou non. Dans un modèle d'auto-gouvernance, les organisations et les individus doivent contribuer au bien commun en étant responsables pour leur part, tant pour les risques qu'ils engendrent pour eux et pour les autres. Il faut être auto-suffisant, être capable de gérer sa biographie de manière compétente, de bâtir sa propre économie politique. Tout cela ne débouche pas sur l'autonomie mais plutôt sur la structuration institutionnelle des carrières individuelles et des organisations à des fins de gestion pratique des risques.

Dans la troisième partie, on trouve une analyse de la manière dont la police participe à la communication sur les risques en matière de surveillance du territoire et de sécurité. La police a recours à une grande variété de technologies électroniques pour dresser une cartographie des troubles. Elle fonctionne comme un outil de suivi des mouvements de population dans l'espace et le temps, par exemple à travers les contrôles d'identité sur la voie publique, le fichage des contrevenants, les services d'ordre mis en place lors d'événements exceptionnels, la surveillance de la sécurité des entreprises et des particuliers, les systèmes d'enregistrement des voitures et des permis de conduire. Elle offre une expertise en

matière d'implantation territoriale pour les institutions qui ont à gérer des zones données. Au total, ce que chacun peut voir fonctionner de manière concentrée dans les lieux gérés par des entreprises de sécurité privée comme les centres commerciaux et les parcs de loisirs, existe également de manière plus dispersée dans l'ensemble du paysage urbain.

La quatrième partie offre une analyse empirique de la manière dont la police participe à la communication sur les risques en matière de sécurité, de carrières et d'identités, domaines plus larges qui ne réfèrent pas directement à la gestion des territoires. Ces systèmes permettent de délimiter des profils types en matière de risque afin de faciliter les échanges économiques, la gestion des cycles de vie et des identités. Ils sont fondés sur des systèmes abstraits de confiance et de risque requérant des mécanismes sophistiqués de surveillance qui ne soient pas reliés à des limites territoriales. Ils renvoient en fait à des limites institutionnelles qui traversent le temps et l'espace mais qui contribuent néanmoins à maintenir les individus à leur place.

Des garanties comme les certificats, les lettres de référence et les instruments financiers attestent du crédit, de la propriété, de l'identité et des niveaux de réalisation. Ils offrent une sécurité et une protection contre tout risque de perte, de dommage ou de défaut qui pourrait survenir. Dans ce travail par lequel les institutions établissent la confiance et l'efficacité au moyen de

ces sécurités, la police joue un rôle essentiel. En particulier, la police participe à la coordination des connaissances inter-institutionnelles, à la définition des risques, à l'audit, toujours dans le but de vérifier la valeur des données liées aux garanties, les produits et les marchés.

La police aide également les institutions à construire les carrières des populations qu'elles ont à gérer. Dans les aspects les plus routiniers de leur travail - par exemple, en faisant un rapport d'accident de la route, dans un contrôle d'identité sur la voie publique, un contrôle du personnel d'une entreprise, en fichant les informations sur les suspects, les victimes et les informateurs - les policiers enregistrent les échecs et les réussites les plus significatifs des individus, leurs bonnes références et leurs démérites, leurs comportements routiniers comme leurs accidents de parcours.

Ces routines du travail policier aident également les institutions à construire les identités des populations. La seule existence de cases à remplir dans les formulaires de police, mentionnant par exemple l'âge, la race, le genre et l'appartenance ethnique, force les gens à adopter des identités institutionnelles spécifiques. Dans ce livre, nous donnons quelques exemples de cette police des identités. Nous analysons par exemple la police de la jeunesse. La police aide à définir des limites sociales en travaillant dans les interstices laissés par les institutions qui prennent en charge les différents problèmes de la

jeunesse. Une analyse des actions de la police à l'école révèle que les agents fonctionnent simultanément comme des agents de sécurité, éducateurs sur les risques, opérateurs des systèmes d'information, conseillers, et qu'ils mobilisent les employés des écoles comme les jeunes pour remplir également cette diversité de rôles. L'implication de la police dans la gouvernance des groupes raciaux et ethniques est également examinée. En réponse aux demandes pressantes d'autres institutions, la police utilise des classifications raciales et ethniques pour comprendre les problèmes et définir le profil des populations à risque. Les unités multiculturelles de la police sélectionnent ceux qui vont se ranger dans la catégorie « autre » (c'est-à-dire autre que « blanc ») afin de mieux cerner les problèmes qui sont les leurs et qu'ils peuvent poser. Ces unités s'engagent également dans une intense mise en réseau inter-institutionnelle afin de développer la connaissance des problèmes spécifiques liés aux groupes raciaux ou ethniques.

La cinquième partie du livre porte sur la manière dont, en interne, la police perçoit et gère la question de la communication sur les risques. Cette partie constitue une analyse des évolutions de la profession du fait que la société du risque est aussi une société de la connaissance. Les policiers sont des « travailleurs du savoir » qui de même que d'autres institutions majeures, croient qu'il est possible de bâtir un monde plus sûr par une connaissance

de plus en plus parfaite des risques. Cette croyance les pousse à chercher toujours ce qui pourrait les amener à un plus haut niveau de perfection. Le problème est qu'ils sont constamment confrontés à l'imperfection des règles qu'ils se donnent, d'où à la fois le développement d'un sentiment d'échec et d'un espoir. Ils espèrent que les prochaines procédures seront plus efficaces. En même temps, ils sont confrontés à de nouvelles demandes de la part d'autres institutions car ces institutions sont exactement dans la même position en ce qui concerne la connaissance nécessaire au *management du risque*.

La société du risque se caractérise par le raffinement perpétuel des règles présidant à la circulation de la connaissance. Aussi la police est-elle de plus en plus soumise à de fortes pressions extérieures pour produire et distribuer de la connaissance sur les innovations en la matière. Par exemple, le droit pénal définit les conditions et critères de divulgation du renseignement, de même qu'un ensemble important de dispositions légales concernant le respect de la vie privée et l'accès à l'information. La nécessité d'être publiquement responsable conduit également la police à élaborer en interne des règles concernant la communication en matière de gestion des risques. Des règles sont mises en place pour centraliser l'accès d'autres institutions aux données policières, pour faciliter l'échange ou la vente à des agences extérieures et pour réguler les systèmes

de production et de distribution de ces informations en interne. Ces dispositifs protègent les organisations policières d'une image d'irresponsabilité dans la gestion de leur savoir technique.

Le savoir pratique conçu, reconnu, et présenté dans un rapport de police dépend du cadre d'interprétation dans lequel il s'inscrit, et reste toujours secondaire par rapport à ce cadre. Les cadres d'interprétation contraignent la manière dont les policiers agissent et gèrent les actions qu'ils entreprennent. Des interprétations alternatives tendent alors à paraître comme irréalistes, voir à disparaître complètement. De ce point de vue, les cadres dans lesquels est pensée la communication sur les risques sont au centre de la manière dont les institutions définissent et sélectionnent les risques. Connaître une institution, c'est connaître les cadres de communication qu'elle utilise pour définir et sélectionner les risques.

Des ressources considérables ont été consacrées par la police à la régulation des cadres d'interprétation. Cette dernière est nécessaire car elle est le seul moyen qui puisse garantir que les classifications utilisées sont adaptées à la production d'une connaissance adéquate sur le risque. Nous analysons ici la manière dont cette régulation s'opère au niveau des cadres créés par les agents à des fins pratiques, au niveau local, et qui n'ont pas fait l'objet d'une sanction par l'administration centrale de la police. Notre analyse d'environ soixante années de travail policier nous conduit à montrer que l'on est passé

d'un monde de la page blanche laissant toute latitude narrative, à un système de classification fixé qui satisfait aux exigences des institutions demandeuses. À la fin des années quatre-vingt-dix, le contrôle des comptes rendus se traduit par la limitation des rapports écrits. Il s'agit tout au plus de remplir des cases prédéfinies, ce qui ne laisse plus aucune place à un langage interprétatif et abstrait. Le compte rendu est ensuite transformé en données chiffrées au moyen d'un scanner.

L'introduction de l'informatique a eu une influence significative sur les cadres d'interprétation des situations. Les agents de police font plus souvent leur ronde avec un clavier d'ordinateur qu'avec le bâton. Dans certains cas, ce recours à l'informatique sert des nécessités internes. Par exemple, la présence d'ordinateurs dans les véhicules de police contribue à accélérer les contrôles d'identité sur la voie publique, ce qui permet à la police de détecter un plus grand nombre d'individus en situation irrégulière. Dans d'autres, cela sert en externe, par exemple, lorsque la police harmonise la structure de ses bases de données avec d'autres institutions afin d'accroître l'efficacité de la communication sur les risques en direction de ces institutions.

À chaque coup frappé sur le clavier, l'agent au travail se voit également catégorisé en fonction de la qualité et de la quantité de savoir qu'il produit. L'ordinateur contribue donc aussi à mettre en place une discipline de travail, qui permet de se passer d'un

contrôle hiérarchique direct omniprésent. L'ordinateur du véhicule de patrouille est un moyen de surveillance et de contrôle des activités policières. Il mesure de manière routinière tout ce qui se fait et permet de classer finement les agents en fonction de leurs performances et donc de leurs perspectives de carrière.

Malgré les mesures prises pour réduire la paperasserie, celle-ci ne fait que croître du fait de la demande de données par d'autres institutions. Si la demande est croissante, cela n'est pas seulement lié au besoin d'en savoir toujours plus sur le risque, mais aussi au simple fait que l'ordinateur offre la possibilité de faire circuler de l'information, de mettre au point de nouvelles classifications et de faciliter la tâche lorsque l'on veut modifier les protocoles pour les adapter à de nouvelles classifications. La demande externe pour plus de savoir sur le risque et la facilitation technologique viennent nourrir la tendance compulsive de la police à produire des données. Ce qui au départ apparaissait comme une innovation technologique intéressante en termes d'organisation du travail est devenu au cours du temps une contrainte de plus, tant pour les officiers que pour les hommes du rang.

La technologie informatique altère les structures hiérarchiques de commandement et de contrôle. Les rôles remplis par les uns et les autres sont plus troubles et nivelés, si bien qu'il n'est plus possible de dire clairement qui prend la décision. La prise de déci-

sion se fait dans un cadre prédéfini, qui a ses propres autonomie et réalité au niveau du système. Cela dit, l'ambiguïté des rôles et l'altération de la hiérarchie ne renforcent pas l'autonomie des hommes du rang. Au contraire, celle-ci est circonscrite et fragmentée dans un système de surveillance des risques qui porte à la fois sur les citoyens et sur les policiers eux-mêmes.

Notre modèle ouvre de nouveaux horizons pour l'analyse du travail policier et des mécanismes constitutifs de la société. En même temps qu'elle éclaire de nombreux aspects qui demeureraient jusqu'à présent dans l'ombre, cette perspective permet de souligner les limites des approches précédentes et d'ouvrir de nouveaux champs de recherche pour une exploration empirique et des discussions théoriques. Le risque est un des traits dominants de la modernité, et il est nécessaire de s'y arrêter en détail et de la manière la plus large possible. Les institutions gestionnaires du risque et leurs systèmes de communication ont désormais une emprise importante sur la société, et notre recherche empirique sur la participation de la police à cet univers vient confirmer cette idée.

Il est curieux que les chercheurs soient restés inattentifs ou insensibles à ce que nous analysons ici. D'après nous, ils restent par trop familiers de cadres d'interprétation proches du sens commun policier. Ils ont accepté sans discussion l'idée communément admise selon laquelle la police est toujours organisée selon un modèle militaire

dans le but de protéger les personnes et la propriété dans des limites territoriales bien définies, et que cette protection s'effectue à travers de stratégies et de tactiques d'application de la loi, de maintien de l'ordre et de fourniture de prestations. D'après eux, les policiers sont en tout premier lieu chargés du respect de la loi, ce qui leur procure toute l'autorité institutionnelle et coercitive nécessaire pour maintenir l'ordre.

Les policiers voient leur métier de la même manière. Mais, ils ne peuvent nier qu'ils sont particulièrement investis dans la question de la gestion des risques, dans la mesure où cet aspect des choses est omniprésent dans leur travail et que par ailleurs, ils rationalisent cette activité comme un moyen à la disposition de la réponse judiciaire et du maintien de l'ordre. Lorsqu'il arrive qu'ils ne peuvent rationaliser ainsi leurs activités de communication sur les risques, ils les considèrent comme un processus indépendant et s'en détachent dès lors.

Si la mise en œuvre du droit, le maintien de l'ordre et la fourniture de prestations diverses font évidemment partie du travail policier, ils ne rendent pas compte de manière adéquate de la manière dont la police contribue effectivement à la régulation, à la gouvernance et à la sécurité. La police est impliquée dans de nombreuses régulations légales qui vont bien au-delà de la mise en œuvre de la réponse judiciaire. Par exemple, du point de vue de la prévention et de la régulation des cam-

briolages, les textes juridiques sur les contrats d'assurance, et les informations fournies par la police aux compagnies sur les risques encourus, sont bien plus significatifs que la stricte application du droit pénal. La police est également largement impliquée dans la fourniture d'informations sur les risques à d'autres institutions, à propos de dangers qui ne relèvent ni du pénal, ni du maintien de l'ordre. Leur contribution se définit plutôt en terme de systèmes inter-institutionnels de communication sur les risques.

La police du risque s'est développée parallèlement à l'augmentation de la population carcérale, à des niveaux jamais atteints auparavant dans certaines juridictions. D'après certains, cet indicateur prouverait qu'une répression accrue aurait pris le pas sur des méthodes plus douces et plus subtiles de gestion des risques. De notre point de vue, les deux ne sont pas exclusifs ni ne se concurrencent. Il est erroné d'instituer un dualisme simpliste entre pouvoir coercitif/disciplinaire et gestion des risques comme si la complexité des phénomènes impliqués pouvait se réduire à une simple opposition binaire.

Le fait que le travail policier soit de plus en plus pris dans une logique de gestion des risques n'est pas contradictoire ou antithétique avec des fluctuations dans les degrés de répression. Il s'organise lui-même autour de la notion de gestion des risques. De fait, la justice a une longue expérience en matière d'invention de techniques « probabilistes » en matière de dangerosité, de

mise en liberté sous caution, de remise de peine, etc. Un accroissement de la répression indique que les seuils de tolérance ont été abaissés et que de nouvelles techniques de réduction des risques ont été introduites. D'un autre côté, si le système pénal n'avait pas en priorité mis l'accent sur les technologies de gestion des risques qui permettent de tenir la plupart des gens en marges ou même de ne pas traiter leur cas, le niveau de répression serait beaucoup plus élevé. La justice s'efforce la plupart du temps de se décharger de divers cas sur d'autres juridictions. Sans cet effort, et la collaboration de la police en ce sens, une bonne partie de la population serait tout simplement en prison. La police communautaire serait remplacée par la prison communautaire.

De la même façon que le discours sur les risques se diffuse dans toutes les institutions, le discours sur une répression accrue n'est pas propre à la sphère judiciaire. Les médias de masse et les élus en particulier joignent leurs efforts pour suggérer que la vie sociale serait d'autant plus facilitée si la répression pouvait être plus dure et plus rapide. La faveur pour une répression accrue, telle qu'elle s'exprime là, contribue certainement à la recherche de nouveaux moyens de contrôle des risques. Pourtant, de tels sentiments sont aussi très éloignés de la gestion routinière des risques liés aux crimes. Cette gestion est fondée sur un calcul utilitariste de minimisation des pertes et d'indemnisation, qui se traduit par la redistribution de la responsabilité de certains risques vers

d'autres institutions dont les seuils de tolérance sont plus lâches.

Comme nous l'avons suggéré *supra* à propos de la longue tradition d'invention de moyens de gestion des risques dans le secteur de la justice, la police des risques n'est pas quelque chose d'absolument nouveau. Bien souvent, ce qui est présenté comme de « nouveaux risques » renvoie à des risques anciennement connus mais assortis de nouveaux labels. En fait, ce type de police remonte à la fin du XVII<sup>e</sup> siècle, début XVIII<sup>e</sup> siècle. Le mode de gouvernement propre aux débuts de la période moderne a mis l'accent sur la surveillance des populations comme un moyen de développer la connaissance statistique et dans le but d'améliorer le fonctionnement social en matière d'utilité sociale, de santé et de bonheur. Cet aspect fut particulièrement frappant dans certaines organisations policières, telle la police montée du nord-ouest qui lui a succédé, la Police montée royale canadienne. Dispersées dans des zones immenses et peu peuplées, elles devaient assumer toutes les tâches afférentes au gouvernement de ces populations. Pourtant, même dans les zones urbaines à forte population, la police fut amenée à prendre en charge la gestion des risques dans un sens large : d'autres institutions la sollicitaient pour obtenir de l'information et mettre au point leurs propres politiques de sécurité.

Malgré ces aspects historiques, il existe des dimensions radicalement nouvelles dans la société contemporaine

qui justifient qu'on la caractérise comme étant conduite par les demandes institutionnelles de connaissance des risques. De nouveaux besoins émergent tels que les risques sanitaires liés au sida. Les populations sont de plus en plus mobiles, ce qui contribue à de nouvelles demandes en matière de suivi et de surveillance. L'explosion des connaissances scientifiques et technologiques a contribué à une transformation structurelle des conditions sociales. En effet, la science et les technologies n'ont pas seulement contribué à réduire les risques, elles en ont généré de nouveaux. En retour, les ripostes élaborées pour répondre à ces nouveaux risques font appel à des technologies de plus en plus sophistiquées qui elles-mêmes génèrent de nouveaux risques, par un effet amplifié de spirale.

L'émergence de l'ordinateur est un changement technologique d'une signification particulière. L'ordinateur permet le développement de nouveaux cadres d'analyse des risques, en même temps qu'il autorise une diffusion immédiate de l'information vers les institutions intéressées. En scannant une carte de crédit, une carte de bibliothèque, de santé, un passeport, etc., on peut collecter localement une information qui est intégrée immédiatement dans les bases de données institutionnelles. La connaissance devient systémique, opérant plus aux niveaux collectif et institutionnel qu'à un niveau individuel.

Nous ne prétendons pas que la société du risque est déterministe. Les règles, les cadres d'interprétation et les

technologies des systèmes de communication sur les risques sont des créations humaines visant des objectifs de gestion spécifiques. Ils sont programmables. Il faut donc se poser la question de savoir quel type d'organisation cherche à mettre au point et à utiliser des modes de gestion des risques. De ce point de vue, les systèmes de communication en matière de risques sont plutôt déterminants que déterministes. On les utilise dans le cadre de schémas culturels d'interprétation spécifiques et ils s'organisent autour de visions données de l'organisation sociale, si

bien que leur influence doit toujours être ramenée à ces cadres et à ces visions.

Pour parler comme Foucault, notre étude est une archéologie et une généalogie des modes de gestion des sociétés du risque. Nous nous abstenons de poser la question de l'efficacité, laquelle fonde la logique utilitaire de notre société. Nous nous contentons d'une analyse des infrastructures et des pratiques policières en matière de production et de diffusion du savoir sur les risques.

## Le travail policier : informer sur les risques (Partie I, chap.1)

Dans ce livre, on entend montrer comment la police est organisée autour d'un impératif de communication sur les risques, en collectant de l'information comme en la distribuant auprès d'autres institutions comme les compagnies d'assurance, les diverses agences de contrôle, les institutions financières, les services de santé et de protection sociale, les services des cartes grises, etc.

Le travail décrit ici ne consiste pas seulement à répondre à des demandes individuelles mais aussi à des demandes institutionnelles de connaissance sur les risques. La police est prise dans un réseau inter-institutionnel au sein duquel les champs de compétence se définissent par rapport à la revendica-

tion d'une expertise sur tel ou tel type de risque et par rapport au besoin exprimé par les institutions de maîtriser ces risques.

La notion de risque, nous l'avons dit, renvoie aux dangers extérieurs, comme les catastrophes naturelles et les menaces agressives de la part d'ennemis<sup>1</sup>. Il faut encore mentionner un certain nombre de risques produits par la technique, comme ceux résultant d'interventions scientifiques et technologiques sur la nature et la vie sociale<sup>2</sup>. C'est-à-dire en voulant maîtriser par des moyens techniques et scientifiques les dangers extérieurs auxquels nous sommes confrontés, les humains produisent de nouveaux dangers pour leur

•••(1) DOUGLAS (M.), 1990, «Risk as a Forensic Resource», *Daedalus*, n°119, p. 1-16 ; DOUGLAS (M.), 1992, *Risk and Blame. Essays in Cultural Theory*, London, Routledge.

(2) GIDDENS (A.), 1994, *Beyond Left and Right. The Future of Radical Politics*, Cambridge, Polity.



environnement et leurs vies. La pollution en est un bon exemple<sup>3</sup>. La notion de risque se réfère également aux méthodes utilisées pour gérer les menaces et les dangers. Nous insistons particulièrement sur les règles, les cadres d'interprétation et les technologies développés par les institutions pour gérer les dangers qu'elles identifient, mais aussi sur les raisons qui amènent la police à se transformer en prestataire de services pour ces institutions en mal d'information.

Nous faisons l'hypothèse que les logiques à l'œuvre dans l'évaluation des risques et les besoins d'information qu'elles génèrent de la part de ces institutions influencent fondamentalement la police. Les schémas de perception par lesquels les policiers pensent et agissent ne sont pas seulement le produit de règles légales formelles et administratives, ni de règles informelles liées à la culture professionnelle, mais aussi des manières dont les institutions externes conçoivent et gèrent les risques. En d'autres termes, c'est la structure de la communication institutionnelle qui, plus que les règles légales, administratives ou informelles, détermine les marges de manœuvre des policiers. Les règles légales et administratives ne sont pas sans rapport avec les classifications des risques, mais ce sont ces classifications qui, en retour, modèlent et déterminent l'autonomie de la police. Plus encore, l'autonomie de l'institution policière est elle-

même circonscrite par les règles imposées de l'extérieur en matière de circulation de l'information sur les risques.

Il nous semble également que le rôle d'informateur sur les risques auprès des institutions extérieures que remplit la police change la manière dont elle assure la sécurité des individus, des organisations et des institutions. Alors que la police traditionnelle se focalise sur la déviance et le contrôle, dans la société du risque, les priorités se déplacent vers le risque, la surveillance et la sécurité. Il s'agit moins dès lors de pointer l'existence de déviants et de les placer en marge de la société que de développer une capacité à tracer les profils potentiellement à risque afin de bien gérer les places auxquelles ils sont assignés dans les institutions. La préoccupation est moins de contrôler les déviants au moyen de la répression que de mettre en place un réseau de surveillance permettant de construire des catégories d'individus, d'organisations et d'institutions en fonction des risques spécifiques les concernant. Même si l'on met toujours l'accent sur le maintien de l'ordre social, au sein d'un environnement spatial prévisible, il existe en même temps une pléthore de mécanismes devant permettre de garantir la bonne santé et la productivité des « ressources humaines et organisationnelles », et donc d'offrir de la sécurité.

La réorientation vers le risque, la surveillance et la sécurité sont stimulées

•••(3) DOUGLAS (M.), WILDAVSKY (A.), 1982, *Risk and Culture : An Essay on the Selection of Technical and Environmental Dangers*, Berkeley, University of California Press.

par une modification du régime légal propre à la société du risque. Au fur et à mesure que l'accent mis sur la répression perd de sa vigueur, les institutions judiciaires passent d'un modèle répressif/dissuasif à un modèle négocié de respect de la loi<sup>4</sup>. La priorité est alors donnée à tout ce qui permet d'élaborer des niveaux acceptables de risque. On s'intéresse donc moins au contrôle du crime qu'à la mise en place d'une société de surveillance, pensée comme une fin en soi. Cela signifie aussi que les protections légales pour les suspects sont relativement supplantées par « les droits du système » à améliorer la surveillance de la société. Dans le même temps, la police fournit des renseignements sur des risques qui n'ont rien à voir avec les comportements criminels. Par exemple, afin de renforcer la confiance et les droits statutaires, les risques sont de plus en plus « légalisés » à travers des contrats, des licences, des garanties « zéro défaut », et le recours aux indemnisations pour dommages civils. Toutes ces méthodes légales d'interprétation et de renforcement des pratiques sociales du risque affectent le volume, la direction et la nature du travail policier en matière de communication sur les risques. Cela nous renvoie à la nécessité d'analyser le travail policier au regard des théories du pluralisme légal.

Finalement, il nous semble que les changements dans le travail policier

soulignés ici s'articulent en partie au discours sur la police de proximité. La police de proximité se comprend mieux si on la pense comme un moyen au service de la communication institutionnelle sur les questions du risque et de la sécurité et si l'on comprend que ce modèle sert à rationaliser la modification du rôle tenu par les organisations policières dans la société du risque. (...)

#### LES POLICIERS, TRAVAILLEURS DU SAVOIR

##### REQUÊTES INSTITUTIONNELLES

Le fait que la police soit avant tout une instance de production de savoir nous conduit à nous interroger sur ceux qui réclament une telle production. Dans la recherche existante, la réponse est que la police produit du savoir à ses seules fins internes de *management*. L'observation de Wilson selon laquelle les systèmes de comptes rendus propres aux organisations policières ne sont pas faits « *pour s'assurer de ce que les problèmes enregistrés seront résolus (bien souvent cela n'est pas possible) mais de protéger le service contre l'accusation de n'avoir rien fait* »<sup>5</sup> a été reprise par nombre de chercheurs. Ceux-ci se sont focalisés sur la manière dont les policiers qui en sont chargés remplissent leurs papiers en cherchant toujours à couvrir leurs arrières vis-à-vis de la hiérarchie.<sup>6</sup>

••••(4) REISS (A.), 1984a, « Consequences of Compliance and Deterrence Models of Law Enforcement for the Exercise of Police Discretion », *Law and Contemporary Problems*, n° 47, p. 83-122.

(5) WILSON (J.), 1968, *Varieties of Police Behavior*, Cambridge, Harvard University Press, p. 90.

Lorsque les recherches vont au-delà de ces effets de censure introduits à ce niveau de base de la décision, elles en restent malgré tout à un niveau d'analyse uniquement centré sur l'institution policière et ne s'intéressent qu'aux flux d'informations en interne<sup>7</sup>. Le savoir produit est rarement compris comme ayant une importance qui va au-delà de l'institution policière elle-même.

Dans cette vision policière du travail de collection de l'information, la possibilité d'un environnement de communication en dehors de l'institution policière n'est même pas imaginée. Parmi les quelques rares chercheurs qui ont pris en compte cet univers de communication, l'accent est plutôt mis sur la production de savoirs utiles au système pénal. Ce qui indique que les chercheurs ont admis l'idée commune selon laquelle le travail policier est largement centré sur la criminalité<sup>8</sup>. Le polycentrisme de l'analyse a même conduit certains chercheurs à conclure que la production de savoir policier et sa distribution répondaient uniquement à des critères policiers et ne servait qu'à

des buts propres à l'institution. C'est ainsi que Chatterton fait cette extraordinaire remarque selon laquelle «*la police n'est pas soumise à la demande d'information. Au contraire, elle est parvenue à faire de l'information sa propriété. Elle en est venue à l'interpréter en fonction de ses propres intérêts et au travers du filtre de ses propres préjugés culturels et typifications. L'information est plus utilisée pour remplir que pour définir des objectifs*»<sup>9</sup>.

Certains chercheurs ont reconnu le fait que la police est prise dans un champ complexe d'institutions et que le travail policier renvoie aussi à la gestion des relations avec l'ensemble de ces institutions. Pourtant, ils ont surtout mis l'accent sur la manière dont la police s'organise pour obtenir de l'information auprès d'autres institutions.<sup>10</sup> L'accès à l'information est restreint par les droits de la propriété et par le devoir de l'État de protéger la vie privée, ce qui limite doublement la possibilité pour la police de lutter contre le crime.<sup>11</sup> Certains analystes se sont

•••(6) MANNING (P.), 1980, *The Narc's Game : Organizational and Informational Limits on Drug Law Enforcement*, Cambridge, MIT Press ; ERICSON (R.), 1982, *Reproducing Order : A Study of Police Patrol Work*, Toronto, University of Toronto Press ; CHATTERTON (M.), 1991, « Organizational Constraints on the Uses of Information Technology in Problem-Focused Area Policing », Paper Presented to the British Criminology Conference, July.

(7) MANNING (P.), 1988, *Symbolic Communication : Signifying Calls and the Police Response*, Cambridge, MIT Press ; CHATTERTON (M.), 1989, « Managing Paperwork », in WEATHERITT (M.), (ed), *Police Research : Some Future Prospects*, p. 107-136, Aldershot, Gower ; SOUTHGATE (P.), MIRLESS BLACK (C.), 1991, *Traffic Policing in Changing Times*, London, HMSO.

(8) ERICSON (R.), 1982, *op. cit.* ; ERICSON (R.), 1993, *Making Crime : A Study of Detective Work*, 2nd Edition, Toronto, University of Toronto Press ; MCCONVILLE (M.), SANDERS (A.), LENG (R.), 1991, *The Case for the Prosecution : Police Suspects and the Construction of Criminality*, London, Routledge ; MANNING (P.), HAWKINS (K.), 1989, « Police Decision-Making », in WEATHERITT (M.) (ed), *Police Research : Some Future Prospects*, p. 139-156, Aldershot, Gower.

(9) CHATTERTON (M.), 1991, *op. cit.*, p. 8.

(10) MANNING (P.), 1980, *op. cit.*, p. 34 ; REISS (A.), 1983, « The Policing of Organizational Life », in PUNCH (M.) (ed.), *Control in the Police Organization*, p. 78-97, Cambridge, MIT Press. ; MARX (G.), 1988, *Undercover: Police Surveillance in America*, Berkeley, University of California Press ; HOOGENBOOM (B.), 1991, « Grey Policing: A Theoretical Framework », *Policing and Society*, n°2, p.17-30.

rendu compte que les capacités de la police à pénétrer d'autres institutions avaient changé au fur et à mesure que changeaient les technologies de communication et que se développait le processus de bureaucratisation. Comme le soulignent Meyer et Scott, « *l'environnement des organisations formelles est lui-même organisé de manière formelle à un degré étonnamment élevé* »<sup>12</sup>. Ce haut degré d'organisation autorise la police à acquérir des formes nouvelles et variées de connaissances au moyen des inspections, de la surveillance et des audits.<sup>13</sup>

Ce que les chercheurs n'ont pas réussi à analyser, ce sont les voies par lesquelles ces institutions extérieures sollicitent la police pour obtenir des informations utiles à leurs propres activités. Pour tous les types d'incidents qu'elle a à connaître, la police doit produire un savoir destiné à la fois à ses propres fins mais aussi pour satisfaire les demandes d'autres institutions en matière de *management* du risque. Ces demandes ont un impact profond sur la manière dont la police agit et pense. (...)

La police produit et distribue des comptes rendus d'événements formatés selon les besoins des diverses institutions qui pourraient y trouver un inté-

rêt. Si les policiers conservent un certain degré de latitude dans la manière dont ils établissent le compte rendu, cette marge de manœuvre est néanmoins sévèrement circonscrite par les impératifs liés aux schèmes classificatoires imposés par les institutions extérieures. (...)

Une institution consiste en un ensemble de relations, de processus et de manières de faire associées à un certain type d'intérêt. Elle incorpore des éléments matériels (par exemple des bâtiments et des technologies), des éléments culturels (par exemple, des traditions, des rituels et des technologies scientifiques et légales), des éléments politiques (comme le besoin de légitimation) et des éléments sociaux (lorsque tous ces éléments sont reproduits à travers une connaissance sociale et une activité routinière). Les institutions « *pensent de manière routinière à la place des individus* »<sup>14</sup> en contribuant à l'élaboration perpétuelle de classifications et de formats de communication tournés vers la production et la distribution de connaissances pour le *management* du risque. Ce savoir est utilisé pour réduire l'entropie, résoudre les problèmes et prendre les décisions de routine.

•••(11) STINCHCOMBE (A.), 1963, «Institutions of Privacy in the Determination of Police Administrative Practice», *American Journal of Sociology*, n°69, p. 150-160 ; SKOLNICK (J.), 1966, *Justice without Trial: Law Enforcement in Democratic Society*, New York, Wiley ; REISS (A.), 1971, *The Police and the Public*, New Haven, Yale University Press ; REISS (A.), BORDUA (D.), 1967, «Environment and Organization: A Perspective on the Police», in BORDUA (D.) (ed.), *The Police: Six Sociological Essays*, p. 25-55, New York, Wiley ; BLACK (D.), 1980, *Manners and Customs of the Police*, New York, Academic Press ; SHEARING (C.), STENNING (P.), 1983, «Private Security: Implications for Social Control», *Social Problems*, n°30, p. 493-506.

(12) MEYER (J.), SCOTT (R.), 1983, *Organizational Environments: Ritual and Rationality*, Beverly Hills, Sage, p. 15 ; voir aussi SCOTT (R.), 1991, «Unpacking Institutional Arguments», in POWELL (W.), DIMAGIO (D.) (ed.), *The New Institutionalism in Organizational Analysis*, p. 164-182, Chicago, University of Chicago Press, p. 171.

(13) REISS (A.), 1983, *op. cit.* ; MARX, 1988, *op. cit.*

(14) DOUGLAS (M.), 1986, *How Institutions Think*, Syracuse, Syracuse University Press, p. 47.

La centralité de l'évaluation et de la gestion du risque au sein d'organisations complexes vient témoigner du degré d'institutionnalisation du risque dans la société moderne.<sup>15</sup> Au fur et à mesure que de nouveaux besoins de gestion des risques apparaissent, les institutions développent de nouvelles manières de catégoriser, de classifier, de penser et d'agir qui requièrent la participation de la police. Ce processus n'est pas récent, comme le soulignent quelques spécialistes de la sphère pénale et du risque.<sup>16</sup> On pourrait même dire que ce processus est consubstantiel à l'existence d'une police, partie intégrante de la conception moderne du gouvernement. Dès lors que les institutions modernes ont commencé à mettre en place de nouveaux schèmes pour construire des catégories statistiques et des types de risques, la police a été sommée de contribuer autant qu'elle pouvait à la production de ce savoir et à sa diffusion.

Hacking observe que, avec le développement de la « science morale » après 1820 et l'avalanche de chiffres imprimés, la police fut sollicitée pour aider à la construction des profils de population criminelle pour le compte des institutions étatiques de santé, de protection sociale et de la justice. Hacking note par exemple, que dans la France du XIX<sup>e</sup> siècle,

*« On trouve une classification de plus de 4000 items pour les motifs de meurtres et des demandes faites à la police de classer les causes de suicide selon une typologie en 21 cases. Je ne pense pas que ces mobiles de crime et ces causes de suicide aient existé avant que l'on prenne l'habitude de les recenser... Chaque fait lié à un suicide devient fascinant. Les statisticiens composent des formulaires que docteurs et policiers doivent remplir, enregistrant tout, depuis l'heure de la mort aux objets trouvés dans les poches du cadavre. Les différentes manières de se donner la mort sont abruptement caractérisées et deviennent le symbole d'un caractère national. Les Français préfèrent le monoxyde de carbone et la noyade, les Anglais se pendent ou se suicident par balle. Les aspects les moins prémédités de l'action humaine se voient ainsi rationalisés ».*<sup>17</sup>

Ailleurs, Hacking décrit un tableau mis au point par le ministère français de la Justice en 1836 dans lequel les agents de la force publique doivent consigner, sur les lieux où le suicide a été découvert : *le sexe, l'âge et l'état de santé du mort ; sa profession et sa classe sociale, sa résidence, le lieu de sa naissance, son statut marital, le nombre de ses enfants, ses revenus (est-il « riche », « aisé », « pauvre » ou « misérable ») ; son éducation (« édu-*

•••(15) REISS (A.), 1989, «The Institutionalization of Risk», *Law and Policy*, n°11, p. 392-402, p. 392.

(16) FEELEY (M.), SIMON (J.), 1994, «Actuarial Justice: The Emerging New Criminal Law», in NELKEN (D.) (ed.), *The Futures of Criminology*, London, Sage, p. 173-201 ; GARLAND (D.), 1996, «The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society», *British Journal of Criminology*, London, Sage, p. 445-471.

(17) HACKING (I.), 1986, «Making up People», in HELLER (T.), et al. (ed.), *Reconstructing Individualism*, p. 222-36, Standord, Stanford University Press, p. 223, 235.

qué», «sachant lire et écrire», «illettré»); son état d'esprit, sa moralité («a-t-il été condamné ?», «était-il adultère ?», «joueur», «prostitué» ? , «concubin» ? «alcoolique» ?); sa religion. Ensuite, le tableau exige que soit enregistré le lieu de l'endroit où le corps a été découvert, les circonstances médicales, la date et l'heure, et le temps qu'il faisait. Comment cela s'est-il passé ? Pourquoi ? Le suicidé a-t-il laissé une lettre ? Y a-t-il eu des tentatives précédentes ? Y a-t-il des antécédents familiaux de cas de folie ou de suicide ? Quels objets ont été trouvés sur les lieux, ou dans les poches de la victime<sup>18</sup>

En même temps que la société s'institutionnalisait du fait de la bureaucratization et du développement de la technologie, la police développait son rôle d'agence d'information sur les risques. Pour reprendre l'expression mémorable employée par Hacking, la police, en collaboration avec tout un ensemble d'institutions présentes dans la société du risque, est une «dompteuse de probabilités». De ce point de vue, l'institution fonctionne comme une sorte d'assurance sociale. Une unité de police urbaine normale de la police montée du Canada a recours à des centaines de formulaires de comptes rendus d'opération, dont la plupart servent à faire circuler le savoir recueilli en matière de risques en direction des institutions extérieures. En 1992, la police royale

montée du Canada disposait, en raison de la superposition des niveaux municipaux, provinciaux et fédéraux et des besoins du secteur privé, d'environ 2100 formulaires de comptes rendus d'opération et d'environ 600 personnes affectées à plein temps à une division informatique spécialement dédiée au traitement des données ainsi recueillies. On le verra cette importance accordée à la production d'un savoir est largement le résultat de la demande extérieure en même temps que d'un souci, exprimé en interne, de fournir une connaissance présentable.

Ces myriades de demandes formulées auprès des services de police par des institutions externes suggèrent d'apporter un correctif à un autre lieu commun du monde de la recherche. Du fait de leur vision centrée sur la police et de l'accent mis sur la production et la distribution de connaissances à des fins de gestion interne, celui-ci a surtout insisté sur le secret et la «faible visibilité» du travail policier. À la suite de la formulation séminale de Goldstein<sup>19</sup>, il continue à soutenir que «la plupart des décisions prises par la police sont virtuellement invisibles ou de faible visibilité» et que «le goût du secret est dominant où l'information est rarement partagée»<sup>20</sup>. Au contraire, nous apportons la preuve que, dans un contexte de demandes formulées par des institutions extérieures, la police se livre à de multiples formes institution-

•••(18) Hacking (I.), 1990, *The Taming of Chance*, Cambridge, Cambridge University Press, p. 79.

(19) GOLDSTEIN (J.), 1960, «Police Discretion Not to Invoke the Criminal Process: Low Visibility Decisions in the Administration of Justice», *Yale Law Journal*, 69, p. 543-594.

nalisées de mise en publicité qui, au final, font de son activité quelque chose de hautement visible. En tant que fournisseur d'informations sur les risques en direction de publics multiples, la police ne se contente pas de distribuer du savoir de manière élargie ; elle rend en même temps ses propres actions fortement visibles par la production même de ce savoir. De la même façon que dans d'autres secteurs professionnels tournés d'abord vers la production de savoir, le policier, par le seul fait qu'il produit et distribue une l'information nécessaire à l'accomplissement de son travail, produit aussi un savoir sur ses pratiques professionnelles.<sup>21</sup> (...)

Au même titre que les autres professions qui produisent des connaissances en matière de gestion des risques auxquels elles ont à faire face, le métier policier est à la fois l'objet d'une intensive activité « informationnelle » (soit le fait de traduire des événements et des objectifs en information utilisable dans des cadres préformés) et d'une « automatisation » ou d'une « fordisation » (appropriation par la machine de compétences et de travail humains)<sup>22</sup>. À nouveau, le but poursuivi renvoie à une

simplification des choix face à un kaléidoscope d'interprétations possibles et de scénarios disponibles, en bref, une forme de taylorisation.

La gestion des fonctionnaires de police est de plus en plus perçue comme un problème de communication et de technologie. Inspirés par des syndicats progressistes, les gestionnaires adoptent des techniques de profilage des risques importées de la « gestion des ressources humaines » pour « construire » leur population de fonctionnaires. Ces techniques sont similaires par leur logique et leurs formes aux techniques de définition des risques mises en œuvre par les fonctionnaires eux-mêmes dans leur travail routinier de labellisation des populations qu'ils ont à gérer. Travaillant pour « l'entreprise police », les agents doivent réaliser un travail mental fondé sur la manipulation de symboles<sup>23</sup> qui, en retour, les symbolisent de manière réflexive comme automates.

Il y a toutes les chances que les policiers se sentent spécialement dépossédés de leur travail mental dans la mesure où ils savent très peu à quoi sert ce travail et quelles en sont les conséquences. Ils peuvent se sentir restreints

•••(20) MANNING (P.), 1992a, « Information Technology and the Police », in TONRY (M.), MORRIS (N.) (eds), *Modern Policing*, 349-98, Chicago, University of Chicago Press, p. 357 et 370 ; voir aussi GELLER (W.), MORRIS (N.), 1992, « Relations between Federal and Local Police », in TONRY (M.), MORRIS (N.), (ed.), *Modern Policing*, p. 231-348, Chicago, University of Chicago Press ; CHATTERTON (M.), 1983, « Police Work and Assault Charges », in PUNCH (M.), (ed.), *Control in the Police Organization*, p. 194-221, Cambridge, MIT Press ; CHATTERTON (M.), 1989, *op. cit.* ; REISS (A.), 1982, « Forecasting the Role of the Police and the Role of the Police in Social Forecasting », in DONELAN (R.), (ed.), *The Maintenance of Order in Society*, p. 132-156, Ottawa, Supply and Services Canada, p. 146.(21) ERICSON, SHEARING, 1986, « The Scientification of Police Work », in BÖHME (G.), STEHR (N.), (eds), *The Knowledge Society: The Growing Impact of Scientific Knowledge on Social Relations*, p. 129-159, Dordrecht, Reidel ; POSTER (M.), 1990, *The Mode of Information: Poststructuralism and Social Context*, Cambridge, Polity ; POSTER (M.), 1995, *The Second Media Age*, Cambridge, Polity ; STEHR (N.), 1994, *Knowledge Societies*, London, Sage.

(22) ZUBOFF (S.), 1988, *In the Age of the Smart Machine: The Future of Work and Power*, New York, Basic Books.

(23) POSTER (M.), 1990, *op. cit.*



dans leur liberté d'action dans la mesure où ils produisent du savoir dans le cadre de schémas rigides de communication, d'autant qu'ils savent rarement de manière claire à qui est destinée cette communication, où elle va, et comment elle est effectivement utilisée dans la gestion concrète des risques. Pour eux, tout se ramène à une expérience « boomerang ». Ils sont dans une position identique à celle des utilisateurs de cartes de crédit et des cartes magnétiques d'accès sans savoir que cela permet en même temps de le faire entrer dans des catégories statistiques utiles à des fins stratégiques et analytiques.<sup>24</sup> D'autre part, on peut soutenir que cela ferait peu de différences pour les officiers de police de disposer d'un tel savoir car il est malaisé d'accroître la motivation des employés dans le cadre d'une machine bureaucratique lourde. Comme le suggère Archer dans un autre contexte, « *avoir conscience des causes de l'inflation n'empêchera pas une réduction de notre niveau de vie* ». <sup>25</sup>

Même si le degré de liberté laissé aux policiers est sévèrement encadré, il n'en est pas pour autant réduit à néant. Il est possible de rester dans l'ignorance tout en étant par ailleurs le producteur d'une expertise. En prenant en charge les problèmes d'une personne,

par exemple, le policier peut retenir la manière dont celle-ci définit ses besoins et les traduire en termes institutionnels pour être satisfaits. En tant qu'agent de transmission des besoins, ce n'est pas la personne de l'agent de police qui compte aux yeux de « clients » ayant des « besoins »<sup>26</sup> mais sa fonction de médiation et d'interprétation au sein d'un système expert de production de connaissance. C'est pourquoi on peut dire que l'agent de police taylorisé ressemble au médecin taylorisé, un cadre relativement bien payé et hautement professionnalisé qui examine les causes des problèmes en ayant recours à un large spectre de réponses à long terme, au premier rang desquelles les activités de prévention du crime en rapport avec la pauvreté, le chômage, l'insuffisance d'éducation et de qualifications professionnelles, des problèmes de logement de santé et toutes les autres causes structurelles de la criminalité<sup>27</sup>.

Cette description du travail policier est bien entendu proche de la description que fait Weber du travail bureaucratique déshumanisé. Une division du travail complexe en matière de gestion des risques et de sécurité nécessite des experts strictement objectifs et neutres qui puissent remplir leur rôle de transmetteur de connaissance et de conseiller.<sup>28</sup> L'expert ne fait rien

- (24) GANDY (O.), 1993, *The Panoptic Sort: A Political Economy of Personal Information*, Boulder, Westview, p. 54.
- (25) ARCHER (M.), 1988, *Culture and Agency: The Place of Culture in Social Theory*, Cambridge, Cambridge University Press, p. 68.
- (26) BAUMAN (Z.), 1992a, « Life-World and Expertise: Social Production of Dependency », in STEHR (N.), ERICSON (R.), (ed.), *The Culture and Power of Knowledge: Inquiries into Contemporary Societies*, p. 81-106, Berlin and New York, Walter de Gruyter.
- (27) LEIGHTON (B.), 1991, « Visions of Community Policing: Rhetoric and Reality in Canada », *Canadian Journal of Criminology*, n°33, p. 494-495.
- (28) STEHR (N.), 1992, *Practical Knowledge: Applying the Social Sciences*, London, Sage ; STEHR (N.), 1994, *op. cit.*



d'autre que transmettre et appliquer des connaissances : « *une production automatisée, une communication médiatisée et l'échange économique offrent un monde au sein duquel personne n'entre en contact avec personne. De plus en plus, les actions coordonnées sont des actions subordonnées aux machines. Tout est de plus en plus automatisé. La rationalité revient à une subordination de toute activité humaine à la machine* ». <sup>29</sup>

Dans l'organisation policière automatisée et informée, il existe également des espaces de liberté entre le niveau individuel du policier sur le terrain et celui de ceux qui mettent au point les systèmes d'expertise. Les gestionnaires de la police font partie de cette « élite technicienne experte en classements, rangements et définitions de populations ». <sup>30</sup> Cette expertise s'étend également aux opérations de classement, de mise en ordre, de déplacement des données. <sup>31</sup>

Il n'est pas plus concevable de comprendre les systèmes experts du travail policier et leur impact sur les marges de manœuvre laissées à la police si on limite l'enquête à ce que les policiers font « dans la rue », que de comprendre la vente au détail par l'observation que

fait un serveur lorsqu'il sert ses clients. L'idée « *d'un employé de McDonald's délivrant toujours le même hamburger conçu en laboratoire et cuisiné par des ordinateurs* » est une image suffisamment claire pour illustrer à quel point les activités des employés de McDonald's sont construites par des systèmes experts. Même en médecine, le docteur est subordonné à des systèmes experts et à ceux qui les conçoivent. <sup>32</sup> Il n'est que l'un des maillons d'une chaîne d'expertise qui construit le dossier du patient ; du coup, il perd le contrôle de certains aspects aussi bien que du processus en cours. Qui plus est, le dossier contribue non seulement à constituer la biographie médicale du patient mais il fournit également des données qui viennent nourrir les stratégies de divers hôpitaux, compagnies d'assurance, agences d'éducation, etc. L'opérateur sur le terrain n'est plus qu'un simple auxiliaire d'un gestionnaire qu'il fournit en informations dérivées de ses diagnostics. Ces informations sont ensuite stockées et distribuées selon des canaux complètement déconnectés de ceux de la pratique professionnelle <sup>33</sup>. En retour, les schémas de planification stratégique de l'hôpital, de la compagnie d'assurance,

•••(29) COUCH (C.), 1984, *Constructing Civilization*, Greenwich, Conn., JAI Press, p. 369.

(30) REICHMAN (N.), 1986, « Managing Crime Risks: Towards an Insurance Based Model of Social Control », in SPITZER (S.), SCULL (A.), (eds), *Research in Law, Deviance and Social Control*, p. 151-172, Greenwich, Conn, JAI Press, p. 166.

(31) HACKING (I.), 1992, « Statistical Language, Statistical Truth and Statistical Reason: The Self-Authentication of a Style of Scientific Reasoning », in McMULLIN (E.), (ed.), *The Social Dimensions of Science*, p. 130-157, Notre Dame, University of Notre Dame Press, p. 140.

(32) LOVEKIN (D.), 1991, *Technique, Discourse and Consciousness: An Introduction to the Philosophy of Jacques Ellul*, Bethlehem, Pa., Lehigh University Press. p. 2., p. 143 ; BOAS (M.), CHAIN (S.), 1976, *Big Mac: The Unauthorized Story of Mc Donald's*, New York, New American Library.

(33) CASTEL, 1991, « From Dangerousness to Risk », in BURCHELL (G.), GORDON (C.), MILLER (P.), (ed.), *The Foucault Effect: Studies in Governmentality*, p. 281-296, Chicago, University of Chicago Press, p. 281.

etc. participent à la définition des cadres dans lesquels le docteur pense, agit et organise.

Plus le système abstrait de connaissance spécialisé est pris dans des technologies et des schémas préconstruits, plus il a tendance à vivre sa propre vie. En même temps qu'il fait perdre une qualification, il produit aussi des effets d'aliénation et de fragmentation sur la culture professionnelle et l'identité des individus. De fait, le contrôle local - c'est-à-dire les marges de manœuvre des

individus, l'autorité organisationnelle et l'autonomie de la culture professionnelle - est-il minoré à chaque fois que des compétences de terrain sont transférées au niveau du système abstrait.<sup>34</sup> La confiance se déplace également vers le système abstrait si bien que les nouvelles situations et les nouveaux problèmes sont traités à ce niveau. Ces changements ont en retour un impact profond sur les pratiques, les régimes légaux et les discours sur le travail policier.

## Le travail policier, le risque et la loi (Partie I, chap.2)

### RISQUE, SURVEILLANCE ET SÉCURITÉ

La sociologie est concernée de manière centrale par le problème de l'ordre. Ce souci implique une focalisation sur la question de la caractérisation des comportements déviants et de la compréhension de ses mécanismes. La déviance est définie comme un écart à la norme, qui englobe non seulement les formes sérieuses de comportement anormal, telles que les actes criminels mais également les violations des procédures d'organisation et des comportements habituels. Traditionnellement les désignations de la déviance comportent un élément moral fort : la déviance est mau-

vaise, nuisible et constitue une violation de l'ordre moral.

#### *De la déviance au risque*

En ce qui concerne la déviance, la notion de risque renvoie à la nécessité d'identifier à la fois le problème et le procédé employé. Elle pointe la déviance comme danger. De telles désignations sont souvent profondément morales<sup>35</sup>. Le risque offre également des procédures ou des techniques - moyens de classification, calculs de probabilité, formats de communication - pour traiter de divers dangers. Il est une invention fondée sur des craintes imagi-

•••(34) GIDDENS (A.), 1991, *Modernity and Self-Identity: Self and Society in the Late Modern Age*, Stanford, Stanford University Press.

(35) DOUGLAS (M.), 1990, *op. cit.* ; DOUGLAS (M.), 1992, *Risk and Blame: Essays in Cultural Theory*, London, Routledge, 1992.

naires et sur des technologies inventives destinées à les traiter. En effet, le concept de risque est construit autour de techniques d'assurance. Il transforme les personnes, les organisations auxquelles elles appartiennent, leurs environnements, en d'innombrables catégories afin de les rendre plus maniables. Il les redistribue selon ses propres normes internes de référence plutôt qu'en fonction de normes extrinsèques.

La notion de risque n'évite pas la moralité ; au contraire, elle change fondamentalement les fondements de la moralité. elle défend une moralité utilitaire. Les gens, les organismes, et les environnements sont classés dans des catégories qui correspondent aux buts pratiques de l'organisme qui souhaite les rendre prévisibles. Les possibilités de catégorisation sont illimitées et le processus «de classement panoptique»<sup>36</sup> est sans fin. Les individus, les organismes, etc. sont distingués les uns des autres en fonction de leur plus ou moins grande efficacité, de leur plus ou moins grande utilité, de leur force, et ainsi de suite plutôt qu'en fonction de leurs qualités ou défauts moraux.

En tant que telle, la société du risque est également une « société de transmission »<sup>37</sup>. Elle départage l'importance des contributions à la société en évaluant des qualifications, des handicaps personnels, la solvabilité, la productivité, etc.<sup>38</sup> Certaines per-

sonnes sont autorisées à prendre l'autoroute, d'autres reléguées à des routes secondaires, et d'autres encore à des chemins vicinaux parsemés de dos d'ânes. La justice devient dès lors le maître du jeu dans la juste distribution des risques.

La police vient en aide aux diverses institutions en charge du risque en régulant la circulation au sein de la société de transmission. Elle réalise ce travail au moyen de formulaires composés pour les besoins d'autres établissements. Elle aide également ces institutions en leur adressant les individus et en fournissant des services, y compris en délivrant des avis experts sur le développement social et en fournissant des moyens de gestion des risques. En même temps, la police compte sur ces établissements pour recevoir en retour une connaissance utile à l'établissement de son propre panoptisme.

Cette culture des risques affecte la sensibilité morale vis-à-vis de la déviance. Condamnée parce que mauvais comportement moral, la déviance est traitée comme un « accident normal »<sup>39</sup>. Elle est ramenée à une simple éventualité pour laquelle il existe des moyens de gestion devant garantir sa non répétition. La déviance devient dès lors un problème technique qui exige une solution administrative, et n'est plus l'occasion d'exprimer des sentiments collectifs et une solidarité morale. Comme

•••(36) GANDY (O.), 1993, *op. cit.*

(37) CASTEL (R.), 1991, *op. cit.*

(38) GANDY, 1993, *op. cit.* ; NOCK (S.), 1993, *The Costs of Privacy: Surveillance and Reputation in America*, New York, Aldine de Gruyter.

(39) PERROW (C.), 1984, *Normal Accidents: Living with High-Risk Technologies*, New York, Basic Books.

l'écrit Garland lorsqu'il traite de la déviance criminelle, « *la menace du crime fait maintenant partie intégrante de la conscience moderne, elle n'est rien d'autre qu'un risque journalier à évaluer et contrôler plus ou moins dans les mêmes termes que le contrôle de la circulation. Un autre danger lié à la modernité qui se serait progressivement « routinisé » et « normalisé » avec le temps... l'habitude dans la société moderne de connaître des taux élevés de criminalité a induit une série de transformations des perceptions officielles du crime, à la fois dans le discours criminologique, dans les modes d'action gouvernementaux, et dans la structuration des modes de réponse judiciaire* ». <sup>40</sup>

L'appréciation morale du mal faire, tout comme les sentiments collectifs qu'elle suscite, se développe de telle ou telle façon dans les cultures politiques en fonction des logiques variables des médias de masse. Comme dans le passé, la culture publique contribue à la dramatisation de certains crimes, valorise des formes données de moralité, ces formes se fixant durablement dans la mémoire des individus. Du coup, ces

valeurs morales ont toutes les chances de s'éloigner de plus en plus, au cours du temps, de celles qui sont au principe des institutions officielles <sup>41</sup>.

#### DU CONTRÔLE À LA SURVEILLANCE

Dans la société du risque, le maintien de l'ordre ne renvoie pas seulement à des mesures répressives, punitives et préventives devant s'exercer sur ceux qui ont moralement tort. Le maintien de l'ordre consiste également à instaurer une surveillance, à produire de la connaissance sur les populations <sup>42</sup>. L'accent est mis sur la connaissance permettant de choisir des seuils définissant des risques acceptables et sur des formes d'inclusion et d'exclusion à partir de cette connaissance.

L'accent mis sur la surveillance réoriente la loi, la police, et les institutions de gestion du risque dans le but d'inventer continuellement de nouvelles manières d'accéder à la connaissance et de la distribuer. La tâche principale de la police est de changer le système d'informations pertinentes susceptibles d'être par la suite distribuées aux institutions intéressées et classées par elles. <sup>43</sup> Le pouvoir coercitif se divi-

••••(40) GARLAND (D.), 1996, *op. cit.*

(41) ERICSON, BARANEK, CHAN, 1987, *Visualizing Deviance: A Study of News Organization*, Toronto, University of Toronto Press, Milton Keynes, Open University Press ; ERICSON, BARANEK, CHAN, 1989, *Negotiating Control: A Study of News Sources*, Toronto, University of Toronto Press, Milton Keynes: Open University Press.

ERICSON, BARANEK, CHAN, 1991, *Representing Order: Crime, Law and Justice in the News Media*, Toronto, University of Toronto Press, Milton Keynes, Open University Press ; KATZ (J.), 1987, « What Makes Crime, News? », *Media, Culture and Society*, n°9, p.47-75 ; SCHLESINGER (P.), TUMBER (H.), 1994, *Reporting Crime: The Media Politics of Criminal Justice*, Oxford, Oxford University Press ; SPARKS (R.), 1992, *Television and the Drama of Crime: Moral Tales and the Place of Crime in Public Life*, Milton Keynes, Open University Press.

(42) DANDEKER (C.), 1990, *Surveillance, Power and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*, New York, St Martin's Press.

(43) REICHMAN (N.), 1986, « Managing Crime Risks: Towards an Insurance Based Model of Social Control », in SPITZER (S.), SCULL (A.), (eds), *Research in Law, Deviance and Social Control*, p. 151-172, Greenwich, Conn., JAI Press, p. 155.

se en catégorisations : « le traditionnel monopole de l'État en matière de violence est renforcé par de nouveaux moyens de collecte de l'information et d'analyse qui peuvent même rendre les précédents obsolètes. Le contrôle est plus efficacement exercé par la manipulation que la coercition, par des barrettes d'ordinateur que des barreaux de prison, par les multiples moyens de contrôle invisibles que par les menottes et la camisole de force ». <sup>44</sup>

Aucune population n'échappe à cette surveillance. Les systèmes de surveillance auxquels les individus sont soumis se situent au cœur même des institutions auxquelles ils appartiennent. Ceux que la société du risque a construit comme « population faible », et devant être pris en charge, sont soumis aux mailles du système étatique de répression, de prévention, de protection sociale, de contrôle sanitaire, etc. <sup>45</sup>. Quant à ceux qui ont survécu à la catégorisation panoptique, considérés comme plus forts et plus indépendants, ils sont tout de même soumis à l'imposition par l'État, au système d'éducation officiel, aux multiples règles d'autorisation, à la sécurité sociale, aux systèmes de contrôle sanitaire, mais aussi à toute une pléthore de règlements dictés par les entreprises privées concernées par le crédit, les valeurs mobilières et financières, les cartes d'abonnés, etc. De ce point de

vue, il n'est pas sûr que les populations marginalisées soient les plus soumises à surveillance. Ces populations sont en fait plus mobiles, socialement et dans l'espace, et disposent d'une gamme beaucoup plus large d'engagements et d'enchevêtrements institutionnels. Plus grande est la réputation de la personne, plus forte est la surveillance qui s'exerce sur elle. Plus on fait confiance à une personne, plus celle-ci est soumise à des mécanismes de surveillance qui viennent entériner la valeur de cette confiance.

L'accent mis sur la surveillance en matière de gestion des risques signifie que la qualification d'une personne, d'une organisation, ou de tout autre élément, porteurs de risques est plus importante que la culpabilité morale ou la responsabilité des individus pour mauvaise conduite. Toute chose et chacun d'entre nous doivent être rendus transparents par des mécanismes de surveillance. Chacun est présumé coupable tant que son profil de risque ne permet pas de dire le contraire. <sup>46</sup>

Dans le cadre de l'évaluation des activités nuisibles, « *la focalisation sur le contrôle des risques rend moins centrales les normes morales. Il n'est plus nécessaire dans un tel régime de distinguer le coupable de l'innocent ou le coupable de celui qui n'a rien à se reprocher. Presque chaque action humaine est porteuse d'une perte potentielle ;*

•••(44) MARX (G.), 1988, *op. cit.*, p. 220; voir également POSTER (M.), 1990, *op. cit.* ; POSTER (M.), 1995, *op. cit.*  
 (45) O'MALLEY (P.), 1992, « Risk, Power and Crime Prevention », *Economy and Society*, n°21, p. 252-275 ; SIMON (J.), 1993, *Poor Discipline: Parole and the Social Control of the Underclass, 1890-1990*, Chicago, University of Chicago Press ; NOCK (S.), 1993, *op. cit.*  
 (46) ERICSON (R.), 1994c, « The Decline of Innocence », *University of British Columbia Law Review*, n°28, p. 367-383.

*empiriquement, il est fort peu probable qu'une action donnée n'entraîne pas une perte dans tel ou tel domaine. Il s'ensuit que dans la société moderne du risque, aucune action n'est vraiment innocente*». <sup>47</sup>

La qualité de « coupable » n'est plus qu'une des caractéristiques du profil de risque d'une personne, le simple signe de ce qu'elle ne jouit pas d'un statut ou d'une citoyenneté à part entière aux yeux de telle ou telle institution et pour telle ou telle activité. On perd sa réputation de solvabilité. On n'a pas assez de crédit pour être admis à l'université, pour obtenir le statut d'immigré. Chaque transaction de la vie quotidienne nous labellise ainsi comme étant plus ou moins coupable et digne de prendre part aux échanges instrumentaux gouvernés par les institutions.

#### LA RÉGULATION PAR LA LOI ET LE MODÈLE DE LA CONFORMATION

Si les conceptions du maintien de l'ordre comme gestion des risques, surveillance et offre de sécurité trouvent leurs racines aux débuts de la période moderne, elles prennent un aspect différent sous la période contemporaine. Les risques changent constamment de nature, de même que les règles de communication, les manières de faire et les technologies permettant de les gérer. Dans la société du risque, la police est

prise dans un circuit complexe d'institutions publiques, d'entreprises privées, d'institutions philanthropiques, ce qui nécessite des transformations légales.

La société du risque est une société de normalisation. Il y a eu une expansion des systèmes de normalisation selon un mode de contrôle social de conformation. Cette expansion est conforme à la logique d'assurance sur les risques<sup>48</sup>. Cette logique fournit la base d'une invention sans fin de nouvelles règles, de manières de faire, et de technologies.

L'invention est d'abord le fait des professionnels qui travaillent pour les agences administratives chargées de gérer l'assurance et l'indemnisation. Le savoir d'un spécialiste donné se développe dans une logique de définition isolée et segmentée des problèmes plutôt qu'en termes de liens systémiques entre un savoir donné et d'autres savoirs.<sup>49</sup> La législation et les règles administratives qui résultent des connaissances professionnelles sont également fragmentaires et réduites, perpétuant ainsi le besoin de nouvelles améliorations et de nouvelles régulations pour assurer la compatibilité entre les savoirs.

Le modèle de conformation se décompose en « *une série d'instructions aux administrateurs, plutôt que par des contrôles sur les citoyens* »<sup>50</sup>. Le travail de ces administrateurs

•••(47) PRIEST (G.), 1990, « The New Legal Structure of Risk Control », *Daedalus*, n°119, p. 227.

(48) LOWI (T.), 1990, « Risks and Rights in the History of American Governments », *Daedalus*, n°119, p. 17-40.

(49) BAUMAN (Z.), 1992a, *op. cit.*

(50) LOWI (T.), 1979, *The End of Liberalism: The Second Republic of the United States*, 2e édition, New York, Norton, p. 106.

consiste en retour à instruire leurs administrés sur les risques qu'il convient d'éviter. Ce processus implique une construction et déconstruction permanente des risques qui viennent nourrir l'entreprise?<sup>51</sup>

Ce modèle est très différent du modèle répressif et judiciaire<sup>52</sup> car il traite des activités indésirables comme la pollution de l'environnement plutôt que des actes individuels. Le flux d'activités indésirables est sans fin et fait l'objet d'un haut degré de tolérance. Cette tolérance est en partie le résultat d'une incertitude morale quant à l'équilibre à trouver entre les dégâts causés et le besoin d'efficacité des organisations. L'application de la loi, fondée sur une connaissance scientifique du risque, est intimement liée aux règlements et normes toujours changeantes. La question de la conformité n'est pas simplement une question de restriction de l'action mais implique des actions positives afin d'améliorer l'état des choses et d'atteindre des normes sur lesquelles tous s'entendent. De ce point de vue, les attitudes sont tout aussi importantes que les actions menées dans le processus de mise en conformité. Les poursuites formelles sont le signe d'un échec et sont dès lors extrêmement rares. On privilégie plutôt la mise en place de micros rituels de négociation entre responsables de la mise en conformité et acteurs, dans le cadre d'une redéfinition

perpétuelle du savoir en matière de gestion des risques. Toutes ces caractéristiques indiquent que les activités indésirables sont d'abord des créations administratives, c'est-à-dire le produit d'une constante redéfinition des risques acceptables.

Dans ce contexte de conformation basé sur la régulation, le règlement et la connaissance scientifique du risque, la police s'est transformée. Elle fait elle-même partie de ce système complexe de gestion dans la mesure où elle doit répondre aux sollicitations d'autres institutions impliquées dans le travail de mise en conformité. La recherche sur la police n'a pas tenu compte de cet aspect. Par exemple, Reiss défend l'idée selon laquelle la police exerce une fonction de mise en conformité chaque fois qu'elle décide de manière discrétionnaire de ne pas procéder à une arrestation.<sup>53</sup> Ce faisant, il laisse de côté la manière dont la police contribue ainsi à servir les besoins de conformation d'autres institutions, notamment pour leur production de documents formatés en fonction de leurs nécessités internes. Il manque ainsi la question cruciale bien que négligée du rôle de la police dans la définition de la rationalité du risque pour d'autres institutions dont le but est la mise en conformité.

En réaction aux demandes d'information que requiert le modèle de la conformation, la police s'exécute et

•••(51) REISS (A.), 1989, *op. cit.*

(52) REISS, (A.), 1984a, *op. cit.*, p. 83-122 ; HAWKINS (K.), 1984, *Environment and Enforcement: Regulation and the Social Definition of Pollution*, Oxford, Oxford University Press ; MANNING (P.), 1987, « Ironies of Compliance », in SHEARING (C.), STENNING (P.), (eds), *Private Policing*, p. 293-316, Beverly Hills, Sage.

(53) REISS (A.), 1984a, *op. cit.*, p. 85-86.



devient plus proactive. Comme Reiss le prédit <sup>54</sup>, la stratégie type, tant du point de vue des individus que des organisations, relèvera plutôt des méthodes habituelles du fisc que de celles d'un service local de police. On peut s'attendre à ce que le modèle de la dissuasion évolue vers des formes de mobilisation plus proactives que réactives, et notamment vers des techniques proactives de respect de la loi, qui sont des stratégies instrumentales de contrôle social.

Le cadre de conformation qui guide l'action policière ne renvoie dès lors plus seulement à la nécessité de satisfaire les besoins de connaissance des agences de régulation de l'État. Il s'agit également de répondre aux exigences du secteur privé et de sa conception propre du risque et de la régulation. Dans les formes privées du maintien de l'ordre, essentiellement orienté vers la mise en conformité et la prévention des pertes, «la surveillance change de nature car l'attention se déplace de l'individu moralement coupable aux catégories de personnes qui peuvent être des facteurs de désordre». <sup>55</sup> De même que pour la police d'État, la police privée consiste en un système paperassier qui assure une surveillance en temps réel, et rétrospective par la seule vertu des masses de papier qu'elle produit <sup>56</sup>. Ces deux univers paperassiers

se croisent, mais la nature de cette rencontre a été pour l'instant négligée par la recherche.

La paperasserie policière et celle produite par les compagnies d'assurance sont étroitement intégrées. Cette intégration produit à son tour une intégration légale. Tous les domaines dans lesquels la police travaille pour les compagnies d'assurance - par exemple dans les enquêtes sur la régulation du trafic routier, sur les cambriolages - sont marqués par le pluralisme légal. <sup>57</sup> Par exemple, lorsque l'on considère un taux d'élucidation des affaires de cambriolage de trois pour cent, ce qui compte avant tout, c'est de produire des données fiables pour les compagnies d'assurance. Quant au droit qui s'applique dans ces cas, il relève moins du pénal que du civil. C'est la loi relative aux contrats d'assurance qui pallie les insuffisances du droit pénal, impuissant à punir les cambrioleurs. La police devient de ce fait une agence d'exécution des compagnies d'assurance. Comme le suggère O'Malley, <sup>58</sup> pour conserver son niveau de profit, tout particulièrement contre les risques qui ne font pas l'objet d'une régulation pénale, la compagnie d'assurance doit établir son propre ordre légal dans le cadre du contrat passé avec son client. Le contrat d'assurance (et plus récemment, la loi sur les contrats d'assuran-

••••(54) REISS (A.), 1984b, «Selecting Strategies of Social Control over Organizational Life», in HAWKINS (K.), THOMAS (T.), (eds), *Enforcing Regulation*, Boston, KluwerNijhoff, p. 23-24.

(55) SHEARING (C.), STENNING (P.), 1984, «From the Panopticon to Disney World: The Development of Discipline», in DOBB (A.), GREENSPAN (E.), (eds), *Perspectives in Criminal Law*, Aurora, Ontario, Canada Law Book, p. 340.

(56) *ibid.*

(57) O'MALLEY (P.), 1991, «Legal Networks and Domestic Security», *Studies in Law, Politics and Society*, n°11, p. 171-190

(58) O'MALLEY (P.), 1991, *op. cit.*, p. 172.



ce) établit les conditions obligatoires de protection que les propriétaires doivent remplir pour diminuer la prise de risque.

L'ordre légal institué par le contrat d'assurance contraint les assurés à gérer eux-mêmes les risques encourus. Par exemple, on interdit aux assurés de domicilier un commerce ou une profession à leur adresse privée ; on les oblige à se doter de suffisamment d'équipements de sécurité pour protéger leurs biens ; à déclarer à la police tout cambriolage, qu'il ait réussi ou échoué, à adresser à la compagnie d'assurance toutes les informations possibles et à accepter d'être cité comme témoin dans le cas d'un procès ; à accepter la surveillance quotidienne des programmes de police communautaire et de suivre les instructions que l'on pourrait leur communiquer afin de diminuer leurs prises de risque. O'Malley<sup>59</sup> montre comment la police participe de ce mouvement en jouant un véritable rôle de courtier et de co-promoteur des normes édictées par les compagnies. La police est entièrement partie prenante des stratégies de gestions des risques liés aux atteintes à la propriété.

Au-delà du droit pénal, d'autres branches du droit sont devenues des instruments d'interprétation des pratiques sociales du risque. Dans ces domaines, la loi dépend en premier lieu de la connaissance scientifique du

risque. Comme Michel Foucault et ses épigones le soulignent<sup>60</sup>, la science, comme la loi, fourmillent de prescriptions normatives non seulement à l'intention de leurs propres pratiques méthodologiques mais également en direction des populations. En particulier, la science sociale, qui est intimement liée à la science de la prévision actuarielle<sup>61</sup>, participe aux opérations de régulation par la fourniture de cas déjà instruits.

Quant au droit civil, au contact du contrôle des risques qui constitue sa mission principale, il a connu une extension très efficace de ce point de vue.<sup>62</sup> Dans tous les champs couverts par le droit civil, la distribution des risques et des indemnités fait l'objet de droits et le risque se voit ainsi légalisé<sup>63</sup>. Les tribunaux civils s'occupent de toutes sortes de risques en octroyant des dommages et intérêts qui viennent confirmer des règles de responsabilité et des droits statutaires. La question des motifs, des intentions, et de la peine deviennent accessoires face au travail d'évaluation des risques ayant causé le dommage. Les juges sont des ingénieurs d'une justice actuarielle, dont le travail consiste à ranger les parties prenantes dans des catégories d'acteurs prédéfinies afin de déterminer laquelle des parties est dans la meilleure position pour assumer les coûts et supporter les dommages causés. Dans un procès, ce qui

•••(59) O'MALLEY (P.), 1991, *op. cit.*

(60) BURCHELL (G.), GORDON (C.), MILLER (P.) (eds), 1991, *The Foucault Effect: Studies in Governmentality*, Chicago, University of Chicago Press.

(61) HACKING (I.), 1990, *op. cit.*

(62) PRIEST (G.), 1990, *op. cit.*, p. 209.

(63) LOWI (T.), 1990, *op. cit.*

(64) PRIEST (G.), 1990, *op. cit.*, p. 209.

compte avant tout est de savoir qui paiera l'addition.

Dans ce contexte, la distinction binaire entre ce qui relève du normal et de l'anormal perd de sa pertinence. Toutes les actions sont jugées à l'aune de leur contribution potentielle au dommage. La qualité morale des actions jugées est laissée de côté au profit d'une évaluation utilitaire des risques. Une morale utilitaire devient primordiale. « *L'objectif d'une maîtrise la plus efficace des risques devient l'alpha et l'omega* »<sup>64</sup> Paradoxalement, nous sommes tous coupables à un degré ou à un autre, ce degré étant calibré selon notre contribution probable au dommage : « *chacun de nous doit reconnaître que toutes nos actions sont susceptibles de léser les autres dans la société. En conséquence, chaque citoyen se trouve en position d'interaction continue avec la loi dans la mesure où toute action est potentiellement sujette à l'engagement de sa responsabilité* » (ibid, p. 215.)

Le « déclin de l'innocence »<sup>65</sup> s'accompagne d'une élévation de la respon-

sabilité individuelle. Chaque individu doit prendre conscience de ses actions afin de s'assurer qu'il n'accroît pas les risques de dommage. Cette réflexivité est facilitée par les technologies de classification du risque et de la loi, lesquelles instituent une surveillance perpétuelle. L'action judiciaire menace celui qui ne se contrôle pas car la responsabilité légale est facilement mise en jeu dans ce nouveau régime :

« *Notre moderne droit civil encourage le recours au litige comme instrument d'internalisation des coûts afférents au contrôle des risques. Notre système légal moderne, focalisé sur la question du risque, est un système aux dimensions étonnantes. Un tel système aspire à imposer un contrôle légal sur toutes les activités sociales qui contribuent à créer des risques. De cette manière, chaque action de n'importe quel citoyen devient en pratique l'objet d'un contrôle légal potentiel étant donné que chaque action est porteuse, d'une manière ou d'une autre, de risque* ». <sup>66</sup>

••••(65) ERICSON (R.), 1994c, *op. cit.*

(66) PRIEST (G.), 1990, *op. cit.*, p. 214.

# LA « TOLÉRANCE ZÉRO » EST-ELLE APPLICABLE EN FRANCE ?<sup>1</sup>

par Sebastian ROCHÉ

La comparaison de la délinquance et de la criminalité dans deux pays aussi différents que la France et les États-Unis, à la fois par les niveaux et structures de la délinquance, conduit à se demander pourquoi les causes sociologiques du crime discutées dans chacun des deux pays sont si proches. La particularité de la réponse new yorkaise à la délinquance n'est-elle pas précisément de rompre avec la recherche de ses causes sociologiques pour se tourner vers les actions pratiques qui peuvent favoriser sa diminution? Mais, étant donné les différences entre les deux pays, on est en droit de se demander en quoi la politique de « tolérance zéro » menée à New York serait applicable à la France.

Notes et études

203

En France, la délinquance et la criminalité ne progressent plus de manière linéaire depuis près de douze ans. Le niveau moyen de criminalité, connu des services de police, par habitant en 1997 est le même qu'en 1985. Ceci apparaît d'autant plus curieux que notre pays traverse une crise économique sans précédent par sa durée, qui tient les jeunes massivement au chômage et voit les inégalités sociales progresser à nouveau depuis quinze ans. Depuis maintenant six ou sept ans, les États-Unis vivent en matière criminelle un phénomène qui peut paraître étrange : une baisse substantielle et continue

des crimes violents, y compris ceux qui sont les mieux dénombrés et dont la statistique est la plus fiable, les homicides. Ce phénomène apparaît d'autant plus étrange aux Européens qu'ils ont des États-Unis une image très violente<sup>2</sup>, et que cette violence est perçue chez nous comme un phénomène structurel, peu susceptible de diminutions à la baisse.

L'explication de ces baisses est aussi difficile à donner pour les spécialistes que l'était celle de l'augmentation de la vague criminelle que les différents pays industrialisés ont connu depuis 1950. Aucune théorie sociologique n'est dura-

••• (1) Une première version de ce texte est issue d'un rapport rédigé à la suite d'une mission en tant que *Visiting Research Fellow* à l'université de Princeton, NJ, aux États-Unis de mars à juin 1997. Elle a été rendue possible par les soutiens du PIR-VILLES (CNRS) et de l'IHESI. L'auteur remercie particulièrement les personnes suivantes : Ezra Suleiman, directeur du *Center for European Studies*, université de Princeton, et John Dilulio, Woodrow Wilson School, université de Princeton.

(2) qui n'est d'ailleurs pas fautive si l'on se contente de considérer les homicides, mais en revanche très inexacte si l'on jette un œil sur l'autre forme de mort volontaire qu'est le suicide, ou encore les risques sur la route.

blement dominante dans le champ<sup>3</sup> et chaque théorie semble tirer sa force autant des faits que des choix politiques ou moraux. Personne ne paraît être en mesure de fournir d'explication scientifique du phénomène complètement satisfaisante ou documentée au plan empirique, ce qui laisse chacun libre de rechercher les aspects qui le satisfont le plus et de les mettre en valeur.

Nous voudrions présenter ces évolutions de la délinquance et de la criminalité dans deux pays aussi différents à la fois par les niveaux et structures de la délinquance. Ceci devrait nous permettre de revenir sur un certain nombre de stéréotypes. En dépit des différences entre les deux États, il semblera peut-être paradoxal que les causes sociologiques du crime discutées dans chacun des deux pays soient si proches. Et, enfin, la présentation comparée de la délinquance permettra de se demander en quoi les politiques publiques mises en avant pour répondre au phénomène délinquant se sont construites en relation avec les causes sociologiques, et en quoi les politiques menées à New York sont transposables à la France.

#### ÉVOLUTION ET STRUCTURE DE LA DÉLINQUANCE EN FRANCE ET AUX ÉTATS-UNIS

Les critiques les plus virulentes faites aux statistiques de police comme pur construit organisationnel ont finalement été balayées par l'ampleur du mouvement délinquant et les résultats

des enquêtes de victimation (ce qui ne veut pas dire qu'elles soient exemptes de défauts), tandis que les arguments qui faisaient de la peur du crime le résultat d'une manipulation des médias ont été mis au placard : le sentiment d'insécurité est maintenant une composante du problème de la sécurité.

Pour tous les pays occidentaux, il est maintenant avéré qu'une hausse substantielle de la criminalité a eu lieu entre 1930 (ou 1950 suivant les pays) et la fin du siècle. Des criminologues et historiens américains l'ont, les premiers, souligné parce qu'ils ont été touchés plus tôt et plus massivement. On parle de la théorie de la « réversion de tendance à la pacification des mœurs » (LANE, 1989) ou de la « courbe en U » (GURR, 1989). Depuis plus de quinze ans, le caractère international en a été souligné par des Américains (ARCHER et GARDNER, 1984), des Canadiens (CUSSON, 1990) et des Européens (VAN DIJK, 1991 ; EISNER, 1995 ; SMITH, 1995).

#### LA STRUCTURE DE LA CRIMINALITÉ

D'une manière générale, les sources disponibles sont de trois types : les statistiques de police et de gendarmerie, les sondages sur les victimes et les statistiques sanitaires. Nous allons revenir sur les critiques faites aux sources officielles, mais il nous semble qu'elles sont suffisamment fiables pour décrire correctement une tendance lourde et durable. D'une manière générale, les pays qui ont mis au point des enquêtes

••• (3) Voir notamment la synthèse que Maurice Cusson vient de publier sur les nouvelles théories (1998).

de victimation notent une convergence globale avec les statistiques officielles (pour un bilan, cf. CUSSON, 1990).

On sait que les atteintes aux personnes sont nettement moins fréquentes que les vols. Les statistiques de police rejoignent ici les résultats des enquêtes de victimation à l'instar des autres pays européens et même des États-Unis (KILLIAS, 1995).

#### *Homicides*

En France, d'après les statistiques de police, en 1972, on compte 1 173 homicides volontaires<sup>4</sup>. En 1996, on dénombre 2 385 homicides et tentatives (1171 sont réussis). Le taux d'homicidité est passé au taux de 2 pour 100 000. Mais la structure des homicides en France ne s'est pas fondamentalement transformée. En 1972, les homicides « ordinaires » (dont les motifs sont passionnels, sexuels, raciaux, dus à des différends, etc.) sont au nombre de 952, soit 81% du total ; on recense 152 meurtres crapuleux (pour vols), soit 13% ; le reste, 6%, étant composé des règlements de compte entre malfaiteurs. Les homicides ordinaires représentent, en 1996, 83% du total, les meurtres motivés par le vol, 13% et les règlements de compte entre malfaiteurs, 4%. On ne connaît pas en France d'études fouillées sur les relations qui unissent auteurs et victimes. Mais les statistiques de police citées montrent que la part des homicides ordinaires est dominante, et, au sein de ceux-ci, la

cause la plus fréquente est le différend ou la vengeance. Les homicides pour vols restent peu nombreux, mais cela évolue pour les mineurs (cf. tableau 3).

Aux États-Unis, la situation est très différente. D'une part, le taux d'homicidité est beaucoup plus élevé. Alors que le taux en France, d'après les statistiques de police, varie entre 2,6 pour 100 000 en 1993 et 2 en 1996 (pour les statistiques sanitaires, il est de 1,1 en 1993, sachant qu'il y a là une sous-estimation d'après les spécialistes de ces sources), aux États-Unis, il varie entre 8 et 10 pour 100 000 depuis 1970, il est de 9,3 en 1993 (*US Department of Justice, FBI, Criminal Justice Information Services Division*). De plus, la nature des homicides s'est radicalement transformée. Ils sont aujourd'hui beaucoup plus liés aux vols et de moins en moins aux conflits et à la vengeance : entre 1965 et 1992, on est passé d'un taux de 33% d'homicides familiaux à 10% (*US Department of Justice, Crime Data*).

*Vols de voiture, cambriolages, vols avec violences sur personnes*

Les homicides mis à part, les États-Unis sont-ils un pays plus criminel que la France ? Ce stéréotype demande à être discuté sur la base de données fiables. Or, nous savons que la statistique officielle est difficilement comparable d'un pays à l'autre si l'on veut être précis. Pour contourner en partie le problème, et notamment celui du taux

•••(4) Ce chiffre inclut les tentatives, qui ne sont, à l'époque, pas isolées des actes menés à terme.

de déclaration des atteintes à la police, nous pouvons utiliser les enquêtes de victimation américaines et européennes disponibles. Il reste à disposer de questions comparables pour tous les pays, ce qui est notamment le cas pour les cambriolages, les vols de voiture puis pour les agressions sexuelles et vols avec violence (cf. tableau 1).

TABLEAU 1 : LES VOLS DE VOITURE  
(% DE FOYERS TOUCHÉS ANNUELLEMENT)<sup>1</sup>  
(% DE PERSONNES TOUCHÉES PAR AN)<sup>2</sup>

	France	EU
Vols de voiture <sup>1</sup>	2,4	0,97
Vols avec violence <sup>2</sup>	0,4	5,4
Cambriolages <sup>1</sup>	2,4	2,16

Source : enquêtes de victimation européennes de 1988 et 1991 (KILLIAS, 1995) et enquête américaine de victimation de 1989 (*National Crime Survey*) du U.S. Department of Justice (1990, p. 251).

Ces études confirment que les États-Unis sont indiscutablement plus touchés par l'usage de la violence physique (homicides, vols avec violence) que la France et, d'ailleurs, que les autres pays européens. En revanche, les atteintes aux biens qui portent un réel préjudice financier comme le vol de voiture ou le cambriolage ne sont pas plus fréquentes aux États-Unis. Les vols de voiture eux sont même nettement moins fréquents.

#### *La part des jeunes*

En dehors de son intensité en direction des personnes, une autre des caractéristiques de la criminalité américaine par opposition à l'Europe, est la

place que tiennent les jeunes, et notamment les mineurs à la fois comme victimes et auteurs. Entre 1985 et 1991, les adolescents de 15-19 ans ont vécu une augmentation de leur taux d'homicidité de 154%. En moyenne, le décès par balle est devenu la plus fréquente des causes de décès pour ces jeunes. Et les garçons noirs souffrent d'un taux d'homicidité par balle qui est 8 fois supérieur à celui des blancs (*Center for Disease Control and Prevention*, Oct. 14, 1994, *Morbidity and Mortality Weekly Report*, p. 726).

En France, en dépit de l'agitation médiatique et politique que provoque la délinquance, on sera peut-être surpris d'apprendre qu'aucune enquête scientifique nationale n'a été à ce jour consacrée à l'ensemble de la délinquance des jeunes même si des travaux portent sur certains aspects (à l'école, CHARLOT, EMIN, 1997 ; dans la cité, BORDET, 1998). Les données médicales de l'INSERM permettent pourtant de nous assurer que les homicides ne sauraient être une des premières causes de décès chez les 14-18 ou 14-25 ans, il s'agit au contraire d'une des moins fréquentes, loin derrière les taux de suicide et les accidents de la route par exemple.

#### *Intensité spatiale*

Une autre singularité de la criminalité américaine, liée à celle que nous venons d'évoquer, est la concentration spatiale de la violence dans des proportions dont nous n'avons pas la moindre notion vécue. Sur les 3000 comtés

américains, 77 d'entre eux sont le théâtre de la moitié des homicides. 80% des personnes incarcérées dans les prisons de l'État de New York sont issues de 7 quartiers (*neighborhoods*). Don Russell et Bob Warner (1995, p.5) prennent l'exemple de la ville de Philadelphie. En 1994, elle représente 14% de la population de la Pennsylvanie, et 44% des crimes violents de cet état. À l'intérieur même de la ville, 430 homicides ont eu lieu toujours la même année, dont 340 contre des noirs (ces derniers représentent 40% de la population et 80% des victimes d'homicides), et la quasi totalité des 89 enfants tués sont noirs. Si l'on calcule un taux d'homicidité par voisinage, on voit que les «Badlands» affichent 100, soit 4 fois plus que le taux moyen de la ville qui est de 23. En France, aucun quartier, le plus chaud soit-il, ne peut présenter un tel contraste avec le reste de la ville à laquelle il appartient.

#### *Le système pénal face à la criminalité*

Le poids des minorités dans l'appareil pénal découle des faits précédemment exposés. Deux camps s'opposent, ceux qui dénoncent la discrimination raciale de l'appareil pénal (par exemple DONZIGER, 1996, mais aussi le Réverend J. JACKSON) d'une part, et d'autre part ceux qui dénoncent la faiblesse de la répression en direction des « super-prédateurs », ces jeunes issus des minorités

qui commettent des crimes horribles dans des quantités inconnues jusque alors, pour les motifs les plus futiles parfois.

Mais, à criminalité égale, les États-Unis sont-ils un pays où les criminels sont plus punis à des peines d'emprisonnement qu'ils purgent effectivement? Rien n'est moins évident. Il est de notoriété publique que le taux d'incarcération est très élevé (le pourcentage de personnes en prison par rapport à la population totale), avec un score de près de 500 pour 100 000, mais il n'empêche que l'usage de la prison est limité si l'on considère l'ampleur de la criminalité. Bennet, Dilulio et Walters (1996, p. 94) montrent que des personnes jugées « criminels violents » ne sont pas incarcérées dans les proportions suivantes : 47% de celles qui sont reconnues coupables d'un crime violent, 31% de celles reconnues coupables de deux crimes violents, et 23% de celles reconnues coupables de trois crimes violents. De ce fait, les prisons retiennent à 94% des auteurs de crimes violents, ou des auteurs ayant déjà purgé une peine pour d'autres délits (*Survey of State Prison Inmates, 1991, Bureau of Justice Statistics, 1992*). En moyenne, pour les criminels violents sanctionnés par de la prison, la peine effectuée est égale à 48% de la durée de la peine prononcée, y compris pour les auteurs d'homicides ou d'agressions avec l'intention de blesser - *assaults* (BENNET, DILULIO et WALTERS, 1996,

p. 102). En dépit des dénonciations de la dérive pénale américaine (WACQUANT, 1998), la lecture des taux d'emprisonnement sans ajustement par la fréquence des violences nous semblent insuffisantes pour tirer des conclusions définitives quant à la punitivité d'un État. Sans pour autant nier le rôle des politiques publiques, il convient probablement de ne pas faire de l'État « le producteur » de tous les rapports sociaux.

#### AUGMENTATION DE LA VIOLENCE PHYSIQUE

Prenons de la distance et quittons un instant du regard les années récentes : l'insécurité a une histoire qu'il n'est pas inutile de prendre en compte. Nous allons regarder en arrière pour prendre en considération les 45 années écoulées, puis ensuite les 10-12 dernières années.

Peut-on mesurer correctement les évolutions ? Les Américains sont en mesure de comparer l'évolution des statistiques de police et de celles issues des enquêtes d'opinion (pour les atteintes autres que les homicides qui, elles, sont issues des statistiques sanitaires, *vital statistics*)<sup>5</sup>. D'après les chiffres disponibles, ceux de 1996, la criminalité grave (*serious crime*) connue des services de police telle qu'elle ressort de la compilation effectuée par le FBI a encore diminué de 3% par rapport à l'année précédente ; la criminalité violente (*violent crime* :

*robbery, aggravated assault, rape, homicides*) de 7% et les homicides eux-mêmes ont reculé de 11%. Ceci constitue la cinquième baisse successive. Le taux d'homicidité aux États-Unis atteint aujourd'hui le seuil de 7,3 pour 100 000, le plus faible connu dans le pays depuis 1969. Jamais, depuis 1970, les États-Unis n'avaient connu de taux inférieur à 8 pour 100 000.

Les États-Unis ont la chance de disposer d'enquêtes de victimation très importantes (par leur ampleur, elles viennent juste derrière le recensement) depuis de nombreuses années. Chaque année, le bureau des statistiques du département de la Justice publie un volume intitulé *Sourcebook of Criminal Justice Statistics*. Cette chance est toute relative sans doute puisque la dotation en moyens de recherches correspond à l'acuité du problème criminel lui-même. Steven R. Donziger, président de la *National Criminal Justice Commission*, présente dans le rapport de cet organisme les évolutions comparées de l'index UCR (*Uniform Crime Reports*) compilé par le FBI et les chiffres de la NCVS (*National Crime Victimization Survey*) de 1973 à 1992 pour la criminalité violente. On voit que la criminalité violente enregistrée passe de l'indice 100 en 1973 à l'indice 180 (en tenant compte de l'augmentation de population) en 1992. La *National Crime Victimization Survey* n'enregistre rien de comparable. De

•••• (5) Les deux formules ont des biais, et l'une ne saurait remplacer l'autre. Par exemple, les enquêtes de victimation s'adressent à un individu à son domicile, ce qui exclut les personnes qui sont hospitalisées, en prison etc., alors même que, pour une partie d'entre elles, ces personnes se trouvent dans l'incapacité d'être à leur domicile précisément parce qu'elles sont des victimes ou des auteurs de violences.



1973 à 1983, l'indice reste au niveau 100, il diminue ensuite jusqu'en 1986 pour atteindre le niveau 88 avant de remonter progressivement jusqu'au niveau 100 en 1992 (1996, p.7)<sup>6</sup>. Les chiffres du FBI comptent environ 14 millions d'infractions et 2 millions de crimes violents en 1993. En 1973 comme en 1992, le sondage NCVS recense 35 millions de victimations. Il compte 5 millions de crimes violents en 1973 et plus de 7 millions en 1992. Cela dit, l'enquête de victimation américaine publiée début 1997 corrobore la baisse enregistrée par les chiffres policiers pour les crimes violents (-12% en 1995 par rapport à 1994).

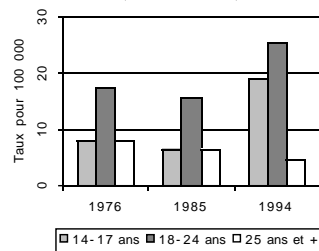
Les métropoles sont les lieux les plus violents. Et les variations, à la hausse puis à la baisse, y sont tout à fait spectaculaires. En 1990, 2154 homicides ont été recensés à New York. On en dénombre encore 1 177 en 1995. Après six années consécutives de baisse, on en compte, en 1997, 756, soit une baisse de plus de 60%. Ce nombre d'homicides fait de New York une ville plus sûre qu'en 1975 avec un peu plus de 1500 homicides enregistrés cette année là, et il faut se reporter aux années soixante pour trouver un chiffre inférieur, aux alentours de 400 homicides par an.

Pour résumer, disons que, aux États-Unis, les statistiques divergent quant à l'évolution de l'ensemble des délits mais convergent pour indiquer que les atteintes violentes (à l'exception de

l'homicide) ont progressé depuis 1973. Deux choses sont donc corroborées par l'UCR, les NCVS et les statistiques sanitaires : l'augmentation de la criminalité violente de 1950 à 1974 puis sa diminution ces dernières années.

Venons-en à la place des jeunes dans les évolutions récentes. Dans *Trends in Juvenile Violence*, James Fox (1996) présente l'évolution des taux d'auteurs d'homicides par classe d'âge. Il distingue les 14-17 ans, les 18-24 ans et les 25 ans et plus.

GRAPHIQUE N°1 : LES AUTEURS D'HOMICIDE ÉVOLUTION DE LEUR PROFIL SUIVANT LEUR ÂGE (1976- 1994).



Source: Fox James Alan (1996), *Trends in Juvenile Violence*, Bureau of Justice Statistics, p. 6.

De 1976 à 1985, les taux diminuent pour les 14-17 ans et ils font de même pour les 18-24 ans (mais à un niveau supérieur, autour de 15 pour 100 000). Pour les 25 ans et plus, la courbe indique une baisse de leur implication dans des homicides, de 8 à 6,3. Puis à partir de 1986, on constate une envolée des courbes pour les populations de moins de 25 ans, tandis que celle de 25 ans et plus continue à diminuer pour atteindre 4,7, soit moins 25%. Les 18-24 ans sont 60% de plus à commettre

•••(6) D'autres auteurs avaient déjà souligné ces points (SKOGAN, 1990).

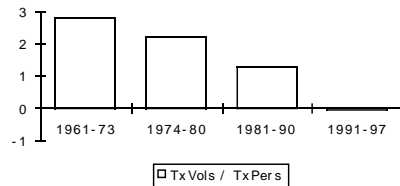
des homicides en 1994 qu'en 1985, les taux passant de 15,7 à 25,3 (FOX, 1996, p. 7). En 1994, les plus jeunes commettent presque trois fois plus d'homicides, les taux passant de 7 à 19,1 pour les 14-17 ans, les distinguant radicalement des 25 ans et plus, alors que jusqu'en 1985 leurs comportements étaient similaires. Bien que leur poids dans la population ait tendu à diminuer ces dernières années, les jeunes de moins de 25 ans, et particulièrement les très jeunes, se sont tournés vers les crimes violents avec une plus grande intensité. Les jeunes gens de 14 à 18 ans représentent 27% des victimes d'homicides et 48% de tous les auteurs (FOX, 1996, p. 2). Et les tendances sont identiques pour les violences qui n'entraînent pas la mort.

En France, la délinquance a commencé son cycle haussier autour de 1955. Il faudra attendre 1985 puis 1992 pour voir la belle courbe linéaire se briser par deux fois. Depuis 1985, la courbe serpente alternant montées et descentes. Notre pays a donc connu une « délinquance de prospérité » (avant le premier choc pétrolier en 1973, puis le second en 1979) ce qui a été nommé une *welfare criminality* (SVENSSON, 1986) puis une « délinquance de crise » avec la remontée des inégalités et l'exclusion dont l'expression « les banlieues » est l'incarnation au plan territorial. Aucune des deux périodes n'a été associée à une baisse durable du niveau de délinquance. Mais, la seconde période affiche une pause : aurait-on atteint les hauts plateaux du crime ? Nous avons déjà eu l'occasion de souligner

que la croissance des vols a suivi celle de la croissance économique mesurée par le PIB : élevée pendant les trente glorieuses, moyenne entre le premier et le deuxième choc pétrolier, faible depuis (ROCHÉ, 1996).

Un second phénomène mérite d'être présenté : il s'agit des taux d'augmentation annuels moyens pour les vols et les atteintes aux personnes. Depuis 1960, ils évoluent de la manière suivante : mesuré par le rapport entre les deux taux (variation moyenne annuelle des vols dans une période donnée divisée par la variation annuelle moyenne des atteintes aux biens dans la même période) l'écart entre le taux de croissance des vols et celui des atteintes aux personnes tend à diminuer puis même à s'inverser sur les années récentes (cf. graphique n°2).

GRAPHIQUE N°2 : TAUX DE CROISSANCE DES VOLS  
RAPPORTÉ À CELUI DES ATTEINTES AUX PERSONNES  
EN FRANCE



Source: calculé d'après les statistiques de police et de gendarmerie, publiées annuellement à la Documentation Française.

Autrement dit, plus on avance dans le siècle, moins la vitesse de progression des vols augmente par rapport aux atteintes aux personnes. Certes, en nombre, les vols restent incomparablement plus fréquents. Mais en tendance, cette orientation à la violence physique

doit être soulignée. Notons encore une fois que ce phénomène n'a pas débuté avec la période de chômage durable et massif depuis 1981, mais qu'il lui est antérieur et qu'il s'est accéléré dans la dernière décennie.

On s'interroge actuellement beaucoup sur la place des mineurs dans la délinquance et la criminalité en France. Les chiffres officiels montrent pour ces dernières années une augmentation tout à fait importante du nombre de mineurs dans les personnes mises en causes. On le voit au tableau suivant :

en 1997, on a gagné de 2 à 14 points de pourcentage suivant les infractions considérées.

Mais, ces chiffres ont des limites : ils dépendent des plaintes ainsi que des comportements policiers (inscription en main courante ou rédaction d'un procès verbal ; anticipation du comportement des magistrats de donner suite ou non) et ils sont calculés sur le nombre des auteurs identifiés qui ne sont qu'une toute petite partie de l'ensemble. Pour les vols, ce chiffre varie autour de 15%. Lorsqu'on indique que

TABLEAU N°2 : POURCENTAGE DE MINEURS PARMIS LES PERSONNES MISES EN CAUSES EN 1994 ET 1997 POUR DIVERSES INFRACTIONS (EN POURCENTAGES ARRONDIS AU POINT PRÈS)

	1993	1997	1993-1997
Toutes infractions	13	19	+6
<i>Tous vols</i>	23	32	+9
dont vols avec arme à feu	9	14	+5
dont contre les particuliers sur voie publique	17	25	+8
dont vols avec violences sans arme à feu	29	43	+14
dont vols d'automobiles	24	33	+9
dont vols deux roues à moteur	54	59	+5
<i>Tous crimes et délits contre personnes</i>	8	13	+4
dont homicides	4	6	+2
dont coups et blessures volontaires	11	15	+4
dont menaces et chantages	14	19	+5
<i>Infractions à la législation sur les stupéfiants (trafic)/toutes destructions et dégradations de biens</i>	6/24	11/32	+5/+9
dont destructions, dégradations de biens publics (autres)	40	48	+8
dont destructions, dégradations de véhicules privés	18	25	+7
dont destructions, dégradations de biens privés (autres)	21	29	+8

Source : statistiques de police et gendarmerie 1997 et 1993, p. 107-110

la délinquance des jeunes en matière de vol a augmenté de 9 points, en réalité ce sont les mises en causes des jeunes qui ont augmenté. La variation de 9 points est à calculer sur les 15% d'auteurs connus (soit 9% de 15%). Autrement dit, s'il n'est pas exclu que la délinquance des jeunes augmente, les taux d'augmentation, calculés sur des faits dont les taux d'élucidation sont bas, se révèlent assez douteux et ne peuvent être pris au pied de la lettre.

Pour autant, tous les crimes ne sont pas commis que par des auteurs inconnus. Les chiffres les plus fiables concernent les homicides qui sont quasiment tous connus et élucidés à près de 80%. Or, l'évolution dont ils témoignent augmente et se transforme en même temps que la contribution des mineurs.

Les mineurs représentent 6,2% des mises en causes en 1997 pour homicide et 8,6% pour tentative d'homicide. Les mineurs victimes représentent 68 cas sur les 963 recensés par la police et la gendarmerie, soit 7% du total (en 1987, on en dénombrait 59, et 61 en 1977).

À la différence des États-Unis, les mineurs représentent à peu près le même pourcentage de victimes et d'auteurs d'homicides. En France, les homicides (et les tentatives) sont de nature largement relationnelle pour les majeurs. En revanche, pour les mineurs elles sont plus souvent des moyens de réaliser un vol. L'homicide est alors plus instrumental (tous les mineurs auteurs de ce type de violence instrumentale sont de sexe masculin). On

enregistre ces toutes dernières années une augmentation sensible de ces violences instrumentales.

La comparaison sur plus de dix ans n'est possible qu'en rassemblant les homicides et les tentatives d'homicides qui, jusqu'en 1988, n'étaient pas dissociés au plan statistique. On s'aperçoit que ces violences sont plus fréquentes ces dernières années (81 homicides en 1975, 109 en 1987, 97 en 1993, 147 en 1996 et 136 en 1997) et également que, ces dernières années, le motif est nettement plus lié à la recherche du profit.

Si l'on regarde en détail l'année 1997, on compte 13,5% de mineurs (et donc 86,5% de majeurs) chez les auteurs d'homicides pour vols, contre en moyenne 6% de mineurs pour les autres motifs d'homicides. Et on compte 22,5% de mineurs (et donc 77,5% de majeurs) chez les auteurs de tentatives d'homicides pour vols, contre en moyenne 7,5% de mineurs pour les autres motifs de tentatives d'homicides.

TABLEAU N°3 : POURCENTAGE DE MINEURS AUTEURS D'HOMICIDES ET DE TENTATIVES D'HOMICIDES SUIVANT LE MOTIF EN FRANCE

	Homicides pour vol (%)	Autres homicides (%)
1975	6,7	5,3
1987	7,6	4,2
1993	7,2	4,3
1997	16,7	6,3

Source : d'après les statistiques de police et de gendarmerie publiées annuellement à la Documentation Française.

En dehors des homicides, on pourrait imaginer que les faits enregistrés par la police et la gendarmerie le sont mieux et plus souvent qu'auparavant. Les sondages sur les actes dont on est victime qui ont tardé à se développer en France nous apportent des éclairages. En 1987, une enquête de victimation montrait que le taux d'appels à la police des victimes de cambriolages et de vols (non différenciés) étaient de 72,6%, de 34% pour les violences familiales et de 26% pour les agressions sexuelles, et enfin de 43,3% pour les autres agressions (Zauberman *et alii*, 1990, p. 89). Le volet français de la première enquête internationale de l'ICVS en 1988 donne un taux de 82% d'information des policiers par la victime d'un cambriolage réussi, et de plus de 96,5% pour les véhicules automobiles et 68,1% pour les

TABLEAU N°4 : LE TAUX DE DÉCLARATION  
DES VICTIMES AUX AUTORITÉS

Avez-vous, ou quelqu'un d'autre a-t-il, déclaré l'incident à la police ? (%)	
Vol de voiture	95%
Cambriolage	78,4%
Vol dans la voiture	61,3%
Vol avec violences	57,4%
Vol sans violence	47,7%
Vandalisme sur la voiture	46,9%
Agression sexuelle	29,8%

Source: tableau réalisé d'après l'*International Crime Victimization Survey*, 1996 ; cité par GRÉMY (JP), 1997, *Les Français et la sécurité*, Paris, IHESI, p 143.

vols dans la voiture (VAN DIJK *et alii*, 1989, p. 8). En 1996, le dernier volet de l'ICVS donne les résultats présentés dans le tableau n°4.

Les enquêtes locales montrent des pourcentages stables : les taux sont de 97,5% pour les véhicules automobiles et 61,5% pour les vols dans la voiture en 1989 (ROBERT et ZAUBERMAN, 1991). Des enquêtes locales plus récentes montrent que ces chiffres gardent leur actualité. À Saint Etienne en 1995, commune de 200 000 habitants, les taux de déclaration sont de 94,4% pour les vols de voiture, de 87,9 pour les cambriolages, de 63,3 pour les vols dans la voiture et les dégradations de véhicules, de 56,4% pour les agressions (ROCHÉ *et alii*, 1998).

On voit que, pour les faits comparables, il n'y a guère eu d'évolution depuis les années 1987-89.

Les vols de voiture sont toujours très bien déclarés (autour de 95%), les vols dans la voiture restent rapportés à 60% environ.

Les cambriolages se situent dans un taux de déclaration aux environs de 80%. La police reste informée des atteintes sexuelles dans environ un quart des cas (+ 3 points).

Si l'on estime que les « autres agressions » (non sexuelles et hors de la famille), soit les agressions dans la rue en 1987, correspondent aux vols avec violence en 1996, il y a là une augmentation de 43% à 57%, soit plus 14 points de pourcentage. Cela n'est pas impossible et correspondrait à l'augmentation rapide des atteintes contre les personnes dans la statistique officielle de police ces cinq dernières années, mais il y a là plus d'incertitude étant donné la comparabilité limitée

des items. Il n'y a donc pas eu de modification radicale dans l'ensemble de la population française (ce qui n'exclut pas des modifications substantielles pour certains de ses segments) du comportement de plainte pour ces atteintes depuis sept à dix ans. Ce facteur ne saurait en conséquence expliquer les variations de la délinquance et de la criminalité pour la France entière sur la période considérée.<sup>7</sup>

Ceci a deux conséquences importantes : d'une part la diminution des vols enregistrée par la police et la gendarmerie a toutes les chances de correspondre à une diminution réelle des faits commis ; d'autre part, l'augmentation des atteintes aux personnes enregistrées a de bonnes chances de correspondre à une réelle augmentation des prédatons dans notre pays<sup>8</sup>.

Le phénomène est incontestablement urbain. Si l'on corrèle différents délits avec les taux d'urbanisation des départements français en 1984 et 1994, on trouve que les destructions et dégradations le sont plus que les vols qui, eux-mêmes, le sont plus que les homicides (ROCHÉ, 1998), mais le taux de délits par habitant est d'autant plus élevé que l'urbanisation est forte. Précisons cependant que toute la délinquance ne trouve pas sa source dans «les banlieues». Il ne faudrait pas ramener la question délin-

quante à celle des banlieues. D'ailleurs, ces espaces n'ont pas une homogénéité totale : on rassemble sous ce terme des quartiers périphériques de grandes ou de petites villes, et également des communes entières (en région parisienne notamment). Certains quartiers des grandes villes ont pourtant une population plus nombreuse que les petites villes prises comme un tout. Faut-il également préciser que les banlieues françaises ne sont pas, à la différence des *inner-cities* américaines, des ghettos mono ethniques (LEPOUTRE, 1997), insalubres (voir les données urbaines rassemblées par PUMAIN et GODARD, 1996) et particulièrement violents en matière d'homicides ? Ce sont des espaces qui s'appauvrissent. Ce ne sont pas les mêmes familles qui deviennent de plus en plus pauvres, mais les lieux où se retrouvent les plus défavorisés à la fois du fait des politiques publiques de peuplement mais également de la fuite des familles appartenant aux couches moyennes (sur les entrants et sortants dans le parc HLM, cf. INSEE, 1993).

Des changements sont probablement en cours ces dernières années. L'étude de victimation de l'INSEE montre notamment que les agressions entre personnes connues sont nettement plus fréquentes chez les plus défavorisés (CRENNER, 1996). Deux choses sont probablement

•••(7) Sur ce point, voir le travail que viennent de publier ROBERT *et alii* (1998) sur la comparaison des chiffres de la police et des enquêtes de victimation entre 1984-85 et 1995-96.

(8) Pour autant, ces chiffres ne nous donnent pas d'indication sur le profil des auteurs, puisque ces derniers restent largement inconnus à la fois des victimes (seuls 17% des victimes d'agressions connaissent l'agresseur à St Etienne, et 28,4% à Romans qui n'est qu'une petite ville, et encore ces taux sont-ils très élevés par rapport à l'ensemble des atteintes : les agressions sont les seuls actes pour lesquels il y a une confrontation) et des policiers (les taux d'élu-cidation pour les vols avec violence sur la voie publique sont de l'ordre de 27,5% à 18,7% suivant qu'on regarde les vols avec arme à feu ou sans arme et ils varient entre 10% et 15% pour les autres vols).

cachées sous ce résultat : d'une part, en milieu rural, il y a une pauvreté qui fait moins parler d'elle et qui s'accompagne d'une forte interconnaissance. Et, d'autre part, en milieu urbain, le fait de voir les banlieues rassembler les plus pauvres au fur et à mesure que le processus de ségrégation spatiale se poursuit a un effet sur la délinquance. Une « délinquance de rétraction » est enregistrée par les enquêtes : les personnes défavorisées, immobilisées dans une position de leur trajectoire résidentielle, ont des comportements agressifs les unes vis-à-vis des autres, se battent pour des questions d'honneur (pour les jeunes, BARREYRE, 1992) ou d'identité territoriale ou même de maîtrise d'un territoire commercial (sur la drogue, cf. DUPREZ et KOKOREFF, 1997).

#### DES CAUSES DU CRIME À CELLES QUI PERMETTENT DE LE COMBATTRE

L'analyse des causes du crime est un puits sans fond. Comme le notait Maurice Cusson, aux causes anciennes se sont ajoutées de plus récentes (1998). Tout semble pouvoir être une cause : l'hérédité, la personnalité, l'urbanisation, l'inégalité économique, les médias de masse, la démographie, l'organisation familiale, l'usage de produits stupéfiants, la certitude de la peine, le comportement des victimes potentielles, l'accessibilité et la vulnérabilité des cibles, etc. Chacune de ces causes a donné lieu à des « théories », plus ou moins concurrentes - elles ont pour nom théorie « de la privation relative », « des routines »,

« des opportunités » etc. - qui ont mis en forme les schémas qui conduisent à la délinquance. Nous ne voulons donc pas trancher ici sur les déterminants de la délinquance. Notre seule ambition est de rappeler celles qui sont le plus souvent invoquées au cours des années quatre-vingt-dix, pour en arriver à nous demander si la connaissance des causes sociologiques de la délinquance a un rapport avec les politiques mises en œuvre. Précisément, aux États-Unis, la politique new yorkaise s'est construite en rupture avec la recherche des causes dites socio-démographiques. Déjà, en 1975, J. Q. Wilson avait indiqué que « *l'exigence de solutions causales (...) nous détourne des choses que le gouvernement peut raisonnablement faire* » (1975, XV). Puis, dans cette ligne interprétative, les premières réflexions sur la « vitre brisée » se sont muées en politiques publiques. Mais, on ne saurait emprunter la même direction aveuglément sur la foi de la réussite Outre-Atlantique sans discuter de la transformation de l'action policière aux États-Unis et de son caractère transposable en France.

#### QUELLES SONT LES CAUSES SOCIOLOGIQUES PRÉFÉRÉES ?

Aux États-Unis ou en France, pour expliquer la délinquance, il faudrait citer des facteurs comme la drogue, le poids des jeunes, l'emploi, la sévérité des sanctions pénales, les méthodes policières. Suivant les courants ou les sensibilités, certaines variables sont mises en avant.

Ce sont les causes préférées du moment. On ne peut qu'être frappé du décalage qui existe, en France, entre la virulence du débat public et l'absence de recherches systématiques. Les rapports officiels établis par des universitaires qui traitent des violences, même s'ils ne cherchent pas à les expliquer, ne contiennent aucune référence à des travaux empiriques systématiques sur ces sujets pour une raison simple : il n'y en a pas (on pourra se reporter au dernier en date : BODY-GENDROT, LE GUENNEC, HERROU, 1998). Tout se passe comme si le phénomène était connu et balisé.

#### *Effet de contexte*

La criminologie quantitative américaine a toujours souligné la place des jeunes dans la criminalité, ne serait-ce que mesurée par des indicateurs aussi simples que leur poids dans la population totale (WILSON et HERRNSTEIN, 1985 ; SKOGAN, 1989). Par ailleurs, une analyse plus culturaliste souligne également ce fait. Le livre de Courtwright, *Violent Land*, vient d'être publié à nouveau (1996) : il insiste sur le rôle des jeunes hommes non mariés dans toute l'histoire de la violence du pays. Si l'on retrouve en France une littérature qui souligne la faible délinquance des femmes, et si les criminologues évoquent parfois la variable démographique au regard des évolutions

récentes (BONFILS, 1996), il n'y pas là de paradigme explicatif. Les sociologues qui s'intéressent aux quartiers pauvres des villes ont en revanche toujours souligné la place des jeunes dans les agglomérations dont elles font partie (les quartiers prioritaires de la politique de la ville ont une population nettement plus jeune, voir CASTELLAN, GOLDBERGER, MARPSAT, 1992). Mais, ce facteur démographique ne semble pas valoir la peine d'une investigation systématique de ses relations avec la délinquance, il est évoqué comme un effet de contexte<sup>9</sup>.

On souligne, en France comme aux États-Unis, le rôle actif des jeunes dans la délinquance. Il s'agit là d'un facteur distinct du premier (mais qui peut se combiner avec lui) : il est constitué d'une sorte de « taux d'activité » illégale. Le nombre de jeunes dans la société ne permet pas de prédire le taux d'activité moyen de chacune de ces personnes. Cette piste explicative conduit vers une autre : la déstructuration des familles. Il s'agit là d'un filon (voir les travaux classiques depuis HIRSCHI, 1969). La principale différence entre les deux pays tient au niveau de violence attribué aux jeunes : aux États-Unis les travaux universitaires portent sur les crimes violents. Une autre différence tient également aux travaux scientifiques réalisés : alors qu'ils sont très précis et nombreux aux États-Unis (par exemple, dans la communauté noire, cf.

•••(9) Cette désaffection peut être alimentée par la perception intuitive qu'il s'agit dans notre pays d'une fausse piste, ce que semblent accréditer nos travaux. La courbe du nombre ou du taux de jeunes est diachroniquement très mal liée à celle de l'ensemble de la délinquance (ROCHÉ, 1998b). L'introduction d'une variable « poids des 14-18 ans » dans des analyses de régression sur la délinquance dans l'ensemble des départements français ne donne aucun résultat (ROCHÉ, 1998a).



MANN, 1993), en France, ils sont très rares (voir la rigoureuse présentation des chiffres officiels par AUBUSSON DE CAVARLAY, 1997) et relèvent souvent d'une position idéologique ou professionnelle.

À ce dernier titre, il est symptomatique que les professionnels du pénal, et notamment les magistrats aient pris une telle place dans la médiatisation de la question. On ne peut que déplorer la faiblesse des sources scientifiques dans notre pays.

#### *Le crack et la drogue*

Une autre explication avancée de la violence est la drogue. Ainsi, entre 1990 et 1996 aux États-Unis, le crack fait irruption puis se retire : « *crack came, crack went* ». Le crack fait son entrée au début des années quatre-vingt, puis, après le pic de 1985, les données montrent une diminution de son usage. Le crack est un agent psychoactif plus puissant que les autres drogues. Il provoque des addictions plus rapides, il favorise des comportements très violents, et a été impliqué dans les cas d'abus sur les enfants les plus monstrueux de la dernière décennie. Entre 1985 et 1992, chez les jeunes de 12 à 17 ans, le pourcentage de ceux qui prennent de la cocaïne (la forme principale étant le crack) passe de 1,4 à 0,3%, avant de remonter à 0,4% en 1994.

La tendance est la même pour les autres drogues illégales (ce qui inclut la cigarette ou l'alcool pour les mineurs,

ainsi que la marijuana) avec des taux respectifs pour les trois années citées de 14,9, 6,1 puis 9,5 (BENNET, DILULIO et WALTERS, 1996, p. 151). Sans qu'on ait d'explication bien documentée du phénomène, le public, jeune ou non, est beaucoup moins réceptif aujourd'hui à l'offre de crack, ou même à d'autres drogues, qu'il ne l'était il y a une décennie.

En France, le rôle de la prise de drogue a fait beaucoup parler de lui. Mais les travaux qui y sont consacrés restent rares. Nous n'avons pas d'études sur les variations temporelles.

En revanche, nous disposons de quelques analyses synchroniques. Lorsque ces travaux partent des données policières, on trouve une association entre usage de drogue et délinquance. M. D. Barré montre ainsi qu'à Paris « *un grand nombre d'usagers de produits illicites sont aussi impliqués dans des affaires de délinquance (autres que l'usage et la revente) : 68% si l'on considère l'ensemble des usagers, et 85% si l'on considère les usagers de drogue dure* » (1994, p.178). Parmi l'ensemble des délinquants, toujours selon la même étude, 13% sont usagers de drogues dures (1994, p.155).

L'étude menée à l'INSERM par M. Choquet et S. Ledoux montre une association entre certains modes de vie et des comportements violents chez les jeunes de 13 à 18 ans (cf. tableau n°5) et notamment la prise de drogue illicite ou l'alcool.

L'emploi est, en France, la variable qui se voit systématiquement associée à la question de l'insécurité. Il apparaîtra peut-être surprenant, encore une fois,

TABLEAU N°5 : QUELQUES FACTEURS ASSOCIÉS AUX VIOLENCES DES JEUNES DANS NEUF ACADÉMIES EN FRANCE

	Vol (> ou égal 1 fois)	Racket
Usagers de drogues illicites	25%	23%
Consommation régulière d'alcool	25%	36%
Moyenne	14%	2,6%

Source : enquête INSERM, avril-mai 1993. Choquet et Ledoux, 1994, p. 131 et tableaux XXV-1 et XXV-3 en annexe (p. 342-343).

de ne pas trouver beaucoup de travaux qui y soient consacrés. Le débat sur la pauvreté et le crime fait, en France comme aux États-Unis, l'objet d'une opposition entre deux camps. D'un côté, on trouve les tenants de la privation relative qui montrent que les pauvres constituent des couches statistiquement plus criminelles que les autres (BLAU, 1982), et par l'observation qu'une criminalité impulsive est associée à la précarité de la vie (FLEISHER, 1995). D'un autre côté, on souligne l'absence de lien sur la moyenne durée entre le taux de chômage et les évolutions de la criminalité (voir la synthèse de RUBINSTEIN, 1992). Aux États-Unis, sa baisse récente peut ainsi être comprise comme une confirmation de l'effet de la privation relative - moins de pauvres, c'est moins de

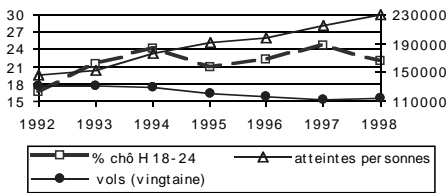
crimes - ou, à l'inverse, comme une confirmation de son absence de pouvoir explicatif - ce facteur ne saurait expliquer une diminution de 50% des homicides. En France, les défenseurs de la théorie de la privation relative pourront se demander pourquoi le recul des inégalités pendant les Trente glorieuses s'est accompagné de plus de vols, d'atteintes aux personnes et de plus de meurtres, mais aussi pourquoi l'accroissement des inégalités n'ont pas accentué les vols plus que les atteintes aux personnes. Mais aussi, pourquoi il a fallu attendre la fin des années quatre-vingt pour voir les motifs d'homicide se transformer nettement chez les mineurs.

Enfin, on peut s'interroger sur l'absence de lien étroit entre le taux de chômage des jeunes et les variations temporelles de la délinquance enregistrée depuis 1992 (cf. graphique 3).

Or, d'un point de vue scientifique, il est beaucoup plus convainquant de montrer que l'addition de chômeurs supplémentaires est associée à plus de délits (ou l'inverse) que de trouver des relations synchroniques au plan géographique (il ne fait pas de doute qu'elles existent, par exemple, au plan départemental, cf. ROCHÉ, 1998). Si le chômage était la cause essentielle on devrait, en dépit des imperfections des mesures, observer un parallélisme des fluctuations : chaque point de pourcentage de chômage en plus devrait se traduire par une certaine quantité de vols ou d'atteintes aux personnes (coups et blessures, mœurs) en plus. Or, ce n'est

guère ce qu'on observe. Entre 1992 et 1994, le chômage des jeunes passe de 20,8 à 27,7% tandis que les vols diminuent de 42 000 unités et sont au nombre de 2 573 074. Entre 1997, le taux de chômage atteint même 28,1% tandis que les vols sont en baisse. Entre 1997 et 1998, le chômage des jeunes diminue, tandis que le nombre de vols se met à augmenter. Pour sa part, la courbe des atteintes aux personnes décrit une augmentation linéaire de 1992 à 1998. En revanche, celle du chômage est faite d'une hausse jusqu'à un sommet (1992-1994), puis d'une baisse et d'une remontée jusqu'à un deuxième sommet (1997), avant une baisse en 1998.

GRAPHIQUE N°3 : LE TAUX DE CHÔMAGE DES HOMMES DE 15-24 ANS, LES VOLS ET LES ATTEINTES AUX PERSONNES



Sources : enquêtes emploi de l'INSEE (chiffre donné au mois de mars de chaque année) et statistiques de police et de gendarmerie.

Ces différentes variables interagissent probablement entre elles. Ainsi, aux États-Unis, on aurait vécu, en dépit de la multiplication des actes de jeunes « prédateurs » ou « super prédateurs », une période de relative accalmie du fait du faible poids des plus jeunes dans la population, tendance temporairement annu-

lée par l'effet du crack sur les comportements violents. À effet constant de la variable démographique, l'Amérique aurait dû connaître une diminution de la criminalité depuis plus de dix ans. Elle apparaît avec un effet retard. Va-t-elle durer ? Les démographes projettent une augmentation rapide de la population âgée de 10 à 17 ans dans les années qui viennent. Entre 1990 et 2010, les 10-14 ans seront 21% de plus, les 15-17ans, 31% de plus (*Bureau of the census, 1993, et Office of Juvenile Justice and Delinquency Prevention, 1995*). Même si les comportements liés à l'usage du crack se tassent, ces projections n'augurent rien de bon en matière criminelle. En dépit de la différence d'intensité avec laquelle se pose la question criminelle entre les États-Unis et l'Europe, le débat s'organise le long de lignes de forces somme toute assez comparables. Les oppositions entre les approches conservatrices et libertariennes du crime sont assez connues. D'un côté, on questionne la réalité de l'augmentation de la criminalité violente (vivons-nous vraiment une époque plus difficile que dans le passé), ce qui débouche sur une mise en cause de la peur du crime comme fondement illégitime des politiques de sécurité<sup>10</sup>. De l'autre côté, il y a ceux qui tiennent pour effective l'augmentation de la criminalité violente, et s'appuient sur les chiffres officiels. Puis, viennent les causes : et là, à nouveau, chacun fait son marché dans les rayons des meilleures explications.

•••(10) Sur ce point cf. *Thinking About Crime* de James Q Wilson (1975) dans le débat américain, et ce que nous avons nous-même souligné dans le débat français (cf. la discussion sur « la peur illégitime », ROCHÉ, 1994).

Il est assez saisissant que l'abondance de matériaux scientifiques aux États-Unis n'ait pas permis d'aboutir à un consensus plus fort qu'en France sur cette question.

#### UNE NOUVELLE PRÉVENTION ?

C'est l'abondance même des causes supposées du crime et des expertises qui a motivé une dénonciation des « têtes d'œuf » (*egg heads*) universitaires.

En effet, à côté de ces causes débattues dans l'arène politique (les jeunes, la drogue, le chômage) du fait de leur caractère politisable et moral, d'autres causes ont fait l'objet de travaux importants (sur les opportunités), et ont alimenté la transformation des modes d'action des professionnels en charge de la sécurité : il s'agit de l'approche contextuelle ou situationnelle, et de l'approche par les désordres plus connue sous le nom de « théorie de la vitre cassée ».

Ces théories avaient en ligne de mire d'obtenir des améliorations dans un délai raisonnable par l'activité des personnes et services responsables de la sécurité.

Clarke a ainsi reconnu que la prévention situationnelle n'était pas une réponse aux inégalités sociales (1980) tandis que Kelling et Coles ne se sont pas cachés de chercher à « identifier des objectifs réalistes et susceptibles d'être atteints en matière de politiques à mettre en œuvre » (1996, p. 5).

Ceci fait aussi la nouveauté de ces approches et leur donne un aspect constructif.

#### *Les freins de la délinquance*

Si l'on identifie beaucoup des facteurs qui accélèrent la délinquance (*cf.* plus haut), on entend moins souvent parler de ceux qui la freinent.

Or, on peut faire l'hypothèse que ce ne sont pas toujours les deux faces de la même pièce dès lors qu'il ne s'agit pas de spéculation intellectuelle (au sens noble de la recherche scientifique des facteurs qui déterminent un autre facteur) mais d'action publique à mettre en œuvre.

Certes, ces deux mondes ne sont pas complètement isolés l'un de l'autre : les politiques publiques peuvent être décrites sous l'angle d'une construction intellectuelle, celui d'un référentiel (MULLER, 1990).

Mais, pour autant qu'il en existe un en matière de politique de sécurité, si l'on s'intéresse à la mise en œuvre pratique, il s'agit de réfléchir à des moyens d'action qui correspondent à ce que les pouvoirs publics peuvent raisonnablement faire à court terme et en prenant en compte les impératifs liés à l'existence de mandats électifs (compétences, ressources, temporalités, groupes de pressions etc.).

#### *Importer la tolérance zéro ?*

Que penser des politiques menées à New York ? Et, surtout que penser de

ces politiques comme modèles pour la France ? La présentation française de la politique menée par certaines villes américaines par la presse a fait la part belle à la « tolérance zéro » ainsi qu'à la gestion policière par objectifs (le système COMPSTAT). Si le COMPSTAT (SIVERMAN, 1996) est une vitrine technologique (les crimes et délits sont informatisés d'une semaine sur l'autre, les actes peuvent être localisés sur des écrans géants dans une salle de contrôle et de commandement, mis en relation avec d'autres données sociales ou économiques, etc.), cette technique s'est accompagnée d'autres modifications qui sont rapportées par W. Bratton (1995) ou par G. L. Kelling et C. M. Coles<sup>11</sup>.

La thèse qui sous-tend la politique est assez connue des spécialistes depuis l'article séminal de J. Q. Wilson et G. H. Kelling en 1980 : elle lie la multiplication des désordres et la montée de la criminalité violente, insistant sur le rôle de régulation sociale que la police peut jouer si elle change sa logique d'action. Le premier défi que se donnent les responsables du métro de New York est de reconquérir 26 lignes s'étalant sur 360 kilomètres et 465 stations dans lesquelles 3,5 millions d'utilisateurs passent chaque jour ouvré<sup>12</sup>. Le problème a été attaqué sous l'angle des graffitis et autres désordres qui furent connus sous le nom du « problème des sans abri » (*the homeless problem*). Il y avait des

mendiants inoffensifs et paisibles, mais aussi des drogués sous l'emprise de substances illégales. Les incivilités étaient légion : des personnes saoules, vomissant, urinant, déféquant ou prenant de la drogue en public, ou insultant des passagers. La fraude contribuait également à créer un climat d'absence de règle, soit le fait de voir des jeunes sauter par-dessus les tourniquets, ou s'en prendre aux distributeurs de billets, ou encore de rendre des « services » comme de tenir la porte ouverte en échange du prix du transport.

En avril 1990, William Bratton était recruté pour conduire le *Transit Police Department*. Les responsables ont tenté de comprendre la situation, la nature des problèmes rencontrés (BRATTON, 1995). Par exemple « au lieu de considérer que les graffitis étaient un problème légal (*law enforcement problem*), le responsable de la gestion du Métro comprit qu'il s'agissait d'un mélange complexe de vandalisme, de piètre maintenance, de manque de *leadership* et de manque de résolution ». (KELLING, COLES, 1996, p. 117). Les départements furent réorganisés territorialement, et non plus fonctionnellement de manière à identifier un responsable par station. Ils décidèrent d'appliquer les réglementations de manière ferme, sans compromission, et affirmèrent que les utilisateurs du métro devaient suivre les règles du métro. Une des difficultés consista à

•••(11) Kelling a été conseiller du *New York Transportation Police Department*.

(12) L'avantage du métro new-yorkais est de se trouver dans une seule municipalité, et donc sous une autorité unique.

obtenir les autorisations légales de la part des juges de la Cour Suprême. Une autre à convaincre les policiers que la réduction des désordres faisait partie de leurs missions. Leur nombre était tel que les procédures furent rationalisées et accélérées. Une des choses qui convainquit les policiers du lien entre désordre et criminalité était le fait que, dans certains voisinages, on pouvait trouver jusqu'à une personne interpellée sur dix qui était porteuse d'une arme illégalement détenue ou qui était recherchée pour un crime (KELLING, COLES, 1996, p. 134). Les arrestations pour des actes de petite délinquance, tout comme les éjections hors du métro augmentèrent rapidement dès cette date. Les statistiques disponibles présentent la diminution de la criminalité après le pic de 1990. Dans le métro, cette diminution est nette pour les crimes dans leur ensemble, et notamment les vols avec usage de la force ou menace de l'utiliser mais également la fraude (d'après la police, le nombre de fraudeurs passe de 200 000 à 25 000, les délits diminuent de 80%). Ces réformes dans le métro allaient constituer le modèle de celles qui allaient être appliquées à la police de New York, sous la direction de W. Bratton.

Pour l'ensemble de la ville de New York, les vols avec usage de la force ou menace de l'utiliser et les homicides régressent, tout comme les agressions quoique de manière moins spectaculaire<sup>13</sup>. Il en va de même pour les

atteintes à la propriété comme les cambriolages (entrées illégales dans le but de commettre un délit) et les vols. Ces deux derniers types d'atteintes ayant atteint leur maximum dès 1988. Nous savons que cela se poursuit aujourd'hui, après le départ de W. Bratton et nous allons y revenir à propos des homicides. Certes, il y a un passif de ces politiques qui envoient les policiers dans les rues. En France et aux États-Unis, on a dénoncé l'usage abusif de la force (BODY-GENDROT, 1998, p. 123). S'il n'est pas avéré dans la phase métro, il l'est pour la ville. Si les populations défavorisées souffrent des mauvaises pratiques policières, elles sont les premières bénéficiaires de la baisse du taux d'homicidité. C'est sans doute pourquoi, à New York, les noirs votent plus pour les Républicains qu'ils ne l'ont fait depuis plusieurs élections, et que sur la sécurité leur opinions sur la politique de Giuliani rejoignent en satisfaction celles des autres communautés.

Y a-t-il un rapport de cause à effet entre la baisse de la criminalité et les politiques de sécurité développées dans le métro et dans la ville de New York ? Cet effet est-il aussi direct et profond que le prétendent certains ? Peut-on faire de la lutte contre les désordres le point clé de la reconquête des quartiers invivables ? Bien sûr, certains auteurs ont montré statistiquement une association entre fréquence des incivilités et cambriolages pour les quartiers résidentiels (SKOGAN, 1990), mais de

•••(13) Indications données par KELLING et COLES, 1996, p. 152-154 ; elles sont confirmées par Body-Gendrot qui cite en référence les travaux de REMNICK et LARDNER sur les évolutions entre 1990 et 1996.

manière statique et non par l'analyse des évolutions. Il est, d'un strict point de vue scientifique, très difficile d'établir si la lutte contre les désordres et incivilités a un « effet propre » (au sens statistique) sur la délinquance violente, c'est-à-dire indépendamment des autres variables contextuelles (comme il est d'ailleurs périlleux de tenter d'attribuer d'une manière générale les variations de la délinquance et de la criminalité à un seul facteur). Il y a du chemin entre parler des désordres comme « contribuant à » ou comme « déterminant » par eux seuls quelque chose. N'y a-t-il pas une surestimation de l'effet net de la lutte contre les désordres sur le niveau global de la criminalité (BOUZA, 1997 ; KARMEN, 1996) ?

Peut-on trancher ? D'une part, la baisse du nombre d'homicides à New York est une réalité forte qui se poursuit jusqu'en 1998 avec 606 homicides décomptés (et nous ramène à un niveau égal à celui connu en 1964). Certes, la comparaison dans le temps montre que cette baisse se produit ailleurs. Par exemple, à Washington, on comptait 489 homicides en 1991, 397 en 1996 et 301 en 1997. À Los Angeles, on dénombrait 574 homicides en 1977, 709 en 1996 et 566 en 1997 soit un retour en dessous du niveau le plus bas depuis 20 ans. L'évolution du nombre d'homicides dans une ville libertarienne comme San Francisco, dont J. Q. Wilson a dit que sa police était l'une des moins agressives, suit donc la

même tendance que pour le modèle que constitue New York<sup>14</sup>. En revanche, à Détroit, la tendance se renverse et on compte 454 meurtres en 1997 contre 428 en 1996<sup>15</sup> : il s'agit du seul cas d'augmentation dans l'ensemble des dix plus grandes villes américaines. Il faut pouvoir regarder l'évolution des cinq ou six dernières années dans les villes de plus de 100 000 habitants pour dire si New York a connu, au total, une diminution de la fréquence des homicides plus importante qu'ailleurs. Il semble bien que la réponse à la question soit positive. Certes, entre 1991 et 1997, des villes comme Dallas et Houston ont connu des baisses du nombre d'homicides de près de 50%. Mais, à New York, nous sommes très loin du niveau atteint en 1992 avec 2 262 meurtres recensés, avec homicides en 1997 ; cela constitue une baisse de 66% environ (et même 73% avec les chiffres de 1998). De plus, on sait que pour l'ensemble des États-Unis, la baisse n'est pas aussi spectaculaire : entre 1990 et 1996 on passe de 23 440 à 19 650 meurtres, soit une baisse de 16% « seulement » contre 56% pour New York sur la même période. Même en prenant la période la plus favorable à la décrue nationale, soit 1993-1996, on trouve une baisse nationale moyenne de 23%. Notons que le bilan de New-York, ville qui pèse d'un poids lourd dans la criminalité, a influencé les résultats au niveau de la moyenne pour les grandes villes américaines.

•••(14) Interview donné, à l'occasion de la publication des chiffres du FBI au *New York Times*, 2 Juin 1997

(15) Chiffres données par Xinhua News Agency, 30-12-1997.

En conséquence de quoi, s'il est assez peu probable que le fait de « réparer les fenêtres » ait pu, à lui tout seul, faire diminuer d'une telle manière et ramener le nombre d'homicides à un niveau inconnu depuis 1973, il faut dire que la lutte contre les incivilités à New York doit bénéficier d'un *a priori* positif puisque cette ville a connu une diminution de la fréquence des homicides bien supérieure à l'ensemble du pays. Cela n'implique pas d'ailleurs que la politique de New York soit la seule à être susceptible de contribuer à obtenir des résultats, comme le montrent par exemple d'autres travaux sur Chicago (MORENOFF, SAMPSON, 1997).

Enfin, la vitesse de ces transformations, quelles que soient leurs causes, suggère de ne pas surestimer le poids des variables sociologiques présentées comme explicatives par les analyses quantitatives de la délinquance en coupe synchronique.

#### DES POLITIQUES IMPORTABLES EN FRANCE ?

Les États-Unis sont un modèle repoussoir en ce qui concerne le niveau de violence, mais ils sont un modèle attractif pour ce qui est des évolutions de la criminalité. C'est d'ailleurs pourquoi les expériences américaines sont autant présentées et débattues dans la presse, mais également dans les enceintes spécialisées (IHESI, Gendarmerie, École des commissaires de St Cyr au mont d'Or, Union nationale des éducateurs spécialisés, etc.).

•••(16) Dans l'hexagone, voir les données de deux sondages locaux sur des villes moyennes et grandes, analysées par ROCHÉ, Y a-t-il une vitre française cassée?, (à paraître en 1999) .

Pour comprendre l'intérêt du monde occidental pour ces méthodes, on ne pourra donc pas se contenter de la thèse qui fait du management un sous produit du « génie américain du *marketing* » (BRODEUR, 1997). S'il y a un « modèle français » à défendre, c'est sans doute plus un modèle prospectif (la fameuse politique de la ville) que celui qui a été mis en œuvre et accompagné, depuis 1984-85, d'une augmentation rapide des violences contre les personnes, à l'exception des homicides.

Les baisses de la criminalité posent des questions quant aux approches institutionnelles de la sécurité. Et, notamment sur la transposabilité de l'approche à la France, sur les définitions de la prévention et des modes d'action policiers.

#### LA SPIRALE DU RENOUVEAU : BLOCAGE OU RÉVERSION

Il faut être tout à fait modéré dans l'acceptation ou le refus *a priori* de la théorie positive de la vitre cassée sous prétexte de différences « culturelles », au sens d'établies une fois pour toutes, entre la France et les États-Unis.

Il nous semble qu'il y a deux versants dans la théorie de la vitre cassée, le positif et le négatif. Le versant négatif, la spirale du déclin, est balisé empiriquement (plus de désordre engendre plus de peur, et de crime<sup>16</sup>).

En revanche, le versant positif, que nous proposons d'appeler la spirale du renouveau, (moins de désordre engendre moins de peur, et de



crime) demande sans doute à être mieux connu scientifiquement, même si les résultats de New York peuvent être estimés suffisants par certains acteurs opérationnels pour orienter des politiques.

Peut-être faut-il, à nouveau, distinguer deux cas de figure quant au versant positif de la théorie de la spirale du renouveau. Il y aurait, d'une part, le cas où contenir les désordres et incivilités dans un contexte où le crime est rare permet d'empêcher la délinquance et la criminalité de se répandre (hypothèse du blocage), et d'autre part le cas dans lequel réduire la fréquence des désordres permet d'espérer une baisse de la délinquance et la criminalité (hypothèse de la réversion). Trouver des facteurs pour bloquer une évolution ne revient peut-être pas nécessairement à trouver des facteurs qui provoquent une réversion de l'évolution.

Ces deux phénomènes n'étant pas les mêmes, il convient de ne pas les accueillir ou les repousser dans un même mouvement. Le second cas de figure (hypothèse de la réversion) a fonctionné aux États-Unis pour plusieurs raisons.

D'abord, parce que l'accent mis sur les comportements dans les espaces collectifs contrait l'économie de la drogue. L'agressivité en public avait pour fonction d'asseoir les carrières de *dealers*, la « tyrannie de la minorité » permettant de contrôler les lieux (BOURGEOIS, 1995).

Ensuite, parce que la structure des homicides aux États-Unis est liée à la

recherche illégale de profits, rappelons que seuls 10% des homicides sont familiaux : les meurtres dans les espaces publics motivés par la réalisation d'un vol sont maintenant l'immense majorité. Dans ces deux cas, la présence policière a permis d'endiguer le phénomène. En France, le contexte est différent. D'abord, le niveau d'homicide est bien plus limité, faut-il le rappeler. Ensuite, à la même date, en 1994, les homicides non crapuleux représentent plus de 75% du total : la criminalité reste encore très majoritairement relationnelle et familiale dans notre « vieux pays », en dépit des évolutions manifestées par les mineurs. Pour ces deux raisons, nous sommes, en France, dans le premier cas de figure (hypothèse du blocage et non de la réversion).

Il est d'ailleurs plus facile à mettre en œuvre. C'est pour cela qu'il devrait retenir l'attention des autorités françaises, en sachant qu'on ne peut en attendre une baisse du taux d'homicidité. La lutte contre les incivilités pourrait donner des résultats positifs en France sur la délinquance non-homicide : les agressions, les vols, les cambriolages. Mais encore une fois, s'il s'agit d'une piste qui, à notre sens, mérite d'être explorée en France, on ne peut transposer mécaniquement le modèle new yorkais. La dimension répressive, tout à fait incontournable, ne peut être autant développée qu'aux États-Unis : chez nous, le crime violent est moins présent.

De plus, les organisations en charge de la sécurité ne sont pas les mêmes. Ici, les polices ne sauraient être

l'unique et principal vecteur de la reconquête des espaces collectifs à la fois pour des raisons pratiques (effectifs, budgets, compétences, rôles professionnels) et politiques : les polices américaines sont municipales, et donc répondent, à travers l'élection du maire, plus directement aux demandes de la population ; ce dernier a des latitudes quant à l'organisation des polices et leur mode de travail que n'ont pas leurs homologues français.

#### PRÉVENTION ET CITOYENNETÉ

Cela dit, plusieurs aspects de la spirale du renouveau peuvent être tirés de politiques visant à la réversion pour inspirer une politique de blocage. Les enjeux sont semblables. Ils concernent à la fois la prévention et la citoyenneté.

L'approche par les désordres se situe du côté des entrées préventives, tout en se voulant offensive - c'est le terme utilisé pour la désigner par ses promoteurs - et en se démarquant ainsi d'autres préventions. Depuis une dizaine d'années, l'extension de la prévention rend sa définition délicate (GRAHAM, 1990). Il est cependant un point qui peut être mentionné pour rassembler ceux qui se placent du côté de la prévention. Les auteurs qui se soucient de la prévention réfléchissent en terme d'impact sur la délinquance, et non en terme « d'efficacité » à court terme mesurée par des statistiques organisationnelles (charge de travail

par exemple, vitesse de réponse à un incident par les policiers). Cela dit, les préventions se distinguent les unes des autres. À côté de la prévention spécialisée et de la prévention sociale globale, deux grandes préventions émergent depuis les années quatre-vingt. La prévention situationnelle, qui est certainement beaucoup plus orientée vers la technique et la technologie : le paradigme utilisé est celui de l'acteur - délinquant rationnel cherchant à maximiser le rapport coût-avantage : avec le durcissement des cibles on rend leur accès plus difficile ou plus risqué, bref plus coûteux et donc moins profitable et par là même moins probable. Ensuite la prévention liée à la prise en charge des désordres. Cette dernière insiste plus sur les incitations diffuses que transmet un environnement dégradé, d'une part, à passer à l'acte pour certains et, d'autre part, à s'en éloigner pour les citoyens respectueux de la loi. Toutes les deux sont critiques par rapport au système pénal, et à la croyance suivant laquelle la punition après coup serait, à elle seule, de nature à dissuader et empêcher la délinquance. Mais la lutte contre les désordres insiste sur le rôle des citoyens en tant que citoyens, alors que la prévention situationnelle insiste plus volontiers sur la précaution du propriétaire. Si l'on entend par là qu'elle s'ouvre au citoyen (à ses demandes), il y a donc incontestablement une dimension citoyenne dans la prévention de la

••••(17) Il ne s'agit pas de promouvoir les milices (c'est l'expression consacrée en France, les Américains parlent de *vigilantism*), il s'agit d'ailleurs d'un phénomène extrêmement rare aux États-Unis en dépit de la fréquence des crimes. Sur la définition du phénomène, voir JOHNSTON (1996).

criminalité par la lutte contre les désordres<sup>17</sup>. L'idée centrale concomitante est que les policiers doivent travailler en étroite symbiose avec les collectifs. Or, la culture policière est orientée par l'idée d'un professionnalisme qui se construit à partir d'une rupture entre les citoyens (profanes) et les agents de sécurité (professionnels). Par opposition, le diagnostic des spécialistes est que faire régner la tranquillité publique et résoudre les problèmes des citoyens sont, au mieux, perçus comme des fonctions périphériques perturbantes, et au pire, comme du travail social peu digne d'intérêt. Cela est avéré dans les pays occidentaux (en France, MONJARDET, 1996 ; en Grande-Bretagne, HORTON et SMITH, 1988). Aux États-Unis, la motorisation des patrouilles dotées également de radios a été la première marche de l'escalier qui conduit à la coupure entre police et population (SKOGAN, 1990) et le système centralisé des appels par le numéro de téléphone 911 constitue le parangon de la transformation du travail policier depuis 1945. Les citoyens et les officiers de police sont de plus en plus étrangers l'un à l'autre. Pour le résumer d'une phrase, la patrouille de police en voiture permet d'arriver rapidement sur les lieux du crime après coup, mais ne permet pas de prévenir la violence

par une interconnaissance ancrée dans la vie quotidienne. Le travail policier sur les désordres s'inscrit, de ce point de vue, à contre-courant.

Les préventions peuvent être plus ou moins « offensives » au sens de volontaires et liées organiquement au travail policier. La lutte contre les désordres est la forme la plus offensive ; elle suppose un travail policier actif<sup>18</sup>, en direction des usagers. Les populations marginales, disent les contempteurs, sont visées, tandis que les défenseurs disent que ce sont les comportements inacceptables en public. Mais, toujours, la lutte contre les désordres s'appuie sur la communauté, c'est-à-dire une collectivité particulière dans un univers urbain très ségrégué spatialement, et un ordre social local au sens où la loi ne saurait le définir complètement en elle-même sans prendre en considération les interactions qui font exister des règles. On comprend tout de suite quelles pourraient être les perversions d'un tel argument puisque ceux qui commettent les désordres sont plus souvent des pauvres ou des sans abri. La police, en se focalisant sur les désordres, pourrait s'en prendre aux pauvres et aux exclus. C'est pourquoi, il faut particulièrement veiller à ne pas orienter le travail policier dans cette direction.

•••(18) Elle est pratiquée dans des villes de différentes taille comme New York certes, mais aussi comme Princeton. Dans le district (*Borough*) de Princeton, le responsable de la police, Chief Michaud, a expliqué comment la philosophie de la police communautaire, que son département avait embrassée, encourageait les officiers à rechercher des solutions de long terme et que cela supposait de passer plus de temps avec ceux qui vivent des conflits ou besoin d'aide. Cela inclut la sensibilisation des écoliers à l'usage de drogue dans les écoles, les patrouilles à pied (*Status Report on Police Service* cité par *Princeton Town Topics*, vol LI-14, 11 Juin 1997).

Il faut noter que cette notion de collectivité locale est à l'opposé de l'universalisme que les élus chérissent, et de la répulsion que leur provoque toute communauté organisée dans un autre but que celui de faire de la politique (syndicats, partis). Il est presque tabou de parler des régulations communautaires, qu'elles soient religieuses ou ethniques. Ces affiliations seraient négatives et anti-républicaines : si elles apparaissent malgré tout, elles sont perçues comme devant être secondaires et subordonnées à celle de l'identité nationale (voir les difficultés de proposer une version douce du multiculturalisme en France : WIEVIORKA, 1996). Cela explique sans doute l'accent mis, dans l'hexagone, sur les dispositifs politiques utilisant des découpages spatiaux, ces zones (d'éducation, franchises, etc.) qui permettent de cibler des populations sans les nommer. Une limite à la prise en charge des incivilités dans notre pays réside probablement dans la méfiance que les professionnels de la sécurité et de la politique ont vis-à-vis de la participation de la population ou même de la satisfaction de leurs attentes en matière d'insécurité : la ségrégation spatiale ayant croisé les critères économiques et les origines nationales, il est fatal que les acteurs collectifs locaux en soient le reflet dès lors qu'ils ne se recrutent pas uniquement dans les couches moyennes.

## LE DROIT À LA PARTICIPATION

Un premier enjeu quant à la participation des citoyens à leur sécurité consiste à leur permettre d'influencer le système politique, et pour les responsables publics, d'écouter les citoyens dans la définition de leurs politiques. Y a-t-il une réelle possibilité que les citoyens soient associés à la gestion de la sécurité dans nos démocraties de marché ? Cela recouvre un problème plus vaste, celui de savoir si le citoyen a non seulement des droits attribués par l'État, mais se trouve également en mesure d'avoir la légitimité de juger de ces droits.<sup>19</sup> Et, par défaut, comment faire en sorte que les professionnels publics se tournent vers leurs demandes, et notamment vers les résolutions de conflits, les incivilités et désordres qui restent largement relégués au second plan ?<sup>20</sup> Cela est encore plus crucial en France qu'aux États-Unis, parce que les désordres représentent une bonne part des problèmes des habitants et ne sont pas des faits associés à la criminalité violente.

Un second enjeu porte sur les relations entre la police et la population. La lutte contre l'insécurité nécessite l'exercice de la citoyenneté, à la fois pour soi mais aussi pour aider à assurer la sécurité des autres. Kelling et Coles posent que, dans une démocratie, « les citoyens policiers et la police citoyen-

••• (19) Dans un autre registre empirique, mais avec les mêmes remarques, voir le travail de Lucien Jaume sur les paradoxes du libéralisme français (1997).

(20) La question n'est pas encore perçue dans toutes ses dimensions. Et cela en dépit de la médiatisation du phénomène qui semble poindre, et de l'existence de politiques municipales et de déclarations des actuels ministres de l'Intérieur et de l'Éducation nationale.

ne» (*the citizens as police and police as citizens*) constituent une figure qui encourage « *la tolérance pour les différences et les efforts des citoyens pour maîtriser les personnes irrespectueuses et les prédateurs* » (1996, p. 9). Cette réflexion est tout à fait centrale. Sauf à proscrire d'un côté ce qui est officiellement jugé nécessaire d'un autre, la figure de la milice ne peut durablement servir de repoussoir à l'implication des citoyens qui le désirent. Si la sécurité est « l'affaire de tous », cela implique une participation sous une forme qui satisfasse les citoyens et pas seulement les institutions publiques, le rôle citoyen ne sera que passif s'il est entièrement déterminé d'en haut. Ensuite, sans nécessairement faire de la police l'outil essentiel de recours, on ne peut se satisfaire de l'idée que la tolérance pour les comportements gênants, et dont les conséquences sociales négatives sont fortes, soit la solution à ces comportements. Bien au contraire, la tolérance, au nom de la liberté, vis-à-vis de tous les désordres qui ne sont pas violents doit être questionnée. Cette tolérance, souvent rappelée solennellement par les intellectuels aux couches défavorisées, contribue à alimenter la ségrégation spatiale par le départ de ceux qui se

sentent illégitimes à combattre sur place les désordres.

Un dernier enjeu réside dans la reconnaissance ou non des collectifs d'individus dans l'affirmation d'un ordre social local, d'une morale affichée dans l'espace public. Les formes collectives non universalistes prennent une place importante dans les États-nations européens alors que les théories de la modernisation leur avaient enlevé toute pertinence dans les années soixante. Le modèle d'une démocratie pluraliste se mêlant à celui d'une république intégratrice ne saurait faire autrement que de se traduire par des conséquences sur la manière dont les citoyens conçoivent leur sécurité, mais aussi dont les polices l'assurent, recrutent leurs personnels. Ainsi, on doit se demander pourquoi les personnes d'origine étrangère sont si nombreuses dans les entreprises de sécurité et si présentes dans les forces publiques. Mais, ce débat en est encore à ses prémices, les affrontements politiques ayant lieu sur les principes (le droit à la sécurité), sur la question de la réaffirmation de la frontière des États de l'Union et sur l'attribution de la nationalité qui garantirait une homogénéité interne et les capacités de régulation des pouvoirs publics.

■ **Sebastian ROCHÉ**

*Chargé de recherche au CNRS, CERAT,  
Grenoble.*

## BIBLIOGRAPHIE

- ARCHER (D.), GARDNER (R.), 1984, *Violence and Crime in Cross-National Perspective*, London, Yale University Press.
- AUBUSSON DE CAVARLAY (B.), 1997, «La place des mineurs dans la délinquance enregistrée», *Les cahiers de la sécurité intérieure*, n°29, p. 17-38.
- BARREYRE (J. Y.), 1992, *Les loubards*, Paris, L'Harmattan.
- BARRE (M. D.), 1994, *Toxicomanie et délinquance. Du bon usage de l'usager de produit illicite*, Rapport pour le ministère de la Justice, Paris, CESDIP.
- BENNET (W.J.), DILULIO (J. Jr), WALTERS (J. P W.), 1996, *Body Counts*, New York, Simon and Schuster.
- BLAU (J.), BLAU (P.), 1982, «The cost of inequality: metropolitan structure and violent crime» *American Sociological Review*, n°47-1, p. 114-129.
- BLOCK (M.K), TWIST (S. J.), 1994, *Incarceration works*, *Commonsense*, vol 1, spring.
- BODY-GENDROT (S.), LE GUENNEC (N.), HERROU (M.), 1998, *Mission sur les violences urbaines*, Paris, La Documentation Française, 155 p.
- BONFILS (P.), 1996, «Pourquoi la criminalité a-t-elle baissé au cours des années 80? Le cas français», *Revue Internationale de criminologie et de police technique*, vol XLIX, 2, p. 192-213.
- BORDET (J.), 1998, *Les jeunes de la cité*, Paris, PUF.
- BOURGEIS (P.), 1995, *In Search of Respect : Selling Crack in El Barrio*, New York, Cambridge University Press.
- BOUZA (T.), 1997, «Nypd Blues: Good, Lucky or Both ?», *Law Enforcement News*, vol XXIII, n°460, January 31, p. 8-9
- BRATTON (W.), 1995, «The New York City Police Department's Civil Enforcement of Quality of Life Crimes», *Journal of Law and Policy*, p. 447-464.
- BRODEUR (J. P.), 1997, «La police en Amérique du Nord: modèles ou effets de mode», *Cahiers de la sécurité intérieure*, n°28, p. 171-184.
- CASTELLAN (M.), GOLDBERGER (M. F.), MARPSAT (M.), 1992, «Les quartiers prioritaires et la politique de la ville», *INSEE première*, n° 234.
- CHAILLOU (P.), 1995, *Violence des jeunes*, Paris, Gallimard.
- CHARLOT (B.), EMIN (J.-C.), 1997, *Violence à l'Ecole, l'état des savoirs*, Paris, Armand Colin.
- CLARKE (R.), 1980, «Situational crime prevention: theory and practice», *British Journal of Criminology*, n°20, p. 136-47.
- COURTWRIGHT (D. T.), 1996, *Violent Land, Single Men and Social Disorder from the Frontier to the Inner City*, Harvard University Press, Cambridge, Massachusetts.
- CUSSON (M.), 1990, *Croissance et décroissance du crime*, PUF, Paris.
- CUSSON (M.), 1998, *Criminologie Actuelle*, PUF, Paris.
- DONZIGER (S. R.), (dir.), 1996, *The Real War on Crime, The Report of the National Criminal Justice Commission*, New York, Harper Perennial.
- DUPREZ (D.), KOKOREFF (M.), 1997, *Trafics de drogue et quartiers pauvres, cinquèmes journées de l'IFRESI*, Lille, 23-24 mars.
- EISNER (M.), 1995, «Crime and Economy, proceedings of the 11th Criminological Colloquium (1994)», *Criminological Research*, Vol XXXII, p. 13-51.
- FLEISHER (M. S.), 1995, *Beggars and Thieves, Lives of Urban Street Criminals*, Wisconsin, The University of Wisconsin Press.
- FOX (J. A.), 1996, *Trends in Juvenile Violence*, Bureau of Justice Statistics, March.
- GODARD (F.), 1997, *Le gouvernement des villes*, Paris, Descartes et Cie.
- GRAHAM (J.), 1990, *Crime Prevention Strategies in Europe and North America*, Helsinki, HEUNI, n° 18.

## BIBLIOGRAPHIE

- HIRSCHI (T.), 1969, *Causes of Delinquency*, Berkeley, University of California Press.
- HORTON (C.), SMITH (D.), 1988, *Evaluating Police Work. An action Research Project*, London, Policy Studies Institute.
- HYDEN (G.), 1992, « Governance and the Study of Politics » in HYDEN (G.), BRATTON (M.), (dir.), *Governance and Politics in Africa*, Boulder and London, Lynne Rienner Publishers.
- INSEE, Données sociales, 1993, *La société française*, Paris.
- JAUME (L.), 1997, *L'individu effacé ou le paradoxe du libéralisme français*, Paris, Fayard.
- JOHNSTON (L.), 1996, « What is Vigilantism », *British Journal of Criminology*, n°36-2, p. 220-236.
- KARMEN (A ), 1996, « What's Driving NY's Crime Rate Down? Is Improved Policing Responsible for the Sharp Drop in Murder Rates? », *Law Enforcement News*, vol XXII, n°456, January 31, p. 8-10
- KELLING (G. L.), COLES (C. M.), 1996, *Fixing Broken Windows, Restoring Order and Reducing Crime in Our Communities*, New York, The Free Press.
- KELLING (G. L.), WILSON (J. Q.), 1994, « Vitres cassées », *Les Cahiers de la sécurité intérieure*, n°15, p. 163-180
- KILLIAS (M.) et alii, 1995, *European Sourcebook of Crime and Criminal Justice Statistics*, Council of Europe, Draft Model version 9.
- LANE (R.), 1989, « On the Social Meaning of Homicide Trends in American » in GURR T R (dir.) *Violence in America: the History of Crime*, Newbury Park, California, volume 1, p. 55-79.
- LE GALES (P.), 1995, « Du gouvernement urbain à la gouvernance urbaine », *Revue française de science politique*, n°1.
- LEPOUTRE (D.), 1997, *Cœur de banlieue*, Paris, Odile Jacob.
- MANN (C. R.), 1993, *Unequal Justice, a Question of Color*, Indianapolis, Indiana University Press.
- MONJARDET (D.), 1996, *Ce que fait la police, sociologie de la force publique*, Paris, la Découverte.
- MORENHOF (J.), SAMPSON (R. J.), 1997, « Violent Crime and Spatial Dynamics of Neighborhood Transition in Chicago, 1970-1990 », *Social Forces*, vol 76-1, p. 31-64.
- MULLER (P.), 1990, *Les politiques publiques*, Paris, PUF.
- PUMAIN (D.), GODARD (F.), *Données Urbaines*, Paris, Anthropos.
- ROBERT (P.), ZAUBERMAN (R.), 1991, *Enquêtes locales de victimation, deux tests en milieu urbain*, Paris, CESDIP.
- ROBERT (Ph.), ZAUBERMAN (R.), POTTIER (M L.), LAGRANGE (H.), 1998, « Enquêtes de victimations et statistiques policières (1985-1995) », *Questions Pénales*, décembre, XI.5, p. 1-4.
- ROCHÉ (S.), 1998a, *Sociologie Politique de l'Insécurité*, Paris, PUF.
- ROCHÉ (S.), 1998b, « Déviances et délits », in GALLAND (O.), LEMEL (Y.) (dir), *La Nouvelle société française, tendances et mutations*, Paris, Armand Colin, p. 245-275.
- ROCHÉ (S.), 1994, *Insécurité et Libertés*, Paris, Seuil.
- RUBINSTEIN (D.), 1992, « Don't blame crime on Joblessness », *Wall Street Journal*, Novembre 13.
- RUSSELL (D.), WARNER (B.), 1995, « Fairhill: city's Deadliest Turf in 1994 », *Philadelphia Daily News*, January 9, p. 4-5.
- SIVERMAN (E. B.), 1996, « Mapping Change: How the NYPD Re-Engineered Itself to Drive Down Crime », *Law Enforcement News*, vol XXII, n°457, December 15, p10-12.
- SKOGAN (W.), 1990, *Desorder and Deline : Crime and the spiral of Decay in American Neighborhoods*, New York, Free Press.
- SKOGAN (W.), 1979, « Crime in Contemporary America », in GRAHAM (H.), Gurr (T.) (dir.), *Violence in America: Historical and Comparative Perspectives*, Beverly Hills, California, Sage.

## BIBLIOGRAPHIE

- SMITH (D.), 1995, *Crime Prevention, the National Picture*, communication donnée lors de la «Crime Concern Scotland Annual Conference», 25 May, 8 pages.
- SVENSSON (B.), 1986, «Welfare and criminality in Sweden», in HEAL (K.), LAYCOCK (G.) (dir.), *Situational crime prevention: from theory into practice*, London, 1986, p.113-22.
- US DEPARTMENT OF JUSTICE, 1996, *Sourcebook of Criminal Justice Statistics*, Whashington, Bureau of Justice Statistics.
- VAN DIJK (J.), 1991, «More than a Matter of Security: Trends in Crime Prevention in Europe», in HEIDENSOHN (F.), FARRELL (M.) (dir.), *Crime in Europe*, London, Routledge, p.27-42.
- WACQUANT (L.), 1998, «L'ascension de l'Etat Pénal en Amérique», *Actes de la Recherche en Sciences Sociales*, 114, p.7-26.
- WIEVIORKA (M.) (dir), 1996, *Une société fragmentée ? : le multiculturalisme en débat*, Paris, La découverte, 320 p.
- WILSON(J.), HERRENSTEIN (R.), 1985, *Crime and Human Nature*, New York, Simon and Shuster.
- WILSON (J.), 1985, *Thinking About Crime*, New York, Vintage Books Ed, 1<sup>re</sup> ed en 1975, ed révisée en 1983.
- ZAUBERMANN (R.), 1998, «Le gendarme comme juge», *Sociologie du travail*, XL-1, p.43-64.



# LA MOSAÏQUE DE L'EXPERTISE JUDICIAIRE : ENTRE PUBLIC ET PRIVÉ, MONOPOLE ET CONCURRENCE

— par Laurence DUMOULIN

Le marché français de l'expertise judiciaire a la spécificité d'être particulièrement éclaté entre une multitude d'acteurs et d'instances capables de produire, à destination de ce commanditaire particulier qu'est l'institution judiciaire, les savoirs et savoir-faire contextualisés qui fondent l'expertise, depuis les sciences de l'ingénieur jusqu'aux empreintes génétiques. Si les producteurs d'expertise judiciaire s'organisent autour de la dichotomie classique public/privé, on assiste également au brouillage de ces repères : public et privé se dissolvent et s'interpénètrent pour faire de la production d'expertise une mosaïque complexe et kaléidoscopique.

Notes et études

233

L'absence de centralisation, l'éclatement et la diversité des producteurs d'expertise ont de quoi surprendre dans un domaine comme celui du judiciaire<sup>1</sup>. On pourrait imaginer, dans ce secteur en lien avec les fonctions régaliennes sans doute les plus emblématiques de l'État - la justice et la police - un système très rationalisé, étroitement organisé et centralisé autour de quelques structures qui, bien que plus ou moins spécialisées dans leurs compétences, fonctionneraient selon un modèle statutaire unique. La réalité est bien plus complexe. Le dispositif de production d'expertise judiciaire est

caractérisé par sa variété, son hétérogénéité, voire son anarchie.

Pour distinguer et spécifier chacun des organes qui participent du dispositif de production d'expertise, plusieurs dimensions sont pertinentes : la dimension identitaire<sup>2</sup>, la dimension disciplinaire<sup>3</sup>, la dimension territoriale<sup>4</sup> et la dimension procédurale<sup>5</sup>.

D'une utilité et d'une fonctionnalité incontestables pour une première approche analytique, cette caractérisation met en lumière et restitue quelques uns des principaux axes de polarisation qui structurent le dispositif de production d'expertise. Mais cette grille de lecture ne prend véritablement son sens et

- (1) L'auteur tient à remercier toutes les institutions et personnes qui l'ont aidé dans l'accès particulièrement difficile aux sources, en particulier l'INHSJ, le Laboratoire central de la Préfecture de police de Paris et le Laboratoire de police scientifique de Paris.
- (2) Entendue comme l'appartenance à un ensemble professionnel structuré et structurant, comme la référence à une identité professionnelle forte. Trois ensembles peuvent alors être distingués : le corps médical, le corps militaire et le corps policier.
- (3) Entendue comme l'appartenance à un champ disciplinaire, comme la mise en œuvre de savoirs spécifiques. Trois ensembles sont alors significatifs : le savoir médical, le savoir criminalistique et le savoir social.
- (4) Entendue comme la référence au secteur d'intervention des différentes structures. Trois niveaux d'intervention apparaissent : le local, le national, le local et le national.
- (5) Entendue comme la nature de la procédure dans laquelle intervient chaque type de producteur d'expertise. Là encore, trois champs : le civil, le pénal, le civil et le pénal.

sa pertinence que si on lui adjoint une dimension supplémentaire, la dimension public/privé autour de laquelle s'organise une approche problématique de la question de l'expertise judiciaire.

La distinction public/privé apparaît « *comme une catégorie de pensée constitutive de l'imaginaire des sociétés occidentales* ». C'est ce « *schéma de perception du réel doté de force agissante à travers les représentations qu'il suscite et les pratiques qu'il inspire* »<sup>6</sup> qu'il peut être fructueux de mettre en résonance avec le champ de l'expertise judiciaire. En effet, au-delà du caractère de référence pour l'analyse de l'organisation des sociétés modernes, la distinction public/privé est pertinente et opératoire pour ce champ de l'expertise qu'elle travaille et structure en profondeur.

Par ailleurs, elle est intéressante du point de vue des enjeux qu'elle draine et des questions qu'elle pose. Dans un contexte de « *monopole étatique de la violence légitime* », la production d'expertise destinée aux autorités régaliennes<sup>7</sup> doit-elle être prise en charge par la puissance publique ou bien peut-elle être livrée aux acteurs privés, compte tenu des conséquences de ce choix en matière de libertés et de droits individuels, d'indépendance de la justice et d'égalité des citoyens face à l'institution judiciaire ?

Portée par des enjeux et elle-même porteuse d'enjeux, la dimension

public/privé mérite d'être réinterrogée et confrontée au dispositif de production d'expertise judiciaire, particulièrement au moment où elle est l'objet de remaniements et de recompositions. On observe un double mouvement : d'une part, le brouillage, la dilution des valeurs autour desquelles s'est construite la bipolarité public/privé et d'autre part, la réactivation, la consolidation de cette bipartition qui « *semble épuiser l'univers du pensable et du dicible* »<sup>8</sup>.

La production d'expertise judiciaire s'organise autour d'un dispositif qui aménage de manière spécifique cette bipolarité. Au sein de ce système sont articulées et mises en perspective la sphère publique, la sphère privée et les points de passage entre ces deux ensembles non étanches.

La pertinence et l'intérêt d'une analyse du système de production d'expertise judiciaire se nourrissent d'un double objectif de connaissance : étude de la matrice originale, de l'agencement typique des caractères public, privé et de leurs formes intermédiaires singulières d'une part ; analyse des structures et acteurs constitutifs et animateurs du dispositif institutionnel d'autre part. Ce double objectif de connaissance se justifie tant par l'absence actuelle d'une appréhension globale de l'expertise judiciaire que par la méconnaissance avérée des structures institutionnelles de production d'expertise judiciaire.

••••(6) CHEVALLIER, 1995, p. 6 ; p. 9.

(7) Justice et police

(8) CHEVALLIER, *op. cit.*, 1995, p. 16.

D'un point de vue juridique, l'expertise judiciaire est définie comme un avis technique qui éclaire le magistrat « *sur une question de fait qui requiert les lumières d'un technicien* »<sup>9</sup>. Il s'agit donc en matière civile comme en matière pénale d'« *une mesure [...] confiée par une juridiction à des gens expérimentés dans un métier, un art ou une science, afin d'obtenir des renseignements dont elle a besoin et qu'elle ne peut se procurer elle-même* »<sup>10</sup>.

Au fur et à mesure de nos recherches, est apparue la nécessité de rompre avec cette définition normative et de proposer une définition renouvelée pour un objet non plus juridique mais bien politique et sociologique. Par expertise judiciaire, on désigne alors toute intervention effective d'un diagnostic, d'un avis technique et scientifique dans le processus judiciaire émanant d'acteurs non judiciaires, dont l'intervention est de type professionnel et dont la légitimité est issue à la fois de leurs compétences professionnelles - réelles ou supposées - et de leur reconnaissance par l'institution judiciaire. Cette démarche implique de prendre en compte à la fois les mesures de constatation, de consultation et d'expertise<sup>11</sup> mais aussi toutes les investigations d'ordre scientifique et/ou technique (prélèvements et analyses) effectuées pendant l'enquête. L'expertise judiciaire est alors comprise comme les avis techniques et scienti-

fiques utilisés de fait par l'institution judiciaire.

La production d'expertise judiciaire est organisée en un système fondé sur la distinction public/privé. Il s'agit d'un système dual, bipartite au sein duquel coexistent différentes structures de type public et privé, au sens statutaire et économique du terme. La sphère publique est fondée sur la notion d'intérêt général qui « *est le principe d'ordre et de totalisation, qui permet à la société de parvenir à l'intégration, de réaliser son unité, par le dépassement des particularismes individuels et des égoïsmes catégoriels. Le privé est au contraire dominé par l'intérêt particulier : il donne à chacun la possibilité de poursuivre la réalisation de ses propres fins, en garantissant son autonomie* »<sup>12</sup>.

La pratique à titre privé de l'expertise vise ainsi à satisfaire des intérêts particuliers, qu'ils s'expriment en termes de profits, d'intérêt intellectuel ou professionnel, tandis que la gestion publique de l'expertise correspond à l'idée que c'est à l'État qu'il revient de prendre en charge cet aspect de la vie collective et de le financer par les deniers publics. Experts publics et privés sont donc profondément différents, non seulement d'un point de vue organisationnel mais aussi dans les idéologies et références qui les sous-tendent.

•••(9) Article 232 du Nouveau code de procédure civile.

(10) VOULET, 1983.

(11) Le nouveau code de procédure civile distingue en effet la constatation, la consultation et l'expertise qui constituent les trois formes juridiques de l'intervention d'un technicien dans le processus judiciaire.

(12) CHEVALLIER, *op. cit.*, 1995, p. 7

La partie publique du dispositif est organisée autour de deux grands pôles : des laboratoires généralistes (laboratoires de police scientifique ; Institut de recherches criminelles de la Gendarmerie nationale) et des laboratoires spécialisés (médecine légale, toxicologie).

Cette distinction généralistes/spécialistes fait apparaître la pertinence du clivage disciplinaire pour l'analyse des sources et lieux de production d'expertise judiciaire. La différenciation entre des disciplines médicales (médecine légale et toxicologie) et des activités de police technique et scientifique est particulièrement significative car elle correspond à des savoirs et des apprentissages, à des identités et des sentiments d'appartenance dont la spécificité est fortement affirmée<sup>13</sup>. La médecine légale - plus exactement les médecins légistes - opèrent un travail de démarcation, de distinction à l'égard des structures de police scientifique dont ils se tiennent délibérément à distance. Cette volonté d'autonomie se manifeste dans la permanence d'institutions et de lieux distincts, comme le montre le cas parisien : la place Mazas pour l'institut médico-légal et le quai de l'Horloge pour le laboratoire de police scienti-

fique. La distance identitaire et disciplinaire se traduit alors en distance géographique.

La coupure entre médecine légale et police scientifique particulièrement flagrante en France, correspond à une conception typiquement hexagonale qui prend sa source au cœur de l'histoire de la criminalistique française.

« LA POLICE SCIENTIFIQUE, FILLE DE LA MÉDECINE LÉGALE »<sup>14</sup>

Historiquement, la médecine légale constitue une des formes premières de l'expertise judiciaire en matière pénale<sup>15</sup>. Pionnière en ce qui concerne l'introduction d'un esprit scientifique et d'une approche rationnelle dans l'étude du crime et du criminel, elle a préparé le terrain pour l'émergence d'autres disciplines légales comme la police scientifique. Qui plus est, les médecins légistes ont eux-mêmes, parce que telle était la demande de la justice, développé des pratiques de police scientifique qui se sont ensuite progressivement rationalisées, institutionnalisées et autonomisées.

Les recherches effectuées dans le sillage de la médecine légale mettent en place, dès le milieu du XIX<sup>e</sup> siècle, quelques-uns des grands thèmes qui seront ensuite exploités par la police

•••(13) Sur la constitution de la médecine légale en tant que discipline autonome, voir DUMOULIN, 1996.

(14) Nécrologie de LOCARD, 1966.

(15) Voir notamment BINET, ?

(16) Voir par exemple ORFILA, 1845, p. 112-129.

(17) Voir par exemple MASSON, 1886, p. 336-345.

(18) Voir par exemple MEGNIN, 1888 ; 1889.

(19) Voir par exemple GAUTIER DE CLAUBRY, 1858, p. 201-203.

(20) Voir par exemple CHEVALIER, PEYAL, 1832.

scientifique : reconnaissance des taches de sang<sup>16</sup>, empreintes digitales<sup>17</sup>, entomologie<sup>18</sup>, balistique<sup>19</sup>, et même reconnaissance des faux en écritures<sup>20</sup>. À travers la problématique de l'identification notamment, la médecine légale contribue donc très significativement à l'émergence de la police scientifique, qui tirera toutefois son émancipation du rapprochement avec la police technique, issue pour sa part de l'activité policière de constitution de fichiers.

En effet, au tournant du siècle, plusieurs laboratoires de police technique et services d'identité judiciaires - jusque-là compétents en matière d'identification des criminels - sont dotés de missions de police scientifique, c'est-à-dire d'administration de la preuve indiciale. C'est le cas avec l'actuel laboratoire de police scientifique de Paris<sup>21</sup> qui est l'émanation directe du service de l'Identité judiciaire de la Préfecture de police de Paris, créé le 11 août 1893 par le Préfet Lépine et placé sous la direction d'Alphonse Bertillon<sup>22</sup>. À l'origine, ce service fut mis en place afin de permettre l'identification rationnelle et systématique des délinquants par l'application de la méthode anthropométrique d'Alphonse Bertillon. Ce système fut imaginé par cet ancien commis aux écritures à la Préfecture de police de Paris, afin « *d'établir scienti-*

*fiquement l'identité des délinquants et de sanctionner en eux les récidivistes. L'établissement rigoureux des signalements des prévenus, juxtaposé avec une technique rationnelle de classement, aboutit à l'instauration d'un fichier judiciaire élaboré et efficace. Ces éléments forment la clef de voûte du système anthropométrique*»<sup>23</sup>.

L'adjonction d'une mission de recherche et d'administration de la preuve indiciale à la mission originelle d'identification des délinquants, transforma ce service d'identification en laboratoire de police scientifique. Complètement dissocié du service de l'Identité judiciaire depuis 1987, le Laboratoire est maintenant placé sous la co-tutelle du Préfet de police de Paris et de la Centrale *via* la Sous-direction de la police technique et scientifique. Le lien de filiation et les proximités intellectuelles qui unissaient initialement médecine légale et police scientifique n'ont cependant pas permis la constitution d'un pôle criminalistique commun.

La situation française est donc tout à fait originale, comparée au monde anglo-saxon où la notion de criminalistique englobe l'ensemble des disciplines qui participent à l'administration de la preuve indiciale. En France, le terme de criminalistique est, de ce point de vue, presque dénué de sens.

•••(21) Situé sur le Quai de l'Horloge, à proximité du Palais de Justice, il est dirigé depuis septembre 1996 par Marie-Hélène Cherpin.

(22) KALUSZYNSKI, 1987, p. 276.

(23) KALUSZYNSKI, 1987, p.269.

(24) On remarque dans la littérature concernée, des tentatives constantes et récurrentes de définition de ces disciplines, de délimitation et de spécification de leurs champs d'intervention. Voir par exemple : CECCALDI, 1976 ; LE CLERE, 1967 ; FOMBONNE, 1994.

On évoque distinctement la police technique, la police scientifique et la médecine légale, voire la dactyloscopie ou l'anthropométrie, sans même qu'un consensus règne sur leurs définitions et délimitations respectives<sup>24</sup>.

#### ENTRE POLICE ET GENDARMERIE

Néanmoins, d'un point de vue institutionnel, les activités de police scientifique sont exercées dans le cadre de cinq laboratoires répartis sur le territoire français (Paris, Lyon, Marseille, Lille, Toulouse) et dont le statut est fixé par les textes de 1943<sup>25</sup>. Ils réorganisent l'ensemble des fonctions de police scientifique en créant « *un service de police technique relevant de la Direction générale de la police nationale [...] chargé de rechercher et d'utiliser les méthodes scientifiques propres à l'identification des délinquants* » (art.1). Outre les organismes centraux, régionaux et locaux d'identité judiciaire, ce service comprend les laboratoires interrégionaux de police scientifique (les LIPS), dont les compétences sont aujourd'hui nationales. Suite à la promulgation de ces textes, certains laboratoires qui existaient déjà ont été remaniés tandis que d'autres ont été créés et progressivement mis en place.

Ces structures sont subventionnées par le budget de l'État. Leur personnel relève du fonctionnariat. Il comprend

des policiers formés aux techniques de police scientifique, des scientifiques issus de la société civile et recrutés sur concours et des administratifs. Chaque laboratoire tente de développer des spécialités et thèmes de recherche spécifiques. Ainsi le laboratoire de Lyon expérimente actuellement des systèmes de reconnaissance de la voix.

La fonction de ces laboratoires, telle que définie en 1943, consiste à « *procéder à tous les examens, recherches et analyses d'ordre physique, chimique et biologique demandés par les parquets ou les différents services de police des régions qui lui sont rattachées* » (art.6). Il s'agit alors le plus souvent d'enquêtes techniques destinées à orienter la police ou la gendarmerie. Mais ces laboratoires peuvent également être saisis par des magistrats en demande d'expertises judiciaires.

Délaissés pendant plusieurs décennies, les laboratoires de police technique et scientifique connaissent un nouvel essor à la suite de la politique de modernisation de la police nationale entreprise dans les années quatre-vingt. La création de la Sous-direction de la police technique et scientifique en mars 1985, la multiplication des budgets affectés à la police technique et scientifique<sup>26</sup> ont permis la revalorisation de ces laboratoires, au moment où la gendarmerie se mettait à investir le domaine des activités criminalistiques.

•••(25) Il s'agit de l'acte dit loi n°43-667 du 27 novembre 1943 portant création d'un service de police technique et du décret n°43-3260 du 27 novembre 1943 fixant le mode de recrutement, le statut et la rémunération des personnels de laboratoire de police technique.

(26) À travers en particulier la loi n°85-835 du 7 août 1985 relative à la modernisation de la police nationale.

En effet, une structure de statut militaire, à vocation généraliste, concurrence l'institution policière dans l'exercice de ses fonctions de police scientifique. D'abord apparue sous la forme d'une Section technique d'investigations criminelles (1987), elle est devenue, en 1990, l'Institut de recherches criminelles de la Gendarmerie nationale (IRCGN)<sup>27</sup>.

L'irruption de cette nouvelle structure sur le créneau déjà occupé par les LIPS « dans un domaine purement scientifique dont le coût particulièrement élevé milite pour un regroupement des moyens »<sup>28</sup> a de quoi étonner et susciter des interrogations.

De ce point de vue, le constat dressé dans un passage du schéma directeur de la Gendarmerie nationale (1986) est particulièrement éclairant. « *La gendarmerie reste totalement démunie et se trouve face à l'enjeu suivant : ou bien elle se dote du support technique et scientifique indispensable pour appliquer un traitement professionnel au fait judiciaire et elle assure ainsi sa crédibilité aux yeux des magistrats ; ou bien elle ne prend pas les mesures qui s'imposent et elle risque, à brève échéance, de se voir dessaisie de toute enquête nécessitant des examens techniques ou scientifiques ; elle se trouvera alors placée dans une situation tout à fait marginale dans l'exercice de la police judiciaire* »<sup>29</sup>.

À la lecture de ce passage, apparaissent clairement les enjeux liés à l'exercice de la police scientifique ainsi que l'intérêt pour la Gendarmerie d'être présente sur ce terrain. Aussi la création de l'institut de Rosny-sous-Bois a-t-elle répondu à un triple objectif : restaurer l'image de la gendarmerie et faire la preuve de sa compétence notamment suite aux errements de l'affaire Grégory, alors en pleine effervescence ; garantir le maintien de la gendarmerie dans ses fonctions de police judiciaire, pour lesquelles elle est en concurrence directe avec la Police nationale ; enfin, assurer son autonomie en matière criminalistique.

Il convient de préciser que jusque-là, la Gendarmerie nationale s'était trouvée privée de l'exercice des opérations de police technique et scientifique<sup>30</sup>. En 1958, un décret l'avait rendue compétente en matière de police technique, mais ce n'est qu'en 1985 que la loi de modernisation de la police lui avait permis de mener des activités de police scientifique à part entière.

#### LES STRUCTURES MÉDICO-LÉGALES EN QUESTION

Les laboratoires de toxicologie et les instituts de médecine légale rattachés aux centres hospitaliers et/ou universitaires se distinguent des autres structures publiques par une double spécifi-

•••(27) Depuis sa création, l'IRCGN s'est considérablement développé ainsi que le montrent les effectifs du personnel. Si, en 1987, la section des investigations criminelles comptait 16 membres, sept ans plus tard, l'Institut emploie dix fois plus - 164 personnes exactement - dans un statut essentiellement militaire : seuls 5,5% du personnel total sont des civils, AGOSTINI (F.), 1995, p.50. Sur l'IRCGN, voir également, FOMBONNE, 1994, *op. cit.*

(28) AGOSTINI, 1995, p.2.

(29) Schéma directeur de la Gendarmerie nationale, septembre 1986, cité par AGOSTINI, 1995, p.45-46. Les passages soulignés le sont de notre fait.

(30) L'article 9 de l'acte dit loi n°43-667 du 27 novembre 1943 disposait en effet qu'« il appartient aux officiers de police judiciaire, aux fonctionnaires et aux agents de la police et de la gendarmerie d'assurer par tous les moyens la conservation des traces et indices ». De fait, l'interprétation étroite de ce texte cantonnait la Gendarmerie dans un rôle de protection des lieux et l'excluait ainsi des mesures de police technique et scientifique.



cité qui réside à la fois dans le matériau qui leur est soumis (le corps humain à travers les différents types de vestiges et de traces qui peuvent être exploités) et dans l'identité et le statut médicaux qui les caractérisent. Levées de corps, nécropsies, examens complémentaires liés à l'autopsie, recherches de substances toxiques dans le sang et dans les viscères, examens psychiatriques constituent les principales opérations réalisées en matière pénale. En matière civile, l'éventail des pratiques est peut-être plus large encore, avec toutefois des constantes : les examens d'évaluation du dommage corporel et les analyses du sang pour des recherches en paternité.

La médecine légale a été marquée par un déclin progressif, dénoncé tant par les praticiens<sup>31</sup> que par les commissions *ad hoc*<sup>32</sup>. En 1974 déjà, le bilan dressé par le groupe de travail chargé d'étudier les problèmes de la médecine légale insistait sur la « *crise profonde de l'activité médico-légale française* »<sup>33</sup>.

Depuis vingt ans que la question de la médecine légale suscite par intermittences des volontés de réforme, les solutions proposées ne changent guère. Elles reposent principalement sur l'idée d'intégrer la médecine légale à l'hôpital, ce qui n'avait pas été réalisé lors de la création des centres hospitalo-univer-

sitaires (CHU). Suggérée dès le rapport de 1974, cette voie est, aujourd'hui encore, celle qui retient l'attention des pouvoirs publics, notamment dans le cadre du Conseil supérieur de la médecine légale<sup>34</sup>, chargé de « *dresser un état des besoins et d'établir un programme d'organisation [de la médecine légale] au niveau national* »<sup>35</sup>. Ce regroupement des capacités d'expertise médico-légale viendrait rationaliser une situation éclatée, marquée par de fortes disparités régionales.

Qu'il soit ou non mis en œuvre, ce projet de réforme est intéressant par les réactions et critiques qu'il suscite. Le principal reproche qui lui est adressé concerne le risque de monopolisation des capacités et fonctions d'expertise médico-légale. Face à l'aubaine que représenteraient « *un corps d'experts disponibles et un plateau technique de haut niveau* »<sup>36</sup>, avancés par les promoteurs de cette réforme, les opposants soulignent le risque d'un monopole régional et d'une organisation hiérarchique du centre, placé sous la direction du professeur de médecine légale local. Il est intéressant de noter que ce sont, argument pour argument, les mêmes raisonnements qui, depuis le XIX<sup>e</sup> siècle, s'affrontent à chaque fois qu'il est question d'une réforme du statut de l'expertise judiciaire ! C'est en vertu de ces arguments notamment,

•••(31) Voir par exemple : Davost, 1984, p. 16-18.

(32) Depuis la création du Groupe interministériel de médecine légale en 1974, plusieurs enquêtes et rapports ont fait le bilan de la médecine légale française. Voir notamment : Ministère de la Justice, 1975 et GORTAIS, 1983.

(33) Ministère de la Justice, 1975, p. 54.

(34) Créé par le décret n°94-1210 du 30 décembre 1994.

(35) Le bureau de la police judiciaire, *op. cit.*, p. 62.

(36) DAVOST, 1984, *op. cit.*, p.17.



que la dualité de la production d'expertise (public/privé) demeure encore aujourd'hui. Comme si la compétence était induite par la professionnalisation forcément monopolistique et l'indépendance par la pluralité de praticiens épars. L'expertise serait alors éternellement prise entre les deux termes d'une alternative irréductible : compétence *versus* indépendance.

« L'ONCLE D'AMÉRIQUE » : LE LABORATOIRE CENTRAL DE LA PRÉFECTURE DE POLICE DE PARIS

Le Laboratoire central de la Préfecture de police de Paris<sup>37</sup> est un cas à part. Bien que ses activités de police judiciaire ne représentent qu'une modeste partie de ses missions, il est particulièrement dynamique et innovant dans ce domaine. Malgré une distance effective liée à sa pluri-activité, cet « oncle d'Amérique » fait beaucoup pour la police scientifique.

Le Laboratoire central est un établissement spécifiquement parisien, né de la situation particulière de la capitale en matière de police<sup>38</sup>. « *Organisme scientifique, d'étude, de prévention et de contrôle placé sous l'autorité du préfet de police* »<sup>39</sup>, il est principalement en charge de missions de police administrative (pollution de l'air, sécurité des établissements recevant du

public, etc.) pour lesquelles il assiste techniquement le préfet dans ce qui a trait à la sécurité et à la salubrité de la population de Paris et de sa petite couronne. Il intervient par ailleurs en matière de police judiciaire, en cas d'incendies, d'explosions et d'attentats. C'est dans ce cadre qu'il contribue à la production d'avis techniques sur lesquels s'appuieront la police et la justice. La permanence générale<sup>40</sup>, qui fonctionne 24 heures sur 24, est assurée par le roulement d'équipes d'intervention composées d'un ingénieur et d'un technicien. Contactée par les services de police notamment, l'équipe de garde se rend sur les lieux du sinistre et procède aux constatations et prélèvements nécessaires, qui seront ensuite analysés par les services du laboratoire. L'exploitation de ces éléments matériels vise à orienter l'enquête et plus particulièrement à déterminer le caractère criminel ou accidentel du sinistre.

Doté de compétences multiples, employant plus de deux cents personnes, ce laboratoire surprend par son importance mais aussi par l'originalité de son statut et de ses activités. En effet, malgré une dimension locale et une tutelle spécifique, ce laboratoire a joué un rôle d'entraînement et de moteur en matière de police scientifique. Spécialiste des explosifs, il est

•••(37) Situé rue Dantzig dans le XV<sup>e</sup> arrondissement, il est actuellement dirigé par MM. Henri Viellard (directeur) et Jean-Luc Géronimi (directeur-adjoint).

(38) Le maire de Paris est le seul maire français à ne pas disposer des pouvoirs de police qui sont détenus par le Préfet de police. Voir à ce sujet BERLIÈRE, 1993, p.33-51.

(39) Extrait du fascicule de présentation du Laboratoire Central, p. 5.

(40) Outre cette permanence générale, le laboratoire dispose d'une permanence des explosifs « chargée de tous les problèmes liés à la mise en œuvre de substances explosives » qui intervient selon les mêmes modalités que la permanence générale, fascicule de présentation du Laboratoire Central, p. 7.

devenu l'interlocuteur des pouvoirs publics lors de chaque attentat - que l'événement ait lieu à Paris ou en province. À tel point que le service des explosifs est désormais financé non plus sur le budget de la ville de Paris mais sur celui du ministère de l'Intérieur (Sous-direction de la PTS). À grade égal, les fonctionnaires du même laboratoire ont donc des statuts et des rattachements distincts suivant le service auquel ils appartiennent. Cette situation surprenante qui traduit bien l'éclatement des capacités d'expertise judiciaire déjà souligné, pourrait se trouver régularisée par une pure et simple intégration de ce service dans le dispositif de police scientifique, actuellement en réorganisation. La volonté politique de constitution d'un pôle « criminalistique » milite en effet pour ce genre de regroupement, permettant une rationalisation du système de production d'expertise. Le laboratoire central entretient d'ores et déjà de bonnes relations avec les laboratoires de police scientifique : des politiques d'échanges en matière de formation et d'informations permettent de développer les contacts entre laboratoires<sup>41</sup>. La participation commune aux différentes réflexions et séances de travail du Conseil supérieur de la PTS, auquel prend part le laboratoire central, intensifie ces relations et prépare une éventuelle restructuration.

L'ensemble des structures publiques de production d'expertise - aussi diverses que multiples - s'inscrit dans

un dispositif bipolaire éminemment complexe et éclaté. Ce dispositif global est le résultat de la sédimentation progressive, de l'accumulation désordonnée d'éléments épars, qui se sont superposés, chevauchés pour dessiner les contours sinueux d'un dispositif polycéphale. Les différentes « couches » constitutives de ce système ont été mises en place sans concertation ni harmonisation d'ensemble, sans planification préalable ni construction rationnelle. Chaque élément est venu compléter et améliorer un dispositif jugé peu performant, sans vue d'ensemble, sans souci de la cohérence d'un tout né de l'adjonction « sauvage » de parties.

Bien souvent, la création d'une structure a correspondu à la nécessité de répondre à un besoin précis, dans le cadre d'une conjoncture particulière. Ainsi, la naissance du laboratoire central est le fruit de la multiplication des fraudes alimentaires et de la décision politique de se donner les moyens de lutter contre de tels délits, en identifiant et prouvant les fraudes commises. La naissance de plusieurs laboratoires de police scientifique, à travers la France du début du siècle, visait à l'époque à concentrer et centraliser les savoirs et moyens disponibles afin de permettre le développement des pratiques de police technique et scientifique.

Quant au positionnement des laboratoires privés sur le marché de l'expertise, il est intervenu notamment

•••(41) En 1996, « dans le cadre des échanges interlaboratoires, le service [de chimie analytique] a accueilli des fonctionnaires des laboratoires de PTS de Lille, Lyon, Marseille, Toulouse et de l'IRCGN de Rosny-sous-Bois », Rapport d'activité du laboratoire central, 1996, p. 68.

pour pallier les lacunes des laboratoires de police alors en net déclin.

#### LES STRUCTURES ET ACTEURS PRIVÉS

Les laboratoires privés constituent un des deux grands types d'expertise privée, à côté des experts judiciaires qui participent à titre occasionnel et individuel à l'œuvre de justice.

#### LES LABORATOIRES PRIVÉS, AUXILIAIRES JUDICIAIRES

Ces laboratoires effectuent, particulièrement en matière d'empreintes génétiques<sup>42</sup>, des analyses à la demande des services de police et de justice. « *L'analyse des empreintes génétiques a été et est encore dominée par le secteur privé, ce qui est plutôt nouveau en criminalistique* »<sup>43</sup>. Le dépôt d'un brevet dont les droits ont ensuite été vendus à Cellmark, filiale du groupe *Imperial Chemical Industries* explique que cette technique ait été d'emblée dirigée vers les canaux commerciaux et la sphère privée.

En France, en raison des carences des structures publiques dans la maîtrise de cette nouvelle technologie, un laboratoire privé - le Centre d'application et de recherches en microscopie électronique (CARME) - s'est placé sur ce créneau porteur et a répondu assez largement aux besoins de la gendar-

merie et de la police bordelaise. Après des débuts très prometteurs, la réputation de ce laboratoire a cependant été mise à mal par ses propres dysfonctionnements et erreurs - apparemment liés aux contraintes des lois du marché - qui ont semé le doute sur le sérieux et la fiabilité de ses analyses<sup>44</sup>.

Par ailleurs, le lancement d'une politique volontariste de modernisation de la police nationale - mettant l'accent sur la revalorisation de la police technique et scientifique et sur la nécessité de maîtriser des technologies de pointe comme les empreintes génétiques - mais aussi la création d'une unité de criminalistique par la Gendarmerie nationale ont revivifié le secteur et mis en selle des concurrents publics crédibles face aux laboratoires privés. Le recours à des laboratoires privés se poursuit cependant en fonction des usages régionaux et des contraintes locales. À Nantes, Bordeaux, Paris, des laboratoires privés sont sollicités par les services enquêteurs<sup>45</sup>.

L'autre source d'expertise privée est composée d'une masse d'« indépendants de l'expertise », qui, en matière civile comme en matière pénale, au gré des besoins des juridictions, effectuent des expertises à et pour leur propre compte, en marge d'un emploi de salarié ou de fonctionnaire. Il s'agit

•••(42) Pour un historique des empreintes génétiques doublé d'un exposé des méthodes mises en œuvre par cette technique d'identification, voir notamment : DOUTREMEPUICH, 1998, p. 11-29.

(43) COQUOZ, 1989, p. 339.

(44) Du moins si l'on en croit les informations distillées par la presse sur cette question, voir notamment CHARPIER, 1997, p. 178-182 ainsi que l'émission « Envoyé spécial » diffusée le 4 mars 1993 sur France 2.

(45) Ainsi, lors de l'accident de voiture dont a été victime la princesse de Galles, l'analyse du sang et des urines du chauffeur a été effectuée par le laboratoire Toxlab ; REVERIER, 1997.

alors d'une activité occasionnelle économiquement et statutairement privée.

LES INDÉPENDANTS DE L'EXPERTISE OU LES AMBIGÜITÉS DU PROFESSIONNALISME

Concernant ces experts, la Chancellerie<sup>46</sup> a été et est encore farouchement opposée à l'idée d'une profession d'expert judiciaire. Les praticiens de l'expertise sont censés faire de celle-ci une activité complémentaire en appoint de leur activité professionnelle principale. Ils font bénéficier la justice de leurs connaissances, compétences et expériences ; en retour, celle-ci les indemnise pour le temps passé et les frais engagés, loin de toute idée de profit.

Dans cette optique, l'expertise constitue une activité d'engagement (participer à l'œuvre de justice) ou d'ouverture professionnelle (être confronté à des problèmes techniques nouveaux, dans un contexte original). Le maintien de l'activité professionnelle initiale permet le désintéressement et l'indépendance financière de l'expert lors de sa pratique d'expertise. Pour autant, on observe dans les faits - notamment en raison des difficultés économiques rencontrées par des professions libérales telles que celle d'architecte - l'existence

d'une pratique à titre principal et à temps plein de l'expertise<sup>47</sup>.

Et ce, d'autant plus que ces experts bénéficient depuis les années soixante-dix<sup>48</sup> des titres protégés d'*expert près la Cour d'appel et d'expert agréé par la Cour de cassation*. Chaque année, dans chacune des trente trois Cours d'appel françaises, les magistrats établissent une liste qui indique nominativement qui porte le titre légal d'expert auprès d'elles. Parallèlement, la Cour de cassation fixe la liste nationale qui correspond au titre d'expert agréé par la Cour de cassation, titre plus prestigieux encore que le précédent. Ces deux types de listes qui correspondent au découpage local/national sont communes au pénal et au civil. Véritables catalogues à la Prévert, ces listes compilent une multitude de disciplines et de métiers hétérogènes depuis la médecine jusqu'à l'horlogerie en passant par l'informatique, la plomberie, les sciences de l'ingénieur ou la psychologie.

Constitutive d'un sous-système de production d'expertise, la catégorie des experts privés est historiquement la forme statutaire première de production d'expertise<sup>49</sup>. Si ce type d'expertise a été maintenu au cœur du dispositif, s'il n'a pas été remplacé par des

•••(46) Par cette formule, qui a le défaut d'être trop réifiante et désincarnée, on souhaite faire passer l'idée d'un point de vue officiel, celui du Garde des Sceaux et de son administration, point de vue exprimé et relayé notamment par les magistrats en poste au Bureau des professions juridiques et judiciaires de la Direction des affaires civiles et du sceau du Ministère de la Justice.

(47) Ces experts privés sont alors soumis à des contraintes économiques (faire vivre un cabinet par les seules expertises judiciaires ou presque) et instaurent une relation de type quasi-salarial avec les magistrats, considérés plus ou moins explicitement comme leurs employeurs. Les experts - particulièrement ceux qui ont tendance à faire de l'expertise une activité exclusive - développent alors des stratégies collectives de regroupement, de promotion et de défense de l'identité des experts judiciaires. C'est à travers des associations comme les Compagnies d'experts que les experts tentent de faire reconnaître leur statut. Sur cette question, DUMOULIN, 1995.

(48) Il s'agit de la loi n°71-498 du 29 juin 1971 et du décret n°74-1184 du 31 décembre 1974.

formes nouvelles - tels les laboratoires - c'est en raison à la fois de l'intérêt objectif de cette forme spécifique d'expertise et de l'intérêt d'un double système qui combine les avantages respectifs des structures d'expertise et des experts atomisés.

#### L'INTÉRÊT D'UN SYSTÈME PLURIEL

Le système actuel, par sa complexité, sécrète de multiples zones d'incertitude et de flexibilité. La diversité des formes et statuts d'expertise induit en effet une pluralité d'opportunités pour les magistrats, en termes de disponibilité (ce qui est appréciable en cas d'urgences) et de compétences, ce qui est précieux pour des dossiers particulièrement compliqués ou pointus). Il y a donc un intérêt certain pour le personnel judiciaire à laisser un tel système se perpétuer.

Par ailleurs, ce double système a également le mérite de n'entraver ni la liberté des magistrats dans le choix des experts ni l'indépendance des experts désignés. La pluralité des experts et de leurs statuts permet au magistrat d'exercer un véritable choix lors de la désignation du technicien. Sans compter qu'en cas de contre-expertise, les francs-tireurs de l'expertise offrent une alternative aux laboratoires.

De ce point de vue, la pluralité des instances de production d'expertise

judiciaire est née à la fois de la volonté ponctuelle et itérative de rendre plus efficace le système et de la permanence d'exigences de principes. La coexistence de structures publiques et privées est certes le résultat d'une absence de politique volontariste en matière d'expertise judiciaire et de police scientifique.

Cependant, la survie de ce système aléatoirement constitué peut s'expliquer par l'appropriation utilitaire qu'en ont fait les magistrats. En ce sens, le critère statutaire est, en matière de production d'expertise judiciaire, toujours porteur de sens. Pourtant, si le clivage public/privé structure efficacement le champ de l'expertise judiciaire, on relève plusieurs zones de croisement et d'imbrication du public et du privé.

#### LE PRIVÉ DANS LE PUBLIC ET LE PUBLIC DANS LE PRIVÉ : L'ART DU FONDU ENCHAÎNÉ

La production d'expertise judiciaire offre un bel exemple du « *brouillage de la distinction public/privé, illustré par l'effacement des repères axiologiques, le rapprochement des systèmes normatifs et l'imbrication des sphères publique et privée* »<sup>50</sup>. En témoigne significativement le fait de donner à des fonctionnaires de laboratoires publics, qui pratiquent l'expertise, le statut d'experts privés.

•••(49) Avant qu'ils ne s'organisent en professions ou en structures de type laboratoires, les experts sont d'abord des individus atomisés à qui les autorités ont recours en cas de mort suspecte, de viol, d'avortement, etc. Leurs fonctions s'institutionnalisent et se pérennisent ensuite sous la forme de professions, de charges et de corporations, voir notamment BINET, p. 24.

(50) CHEVALIER, 1995, p. 5.

Entrent en effet dans ce statut d'experts privés, certains fonctionnaires de laboratoires qui figurent en leur nom propre sur ces listes<sup>51</sup>. C'est le cas au laboratoire central où le directeur, le directeur adjoint et certains ingénieurs sont inscrits sur la liste des experts de la Cour d'appel de Paris, voire sur la liste de la Cour de cassation. Il s'agit alors d'expertises exercées à titre individuel, qui n'engagent pas le laboratoire mais bien la personne qui a été nommément désignée et qui accomplit personnellement sa mission<sup>52</sup>. En fonction des besoins du dossier, cet expert peut faire appel, à titre privé, au laboratoire qui réalise alors les analyses nécessaires. Cette saisine directe s'inscrit dans le fonctionnement normal du laboratoire qui, depuis sa création, est ouvert au public.

La présence, sur les listes des juridictions, de fonctionnaires qui travaillent dans des laboratoires publics et réalisent des expertises à et pour leur propre compte brouille la frontière entre public et privé. Elle la trouble davantage encore lorsque ce sont les directeurs des laboratoires publics, qui perçoivent personnellement les rétribu-

tions financières et symboliques, pour des expertises réalisées par le personnel du laboratoire. L'article 7 de l'acte dit loi de 1943 conférait aux « chefs et sous-chefs de laboratoires de police » la possibilité d'être « commis experts par les tribunaux » sans toutefois aménager un statut idoine, ni définir les modalités d'exercice de cette activité. Dans ce contexte d'imprécision juridique, les magistrats n'avaient d'autre choix que de désigner et de rémunérer les directeurs, même si les expertises étaient effectuées par l'entité laboratoire ; à la charge des directeurs d'apprécier l'opportunité d'une redistribution envers le personnel, son ampleur et ses bénéficiaires<sup>53</sup>. De fait, l'enrichissement personnel des directeurs de laboratoire s'est chiffré en centaines de milliers voire en millions de francs. Face à des dysfonctionnements avérés et à des agissements peu avouables<sup>54</sup>, les ministères concernés, particulièrement le ministère de l'Intérieur, se sont saisis de la question. Le groupe de travail sur les laboratoires de police au sein du Conseil supérieur de la PTS a en effet pour mandat de « régler les problèmes juridiques des expertises au sein des laboratoires, notamment le mode de désignation de l'expert et sa rémunération »<sup>55</sup>. C'est dans ce cadre que se

•••(51) C'est également le cas de certains directeurs de laboratoires privés. Ainsi, le directeur de Toxlab est personnellement inscrit sur la liste de la Cour de Cassation, REVERIER, 1997, p.106.

(52) Article 233 du Nouveau code de procédure civile : « Le technicien [...] doit remplir personnellement la mission qui lui est confiée ».

(53) Circulaire n°56-01 du 21 janvier 1956 relative aux attributions des organismes d'identité judiciaire et des chefs de laboratoire et émanant du ministère de la Justice.

(54) L'un des directeurs du laboratoire de police de Paris a été radié de la liste des experts agréés par la Cour de cassation pour avoir fait passer pour siens les résultats de recherches exécutées par un autre laboratoire dans le cadre d'une sorte de sous-traitance. Le scandale est né des problèmes posés à la fois sur le plan de la propriété intellectuelle et sur celui de la rémunération, CHARPIER, 1997, p.169-192.

prépare une réforme de fond de l'expertise pratiquée par les laboratoires publics.

Les débats de cette commission ont fait apparaître plusieurs points problématiques : la rémunération mais aussi la désignation et la responsabilité de l'expert. En effet, le système en pratique induisait des contournements discrets de la légalité : l'expert nommé n'était pas, contrairement aux dispositions de l'article 166 du CPP<sup>56</sup>, celui qui accomplissait effectivement sa mission. Ce qui signifie qu'en cour d'assises, l'expert convoqué - en l'occurrence le directeur - devait décrire oralement les opérations qu'il était censé avoir pratiquées et qui dans les faits avaient pu l'être par ses collègues ! Afin de parer au plus pressé, le directeur central de la police judiciaire a fait circuler en 1994 des instructions à l'attention des laboratoires de police scientifique. En ce qui concerne les rémunérations, il est prévu du point de vue des principes que « *l'expert reçoit du laboratoire une facturation tenant compte des prestations utilisées. La différence entre les honoraires demandés à la justice et la facture du laboratoire constitue la prime d'expertise destinée à rémunérer la*

*responsabilité de l'expert et le travail fourni par les assistants* »<sup>57</sup>. Trois ans plus tard, c'est par décret<sup>58</sup> qu'est instauré un système de rétribution conforme à ces principes. Par une modulation du nombre de points (le point a une valeur prédéterminée révisable le cas échéant), chacun peut être rétribué à hauteur de ses compétences et de sa contribution à un dossier donné. Pour autant, ce système transitoire ne règle pas l'épineuse question du statut juridique des laboratoires de police, question en débat au sein du Conseil supérieur de la police technique et scientifique<sup>59</sup>.

En somme, c'est à partir de failles et de flous juridiques que les laboratoires de police ont établi, au fil des ans, un mode de fonctionnement opérationnel et pragmatique. La structuration autour de ce système explique en partie le lent déclin qu'ont connu ces laboratoires pendant les décennies de l'après-guerre. Certes, la police technique et scientifique dans son ensemble a souffert du désintérêt des pouvoirs publics. Mais le système en vigueur propre aux laboratoires de police était cependant entaché de handicaps majeurs. Ainsi, la possibilité d'assurer « à mi-temps » cette

•••(55) Le bureau de la police judiciaire, *op.cit.*, p. 58. Ce groupe de travail examine deux grandes questions : les problèmes juridiques, financiers et techniques de l'expertise d'une part et la mise en place de contrôles de qualité d'autre part, AGOSTINI, 1995, p.53.

(56) Il prévoit que l'expert doit attester avoir personnellement accompli sa mission.

(57) Note n°4417/1455 PH/DLPJ/PJS/EM du 25 mars 1994 citée par AGOSTINI, 1995, p. 55.

(58) Il s'agit du décret n°97-647 du 31 mai 1997 portant attribution d'une indemnité d'expertise aux personnels de la police nationale en fonction dans les laboratoires de la police technique et scientifique. L'application de ce décret a été reconduite pour 1998.

(59) Un désaccord est apparu entre les différentes institutions en présence : si les représentants de l'IGA, de la Cour des Comptes et de la Chancellerie étaient favorables à l'idée de doter les laboratoires de la personnalité morale via un groupement d'intérêt public ou bien un établissement public, le ministère de l'Intérieur et la Gendarmerie nationale auraient plutôt opté pour une modification de l'article 157 du CPP ; AGOSTINI, 1995, p. 56-57.

fonction de direction, de maintenir simultanément son activité initiale et de percevoir des rémunérations colossales conférait à ce poste les attributs d'une sinécure. Cette position fort avantageuse de la direction ne motivait certainement pas le personnel, conscient de participer à des missions dont il ne récoltait guère les dividendes.

Ce système, dans lequel investissements publics et profits privés sont confondus, a éclaté au cours des dernières années sans que le principe de panachage public/privé ne soit remis en cause en tant que tel. L'actuelle recomposition n'est pas fondée sur un retournement idéologique de fond, elle part d'un constat de dysfonctionnements multiples qu'elle vise à résorber par un remaniement des modalités juridiques et pratiques d'exercice de l'expertise publique. Reste à savoir si le principe d'inscription nominative sur les listes d'experts auprès des juridictions demeurera, ou bien s'il sera remplacé par l'attribution de la personnalité morale aux laboratoires. À l'heure actuelle, le paradoxe et l'originalité de la production d'expertise judiciaire demeurent. Même si l'expertise pratiquée par les laboratoires devenait, au terme de cette réforme, une expertise publique à part entière, il resterait encore une zone d'interconnexion public/privé. En effet, concernant les experts inscrits sur les listes, s'il s'agit bien d'une expertise privée au sens éco-

nomique du terme - dans la mesure où elle est pratiquée dans un cadre libéral, principalement par des indépendants qui appartiennent à la société civile - c'est également une expertise à mi-chemin entre privé et public au sens où elle est en partie organisée et réglementée par l'État *via* l'inscription sur les listes et l'attribution de titres d'experts.

#### DES EXPERTS PRIVÉS SOUS STATUT RÉGLEMENTÉ ET PROTÉGÉ PAR L'ÉTAT

S'il existe bien un marché de l'expertise où sont en compétition une multitude de producteurs aux statuts distincts, pour autant il ne s'agit pas d'une situation de parfaite concurrence : l'accès au marché est réglementé. Les abus (n'importe qui se positionne sur le marché de l'expertise, que sa compétence le justifie ou non) sont régulés et compensés par l'État, sans pourtant qu'un monopole soit instauré. C'est alors que se pose la question du sens de la liste, système utilisé officieusement dans les juridictions civiles jusqu'à ce qu'il soit officialisé par les textes de 1971 et 1974<sup>60</sup>.

Polysémique et ambigu, le principe de la liste reste sur une position tout à fait intermédiaire - notamment par rapport aux revendications corporatistes émises par les experts - puisqu'il ne crée ni corps d'experts, ni monopole d'expertise. En instaurant une sélection, la liste restreint le nombre de

•••(60) Le mécanisme de la liste est apparu dès la loi Chevandier (30 novembre 1892) pour les médecins-experts et a été étendu à l'ensemble des experts, en matière pénale, par l'ordonnance du 4 juin 1960 et l'article 157 du Code de procédure pénale. En matière civile, la pratique est restée officieuse jusqu'à la loi de 1971 qui instaure une liste commune au pénal et au civil.



concurrents potentiels et oint les experts choisis d'un label. Dans tous les cas, si l'inscription sur une liste confère expressément et directement un titre, les experts ne sont effectivement en charge de dossiers judiciaires qu'à partir du moment où un magistrat les a investis d'une mission dans le cadre d'une affaire précise. L'inscription sur une liste garantit une sélection effectuée et consacrée par l'institution judiciaire. Elle ne donne pas de droit à être désigné pour des expertises, ni n'ouvre un fonctionnariat de l'expertise judiciaire. D'ailleurs, en matière civile, il appartient aux magistrats de désigner la personne de leur choix, qu'elle soit inscrite ou non sur une de ces listes<sup>61</sup>. En ce qui concerne les affaires pénales, les magistrats sont tenus de nommer des personnes figurant sur ces listes, même s'ils peuvent s'y soustraire en motivant un choix différent<sup>62</sup>.

#### DE L'EXPERTISE PUBLIQUE/PRIVÉE À L'EXPERTISE INTERNE/EXTERNE

Le dispositif actuel de production d'expertise judiciaire apparaît donc comme une vaste nébuleuse qui rassemble une multiplicité hétéroclite de lieux et de sources d'expertise judiciaire. Ce dispositif est révélateur d'une situation éminemment intermédiaire, mitigée, fruit du croisement de deux systèmes : production publique sans

monopole, système de marché avec acteurs publics. S'il ne s'agit pas là d'un cas unique, cette situation n'en est pas moins paradoxale et inattendue dans un domaine éminemment régalién, où une volonté étatique forte aurait pu permettre la mise en œuvre d'un système précis.

Le clivage public/privé appliqué à la police et à la justice, est particulièrement porteur de sens et d'enjeux. Analysée en termes d'expertise interne à ces institutions, l'expertise publique pose des questions de fond particulièrement en ce qui concerne l'indépendance des experts. Ainsi, dans le contexte français de la procédure inquisitoire, il est intéressant de noter que l'administrateur de la preuve indicielle peut relever de la même autorité de tutelle que les services enquêteurs - c'est le cas de l'IRCGN pour la gendarmerie mais aussi des laboratoires de police scientifique pour la Police nationale. Néanmoins, dans l'hypothèse d'une expertise privée soumise à la loi du marché, les interrogations soulevées sont tout aussi fondamentales. L'expérience du laboratoire privé de Bordeaux a montré qu'une expertise privée n'est pas forcément une expertise fiable et que l'immersion dans une logique marchande peut peser lourdement sur la structure d'expertise. Dans les deux cas, les instances d'expertise ne constituent pas des monades isolées. Des contraintes d'ordres divers

•••(61) Article 232 du Nouveau code de procédure civile : « Le juge peut commettre toute personne de son choix pour l'éclairer... ».

(62) Article 157 du Code de procédure pénale : « Les experts sont choisis parmi les personnes physiques ou morales qui figurent soit sur une liste nationale [...] soit sur une des listes dressées par les cours d'appel. [...] À titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes ».

peuvent peser sur elles et sont susceptibles d'interférer sur l'indépendance et la fiabilité des résultats.

C'est alors que la déontologie - grand cheval de bataille des organismes corporatistes comme les Compagnies d'experts - pourrait peut-être jouer le rôle déterminant de rempart vis-à-vis de ces contraintes. Les débats sur la nature de

ce bouclier éthique, son ampleur, son caractère libre ou imposé, personnel ou collectif, la légitimité des organismes chargés de le promouvoir et de le faire respecter relanceraient alors, sous un autre angle, l'éternelle question du statut des experts judiciaires.

■ **Laurence DUMOULIN**  
CERAT-IEP Grenoble

#### BIBLIOGRAPHIE

AGOSTINI (F.), 1995, *L'exercice de la police scientifique par la Police nationale et la Gendarmerie nationale : environnement juridique et perspectives*, Mémoire de DESS, Sophia-Antipolis.

BERLIÈRE (J.-M.), 1993, « L'impossible police parisienne ? », *Politix*, n°21, p.33-51.

BINET (C.), 1892, *Histoire de l'examen médico-judiciaire des cadavres en France*, Lyon, Paris, Stock/Masson, 116 p.

BOGO (D.), 1996, *La criminalistique : nouvelles méthodes, nouvelle déontologie ?*, Mémoire de l'IEP, Grenoble.

BROCHOT-DENYS (A.), 1995, « La police scientifique : prises de conscience », *Les Cahiers de la sécurité intérieure*, n°21, 2<sup>e</sup> trimestre, p. 17-24.

CECCALDI (P.-F.), 1976, *La criminalistique*, Paris, PUF, Coll. Que sais-je ?, (3<sup>e</sup> éd.).

CHARPIER (F.), 1997, *Au cœur de la PJ. Enquête sur la police scientifique*, Paris, Flammarion.

CHEVALLIER (A.), PEYTAI (F.), 1832, « Essais sur les moyens à mettre en usage pour empêcher et reconnaître les faux en écritures », *AHPML*, tome 8, 1<sup>re</sup> série, p. 154-179.

CHEVALLIER (J.), 1995, « Présentation de l'ouvrage », in CURAPP, Public/privé, Paris, PUF.

COQUOZ (R.), 1989, « Les empreintes génétiques et la criminalistique. Passé, présent, futur », *Revue internationale de criminologie et de police technique*, n°3.

DAVOST (P.), 1984, « La médecine légale en crise », *Le nouveau pouvoir judiciaire*, n°300, p.16-18.

DOUTREMEPUICH (C.) (dir.), 1998, *Les empreintes génétiques en pratique judiciaire*, Paris, La Documentation française, Coll. La sécurité aujourd'hui.

DUMOULIN (L.), 1996, « La médecine légale aux fondements de l'expertise judiciaire, de l'activité de médecin légiste à la profession d'expert judiciaire », communication au Colloque *Homo-Criminalis*, Genève. Actes à paraître sous la direction de PORRET (V.) ET PORRET (M.).

DUMOULIN (L.), 1995, *La Compagnie des experts près la cour d'appel de Grenoble, instance de régulation des rapports magistrats-experts. Contribution à une réflexion sur l'expertise judiciaire*, Mémoire de DEA, IEP Grenoble.

FOMBONNE (J.), 1994, *L'exercice de la police technique et scientifique par la Gendarmerie nationale : une solution rationnelle apportée, par le traitement de l'indice matériel, à la question de la preuve en matière pénale*, Thèse de doctorat de Droit, Paris II.

GAUTIER DE CLAUBRY (H.), 1858, « Des caractères que présentent les armes chargées avec le pyroxile », *AHPML*, 2<sup>e</sup> série, tome 9, p. 201-203.

GORTAIS (J.), 1983, *La médecine légale en France*, Service d'études pénales et criminologiques, ministère de la Justice, Paris, ronéo.

## BIBLIOGRAPHIE

- GRAVET (B.), 1995, « Police technique et scientifique et pratiques professionnelles », *Les Cahiers de la sécurité intérieure*, n°21, p. 25-37.
- KALUSZYNSKI (M.), 1987, « Alphonse Bertillon et l'anthropométrie », in Société d'histoire de la révolution de 1848 et des révolutions du XX<sup>e</sup> siècle, *Maintien de l'ordre et polices en France et en Europe au XIX<sup>e</sup> siècle*, Paris, Créaphis, 1987.
- LE CLERE (M.), 1967, *Manuel de police technique*, Paris, Police-Revue.
- LOCARD (E.), 1940, *Traité de criminalistique*, Tome 7 : L'enquête criminelle, Lyon, éditions Desvigne et Cie.
- LOCARD (E.), 1996, *Bulletin de médecine légale*, n°5, p.302-303.
- MASSON, 1886, « Contribution à l'étude des empreintes digitales en médecine légale », *AHPML*, 3e série, tome 16, p. 336-345.
- MEGNIN, 1888, « La faune des tombeaux », *AHPML*, 3e série, tome 19, p. 160-165.
- MEGNIN, 1889, « Entomologie appliquée à la médecine légale », *AHPML*, 3e série, tome 21, 1889, p. 159-161.
- MINISTÈRE DE LA JUSTICE, 1975, *La médecine légale en France*, Rapport du groupe de travail chargé d'étudier les problèmes de médecine légale.
- ORFILA (M.), 1845, « Mémoire sur un nouveau moyen de reconnaître les taches de sang », *AHPML*, 1<sup>re</sup> série, tome 34, p. 112-129.
- REVERIER (J.-L.), 1997, « Quand les cheveux parlent », *Le Point*, n°1314, 22 novembre.
- Revue de la Gendarmerie nationale*, 1996, « La police technique et scientifique », numéro spécial.
- SANNIE (C.), 1938, *Éléments de police scientifique*, Paris, Hermann et Cie.
- SANNIE (C.), 1952, « Expertise judiciaire et police scientifique : le rôle du service de l'Identité judiciaire », in RETAIL (L.) (dir.), *Techniques de l'expertise judiciaire*, Paris, Sirey.
- SANNIE (C.), 1954, *La recherche scientifique du criminel*, Paris, Armand Colin.
- VOULET (J.), 1983, *La pratique des expertises judiciaires*, Paris, Masson.
- ZAKI (M.), 1929, *Le rôle des laboratoires de police technique au point de vue de la police judiciaire et de l'instruction préparatoire*, Thèse de doctorat de droit, Lyon, éditions Desvigne et fils.



## NOTES BIBLIOGRAPHIQUES

*La criminologie québécoise et la sociologie des institutions et pratiques policières*

Les chercheurs français qui ont commencé à s'intéresser à la sociologie des institutions et des pratiques policières dans les années soixante-dix se souviennent que les références en langue française étaient alors quasi inexistantes. De ce fait, une exploration des ressources bibliographiques conduisait très rapidement à rencontrer l'ouvrage *Police, culture et société* qui avait été publié, en 1974, sous la direction de Denis Szabo, par les éditions de l'Université de Montréal. Ce livre, qui constituait aussi une ouverture sur le courant de recherches qui avait commencé à se développer aux États-Unis dans les années soixante, était issu des travaux d'un colloque international sur la police, organisé en 1972 par le Centre international de criminologie comparée de Montréal (CICC).

Cette date de 1972 est donc un point de repère important pour situer l'évolution de la réflexion intellectuelle et scientifique sur les questions policières dans le monde francophone. Aussi est-il intéressant d'en retrouver le contexte dans le livre d'entretiens que Denis Szabo a réalisé avec un de ses anciens étudiants, Marcel Fournier<sup>1</sup>. Celui-ci retrace d'abord l'itinéraire chaotique du jeune réfugié hongrois qui, ayant fui son pays en 1949,

a fait ensuite des études de sociologie en Belgique, avant de s'établir au Québec en 1958, où il va fonder, à l'Université de Montréal, l'École de criminologie et le centre international de criminologie comparée. Cet itinéraire et, en particulier, sa fréquentation des milieux intellectuels parisiens des années 53-56 l'amènent à prendre conscience de l'originalité de son approche pluridisciplinaire de la criminologie, qui faisait un large appel aux sciences humaines, sociologie et psychiatrie notamment, à une époque, qui n'est pas complètement révolue, où la criminologie était souvent seulement considérée comme un appendice plutôt mineur des études juridiques.

C'est au Québec que Denis Szabo va pouvoir mettre concrètement en application ses idées et ce n'est pas un des moindres intérêts de son témoignage que de voir comment s'est opérée sous son impulsion la construction sociale et institutionnelle d'une discipline scientifique, qui n'est pas seulement affaire, comme certains peuvent être tentés de le croire, de débats intellectuels, mais fait aussi appel à un esprit d'entreprise dont le fondateur du CICC ne manque pas. De ce fait, ce livre n'est pas aujourd'hui sans enseignement pour ceux qui s'efforcent d'institutionnaliser en France la sociologie des institutions et des questions policières. D'autant plus que

•••(1) FOURNIER (M.), 1998, *Entretiens avec Denis Szabo. Fondation et fondements de la criminologie*, Montréal, Liber, 228 p.

Denis Szabo lui-même rappelle les difficultés qui ont entouré le colloque de 1972, qui fut organisé à partir d'un slogan qui n'a pas perdu toute actualité : « *La police. On l'approuve ou on la critique. On ne l'étudie pas* ». À cette occasion, comme cela s'est produit ailleurs, Denis Szabo s'est heurté à la fois à une certaine méfiance des milieux policiers et à une censure idéologique prosolvant, dans le contexte des années post-68, toute réflexion intellectuelle sur ces questions, assimilée à une « compromission » universitaire inacceptable avec les institutions « répressives » de l'ordre établi.

Le mérite de Denis Szabo a été de persévérer dans les voies qu'il avait ouvertes en ne se laissant pas intimider par des conformismes, dont le temps a montré la fragilité et la relativité. En particulier, cette persévérance, liée à la situation géo-culturelle du Québec, a permis aux institutions dont il a été l'initiateur de constituer un lieu de confrontation et d'échanges entre le monde anglophone et le monde francophone. « *Comme les Européens, surtout les Français, parlaient encore très peu l'anglais et que les Américains connaissaient peu les Européens, nous étions, note-t-il, de véritables intermédiaires, une plaque tournante pour les sciences pénales et criminologiques* ». Ce rôle de « plaque tournante » qu'il évoque ici pour la criminologie en général, l'Université de Montréal l'a aussi joué pour les études sur les institutions policières et les questions de sécurité intérieure lorsque, notamment, les chercheurs français ont commencé à s'intéresser à ce champ de recherches. On rappellera par exemple ici que Jean Susini, qui sera dans les années 70-80 un des artisans, du côté français, de ces

échanges intellectuels, en se faisant l'écho des recherches nord-américaines dans ses « Chroniques de Police » de la Revue de Science Criminelle et de Droit Pénal Comparé<sup>2</sup> avait postfacé *Police, culture et société* et avait été pendant trois ans professeur associé à l'École de criminologie de Montréal au début des années soixante-dix.

Plus de vingt-cinq ans après la création du CICC, les travaux de ses chercheurs et de ses enseignants contribuent d'ailleurs toujours à animer, par dessus l'Atlantique, un dialogue intellectuel avec les chercheurs français, dont la fécondité est aujourd'hui renforcée par le fait que ces échanges ne sont plus à sens unique, comme ils ont eu tendance à l'être pendant un temps. De cette fécondité témoigne par exemple l'ouvrage *Criminologie actuelle*<sup>3</sup> de Maurice Cusson, professeur à l'École de criminologie de Montréal, dans lequel celui-ci s'efforce de faire le bilan des recherches les plus récentes, en illustrant l'approche interdisciplinaire de la criminologie dont Denis Szabo s'est voulu le pionnier, ce qui conduit Maurice Cusson, à envisager le phénomène criminel comme un « système » constitué d'éléments interdépendants, résultant de l'action des délinquants, des victimes et des agents de contrôle social. À la lumière de cette approche méthodologique, l'auteur de *Criminologie actuelle* examine les notions de délit et de délinquant, en consacrant un chapitre spécifique à la mafia et au crime organisé. La dernière partie montre que, dans cette même perspective systémique, l'analyse criminologique ne saurait se désintéresser du rôle structurant que jouent les agents de contrôle social - dont la police - dans l'évolution du phénomène criminel et

•••(2) Les principales de ces chroniques ont été réunies en 1982 à l'initiative du Centre d'études et de recherches sur la police de Toulouse (CERP) sous le titre *La police, une approche nouvelle* (Toulouse, Presses de l'IEP, épuisé).

(3) CUSSON (M.), 1998, *Criminologie actuelle*, Paris, PUF, 254 p.

Voir recension in *Les Cahiers de la sécurité intérieure*, n°33, NDLR. On pourra aussi se reporter à son ouvrage plus didactique *La Criminologie*, Paris, Hachette, 1998, 160 p.

donc dans son étude. Ceci explique, que, dans cette perspective extensive, la réflexion criminologique québécoise se soit intéressée plus tôt qu'en France aux recherches sur les institutions policières et sur leurs pratiques.

Maurice Cusson, pour sa part, envisage le contrôle social comme « *l'ensemble des moyens mis en œuvre par les membres d'une société dans le but spécifique de contenir et de faire reculer le nombre et la gravité des délits* ». L'intérêt des développements qu'il lui consacre est de montrer que les mécanismes du contrôle social constituent, eux aussi, un « système », dont les éléments sont en situation d'interdépendance. Ainsi, la réflexion sur le rôle et l'importance du contrôle social de type policier ne saurait se développer sans prendre en considération sa place dans le processus plus général de la sanction pénale, sans envisager ses interactions avec le développement de la sécurité privée, et sans étudier son articulation avec l'évolution des contrôles sociaux informels qui résultent notamment des pressions régulatrices que les membres des groupes de proximité exercent les uns sur les autres, ou des mesures non pénales de prévention situationnelle, qui ont pour effet, en agissant sur l'environnement de la délinquance éventuelle, de rendre plus difficile le passage à l'acte.

Plus largement, M. Cusson insiste aussi sur la coexistence au sein du système de contrôle social d'éléments publics étatiques et d'éléments sociétaux résultant des réactions de la société civile. Ceci l'amène à esquisser une histoire occidentale du contrôle social, mettant l'accent sur l'importance du rôle de la société civile - individus, familles, clans - jusqu'au XV<sup>e</sup> siècle,

puis sur la tendance à privilégier le rôle de l'État du XVI<sup>e</sup> siècle au milieu du XX<sup>e</sup>. Dans cette perspective, il souligne que la seconde moitié du XX<sup>e</sup> siècle se caractérise par un certain essoufflement de l'action publique, qui conduit à remettre en cause l'idée que la sécurité intérieure serait un monopole de la force publique et à redécouvrir l'importance des réactions sociétales et, notamment, du rôle socialisateur et régulateur joué par les groupes de proximité.

Le constat que fait ainsi Maurice Cusson est pour une part à l'origine du débat qui s'est ouvert depuis quelques années autour de la notion de « police communautaire » ou de « police de proximité ». Il s'agit en effet, à travers la mise en exergue de ces notions de souligner la nécessité d'associer la population, la société civile à l'action de la police contre l'insécurité. Tel est, par exemple, le point sur lequel insiste l'un des représentants de la police urbaine de Montréal, Maurice Chalom, dans un plaidoyer pour la « police de proximité » significativement intitulé *Le policier et le citoyen*<sup>4</sup> : « *L'une des principales solutions à l'insécurité et à la criminalité, écrit-il, est celle de la participation de ceux que cela affecte. La police doit faire sien le principe selon lequel il faut agir avec et pour le citoyen* ».

Pour cerner les problèmes théoriques et pratiques posés par la notion de police communautaire, une référence importante est constituée par l'ouvrage *La police professionnelle de type communautaire* publié sous la direction d'André Normandeau<sup>5</sup>. Celui-ci, qui fut le successeur de Denis Szabo à la tête de l'École de criminologie de Montréal, s'est fait le théoricien et le propagandiste de cette conception de la police, notamment à travers sa contribution à la

•••(4) CHALOM (M.), 1998, *Le policier et le citoyen*, Montréal, Liber, 164 p.

(5) NORMANDEAU (A.) (dir.), 1998, *La police professionnelle de type communautaire*, Montréal, éditions du Méridien, 2 tomes, 326 p. et 358 p.

réflexion prospective *Police. Défi 2000* organisée à l'initiative du ministère de l'intérieur du Canada et, aussi, du fait de son implication dans les expériences de police de proximité de la Communauté urbaine de Montréal.

Située dans la perspective du courant de réflexion nord-américain qui, avec Goldstein, tend à définir la fonction policière comme une fonction de «résolution des problèmes» («*problem solving policing*»), la police professionnelle de type communautaire (PPC) est définie par André Normandeau comme une «police d'expertise», supposant une compétence professionnelle de ses membres pour contribuer à la «résolution des problèmes», et comme une «police communautaire» fondée sur des rapports de partenariat avec la population et les différents acteurs de la vie sociale. Avec le célèbre article de Wilson et Kelling sur la police de voisinage et la théorie de la vitre cassée, cet ouvrage propose un certain nombre de textes de Young, Skogan, Barbara Jankowski sur les expériences canadiennes, américaines et françaises en la matière, en rappelant que de nombreuses autres polices s'orientent aussi plus ou moins explicitement dans cette direction.

Ces références permettent à André Normandeau de présenter une synthèse systématique très suggestive, qui recense vingt et un éléments constitutifs, selon lui, de la PPC : sept éléments idéologiques, sept éléments théoriques, sept éléments pratiques. Après quoi il envisage les dix «interrogations professionnelles» que cette approche peut entraîner sur ce qu'est le travail policier, en tentant d'évaluer les chances d'application de ce modèle, ce qui l'amène à recenser dix obstacles susceptibles d'entraver une réforme de ce type et sept motifs susceptibles d'en faciliter le succès. Cette approche permet au lecteur, au milieu

d'une littérature foisonnante, de disposer rapidement d'un ensemble de points de repère très éclairants sur ce que recouvre la notion de «police communautaire» et sur les enjeux théoriques et pratiques que comporte sa mise en œuvre.

L'intérêt de l'ouvrage dirigé par A. Normandeau est aussi un intérêt pratique. D'abord, en raison du guide de lecture qu'il propose pour explorer la documentation bibliographique disponible sur ces questions. Mais, surtout, parce que ce livre étudie comment les orientations théoriques de la PPC sont mises en œuvre à travers l'usage de la «méthode SARA» («Situation - Analyse - Réponse - Appréciation») par la Sûreté du Québec, la Police de la communauté urbaine de Montréal, la Police de Laval, la Gendarmerie royale du Canada. Par là cet ouvrage sera utile aussi bien aux professionnels qu'aux chercheurs, d'autant que sont fournis des documents internes émanant de ces diverses institutions, qui illustrent de manière extrêmement concrète ce type de stratégie, en proposant des exemples dont on peut envisager de tirer profit non seulement pour conceptualiser la notion de police de proximité mais aussi pour l'élaboration concrète de plans locaux de sécurité.

Dans une perspective organisationnelle et culturelle, cette approche de l'exercice de la fonction policière en des termes qui estompent ses aspects répressifs au profit de ses aspects préventifs, en mettant l'accent sur le rapprochement partenarial avec le public et les autres institutions sociales, ouvre un débat, sur lequel insiste particulièrement Maurice Chalom, concernant les conséquences que cela implique dans l'organisation et les pratiques des institutions policières. Rejoignant certaines remarques d'André Normandeau, il considère en effet que cette évolution des pratiques policières



devrait entraîner l'abandon d'un modèle traditionnel d'organisation qu'il qualifie de « paramilitaire », caractérisé par une structure hiérarchisée, centralisée et bureaucratifiée, repliée sur elle-même, fondée sur des rapports de communication de type surtout vertical, et privilégiant une gestion répressive des « problèmes » par la constitution d'unités policières spécialisées.

Au contraire, l'orientation de type communautaire impliquerait une organisation déconcentrée et décentralisée de la police, faisant davantage de place aux communications horizontales entre policiers et entre services, en accordant un rôle déterminant à la base des policiers « patrouilleurs » et « îlotiers », tout en associant à sa stratégie extensive de prévention sociale l'intervention de partenaires sociaux non-policiers. Ces changements correspondraient, selon M. Chalom, à une exigence culturelle de « démocratisation » de la police de Montréal que concerne plus spécifiquement son attention : *« Pour assumer pleinement sa nouvelle mission, la police doit se démocratiser. Bref, sans un changement radical de la mentalité policière, caractérisée, entre autres choses, par la méfiance envers le public, une compréhension restreinte du métier policier, une uniformité dans les modes de gestion et de contrôle et une observance du mot d'ordre « obéis et tais-toi », il y a peu de chances de voir ces principes s'enraciner ».*

Ceci dit, l'abondante littérature suscitée par la notion de police communautaire, qui tend plus ou moins à être présentée comme une panacée, peut susciter des interrogations, dont se fait l'écho Jean-Paul Brodeur dans une contribution critique au livre d'A. Normandeau. Il rappelle d'abord que le développement de la réflexion intellectuelle sur la police s'est trouvée en relation, depuis la deuxième guerre mondiale, avec

un mouvement plus général, militant pour une réforme de la police, particulièrement dans les pays anglo-saxons. Ce mouvement a donné naissance à une floraison de concepts, comme les unités locales de police, la police en équipe, la patrouille-contact avec les citoyens, la surveillance de voisinage, la police communautaire, la police de résolution des problèmes, ou encore les formes récentes de maintien de l'ordre ou de police intensive. Ce recensement est l'occasion pour Jean-Paul Brodeur de mettre en garde contre la tentation de s'évader dans la dogmatisation intellectuelle d'un type de solution, en négligeant la mise en œuvre concrète des réformes envisagées et les adaptations qu'impliquent les besoins du milieu dans lequel elles s'appliquent, d'autant, souligne-t-il, qu'un des problèmes pratiques soulevés par beaucoup de ces expériences est celui de la difficulté d'évaluer l'effectivité de leurs résultats.

Par ailleurs, avec la vigueur « déconstructrice » qu'on lui connaît, Jean-Paul Brodeur note que les différentes approches prétendant proposer « une nouvelle conception de la police » ne sont pas aussi convergentes et compatibles qu'on le prétend. Il s'attache ainsi à montrer que la police de résolution des problèmes prônée par Goldstein peut se trouver en contradiction avec l'orientation communautaire lorsque les solutions proposées et les intérêts de la police et du public ne coïncident pas. Ou bien encore, lorsque la police communautaire se transforme en politique de relations publiques et devient pour la police plus un moyen d'améliorer son image dans le public qu'un instrument de solution des difficultés qu'elle a à résoudre. Par ailleurs, il remarque une tendance des textes sur la police communautaire à escamoter les difficultés et les ambiguïtés de sa mise en œuvre. Ainsi note-t-il, à propos de l'ouvrage de M. Chalom qu'il a

préfacé, que ce livre «*fait à l'âpreté de la vie une part trop congrue et que son volontarisme de la résolution des problèmes méconnaît ce que j'appellerai, faute d'une meilleure expression, la force du négatif*».

Cette remarque peut, nous semble-t-il, s'appliquer aussi à la réflexion de J.P. Brodeur lui-même, qui peut paraître très timide par rapport à ce qui constitue pourtant le centre de la problématique de la «*police communautaire*», à savoir la notion de «*communauté*». Il effleure le problème, mais sans en tirer de conséquences, lorsqu'il constate que Goldstein distingue deux types d'engagement communautaire : «*Dans le premier cas, la police sollicite la participation permanente de la communauté toute entière ; dans le second cas, seule la partie de la communauté qui peut contribuer de façon permanente à la résolution d'un problème spécifique est mobilisée*». En fait, cette remarque incidente pose une question centrale : quelle est cette «*communauté*» avec laquelle la police doit dialoguer et concerter son action ? Est-ce l'ensemble du groupe social à «*policer*» ou est-ce seulement la partie du groupe susceptible de s'associer au travail entrepris ? Plus concrètement encore, qu'en est-il lorsque la «*communauté*» est divisée, hétérogène, et exprime des aspirations et des besoins contradictoires ? Avec qui la police va-t-elle et doit-elle dialoguer ?

On a le sentiment que la description qui est faite de la police communautaire postule souvent implicitement une société homogène, apte à exprimer des attentes cohérentes et à collaborer avec la police pour assurer sa sécurité, c'est-à-dire, finalement, une société dont le besoin de protection policière est en réalité limité ! En revanche, la mise en œuvre et le fonctionnement d'une police communautaire paraissent beaucoup plus aléatoires lorsque la société

est divisée, lorsque c'est justement cette division qui est cause d'insécurité et lorsque, de ce fait, cette société a particulièrement besoin de la police pour être régulée et pacifiée. Une «*police communautaire*» peut-elle alors arbitrer entre les pressions contradictoires qui déchirent une telle société ? Et le peut-elle en mettant uniquement en œuvre une gestion consensuelle des problèmes ? Autrement dit, cette solution, même si elle n'est pas totalement sans application dans ces hypothèses, est-elle «*la*» réponse dans les zones urbaines où la sécurité est la plus dégradée par la dislocation du tissu social ?

On le constate, ces débats nord-américains sur la police communautaire soulèvent des questions d'un grand intérêt aussi bien sur ce qu'est la police que sur ce qu'elle doit être. Toutefois, on peut se demander si la volonté réformatrice que l'on retrouve, malgré leurs divergences, chez A. Normandeau et J. P. Brodeur, n'a pas pour conséquence de biaiser parfois la rigueur de la démarche scientifique. En effet, le modèle de police qui est présenté, agissant pour le citoyen et avec le citoyen, afin d'assurer sa sécurité dans le cadre d'une action concertée avec tous les partenaires sociaux collaborant à la même entreprise, ne peut que susciter l'approbation et on ne peut que souhaiter voir les polices des sociétés démocratiques faire leur cet idéal d'évolution des pratiques policières.

Toujours de manière idéale, on ne peut que se réjouir de voir disparaître les notions de coercition, d'usage de la force, de répression, qui sont pratiquement absentes des considérations sur la police communautaire ou sont associées à une conception de la police considérée comme «*dépassée*», qui est stigmatisée sous le qualificatif de «*paramilitaire*».

Le problème est néanmoins de savoir si cette perspective normative ne conduit pas,

comme on l'a noté précédemment, à ignorer une partie de la réalité, en décrivant une police idéale fonctionnant dans des conditions sociales idéales. Ne privilégie-t-on pas ainsi une approche qui escamote plus ou moins les contraintes sociétales que l'on rencontre dans les zones qui connaissent justement les problèmes d'insécurité les plus aigus et dans lesquelles la police se heurte au plus grand nombre d'obstacles dans l'accomplissement de ses missions ? À trop privilégier la réflexion sur ce que devrait être la police, ne néglige-t-on pas ce qu'elle est, en oubliant que le discours unanime sur son rôle préventif n'empêche pas l'action de la police de conserver des aspects coercitifs et répressifs, que l'on ne saurait ignorer même si on les déplore. Par là, apparaît une source de tension possible entre les exigences de la recherche scientifique et la réflexion sur ses applications, qui renvoie d'ailleurs au caractère quelque peu ambigu du concept de « criminologie appliquée » dont se réclame l'école criminologique montréalaise.

En tout cas, ces ouvrages, très représentatifs de la diversité des chercheurs et des travaux de la criminologie québécoise, illustrent la vitalité d'un courant de recherche et de réflexion sur les institutions et les pratiques policières, qui, au carrefour du monde anglophone et du monde francophone, a contribué depuis une vingtaine d'années, pour une part non négligeable, au développement de la recherche française sur ces questions, comme en témoignent les relations personnelles et institutionnelles qui se sont créées entre les deux rives de l'Atlantique. Reconnaître cette dette et l'intérêt de ce dialogue n'implique pas cependant d'ignorer les divergences de points de vue qui peuvent naître de la prégnance parfois un peu envahissante des problématiques anglo-saxonnes ou de méconnaître la

spécificité de l'apport français à ces échanges, à partir d'expériences et de réflexions qui s'inscrivent dans un contexte historique, culturel et socio-administratif qui, sur certains points, est sensiblement différent du contexte nord-américain.

■ **Jean-Louis LOUBET DEL BAYLE**

*Directeur du CERP de l'IEP de Toulouse*

Pierrette PONCELA, Pierre LASCOUMES

*Réformer le code pénal ; où est passé l'architecte ?*

Paris, PUF, 1998, 309 p.

259

Les architectes du Nouveau Code Pénal (NPC) français du 1<sup>er</sup> mars 1994 n'ont pas laissé un monument à la postérité, ni donné une idée très originale des libertés réelles que le sujet politique d'aujourd'hui aurait été en droit d'attendre : le citoyen-salarié, consommateur, contribuable et qui plus est personne vivant dans un environnement menacé n'y trouve son compte. Pour comprendre comment le NPC a finalement produit cette conception très restrictive de la citoyenneté en réduisant la personne à la défense de son corps, de son honneur, de son intimité et de ses biens (un « homme partiel et démembré »), les auteurs se sont d'abord livrés à une subtile description de la structure interne du nouveau code. Ils l'ont fait dans le même esprit que lors d'un essai précédent concernant le code pénal de 1810 (cette revue, n° 18), c'est-à-dire en évaluant la cote des intérêts politiques, moraux, civiques, parmi l'ensemble des incriminations. Ainsi en 1994, outre un accroissement des délits, une très nette augmentation des longues peines, des peines complémentaires et de l'amende, ils observent que les incriminations pour la défense des intérêts politiques ont diminué (exception faite des infractions liées au terroris-

me) ; les incriminations défendant la « morale naturelle » sont restées stables, alors que se sont considérablement accrues celles qui défendent la « morale civique » et effondrées celles qui protègent les intérêts économiques et sociaux. Difficile par ailleurs de décider si le NCP est moins ou plus répressif que celui de 1810, bien que le nombre d'articles relatifs aux peines ait triplé entre temps, car si les textes sont plus nombreux, ils sont aussi de qualité plus incertaine : sans grands principes directeurs, le souci de la technique juridique l'a largement emporté dans l'économie générale du texte sur toute autre considération. Les auteurs concluent à un instrument davantage conçu pour les besoins techniques des juges de jugement que pour ceux des justiciables.

Ils procèdent ensuite à une enquête approfondie sur le travail technique des différentes commissions d'experts puis du travail politique des parlementaires. Pour évaluer l'impact de ce chantier, ils ont dépouillé les archives des 508 séances des commissions entre 1973 et 1990 et interrogé la plupart des acteurs clé de ces commissions. Bref, ils ont ouvert la boîte noire de la « mise en forme juridique de l'ordre public », le droit pénal constituant un terrain d'observation presque trop exemplaire des décisions publiques pour faire apparaître comment les enjeux sociaux sont sélectionnés et traduits en dispositions légales. Dans la reconstitution de ce processus, se matérialise le produit cristallisé d'interférences des positions et intérêts concurrents ou complémentaires des juristes, juges et politiques. Autrement dit, entre jurisprudence, doctrine et groupes d'influence politique, on voit se dessiner un incessant travail de ravaudage des échancrures dans la matière, la force d'inertie « auto-poïétique » des contraintes internes au champ juridique

empêchant la réelle concrétisation de véritables innovations mais permettant néanmoins de sauvegarder une cohérence technique à l'ensemble de l'ouvrage.

La première commission de réforme (1972 à 1981) qui n'a qu'une légitimité politique fragile reste cantonnée à un mandat purement technique et son travail ne résistera pas au choc de la « loi Sécurité et Liberté » de A. Peyreffitte en 1981. Les années soixante-dix se sont caractérisées, pour la commission instituée, par une démarche autoréflexive, pénalocentriste, autour de la « personnalité du délinquant » (cette notion organisant l'édifice). Il est d'autant plus remarquable qu'on ait réussi à stabiliser le champ du droit pénal économique et financier (dispositif fiscal et droit du travail notamment).

La deuxième commission (1981 à 1990) se voit au contraire immédiatement dotée d'une légitimité plus politique que technique, le nouveau Garde des Sceaux désirant fonder le code pénal dans un nouveau système de valeurs (les droits de l'homme). Or, si la première commission fut ignorée des décideurs politiques, la seconde fut bel et bien instrumentalisée par R. Badinter, qui, très investi en son sein, joua alternativement de son statut de président technicien, de ses réseaux dans le monde judiciaire, et bien sûr de sa position éminemment politique de Garde des Sceaux. Son travail s'en ressentit d'autant et les changements permanents dans l'exposé des motifs prouvent assez à quel point elle eut du mal à trouver une identité d'action. Le spectaculaire échec du livre 5 devant contenir l'ensemble des incriminations économiques et financières du NCP est l'occasion pour les auteurs de montrer très éloquemment comment, en dépit d'un investissement fort, ce projet capota pour des questions de balisage, de définition des catégories, de mobili-

sations d'alliés autour de l'enjeu à des moments différents, processus qui laissa au total une véritable friche.

On voit enfin le Parlement prendre, après 1989, le relais dans un rôle plus significatif que celui auquel nous ont habitués les analystes de la V<sup>e</sup> République : le compte rendu minutieux de ses activités le fait percevoir tour à tour comme un porte-parole, un arbitre et un décideur qui a besoin pour exister politiquement de réussir à promulguer le code avant les législatives de 93 parce que les socialistes les savent perdues d'avance. Face à ce qui ressembla à un marathon technique assez chaotique et peu glorieux, le Sénat fut assez habile pour réussir à imprimer un tour conservateur et répressif au texte final.

La preuve est faite qu'après quatre échecs de réforme successifs sur un siècle, une telle entreprise n'était pas impossible. Et cela, en dépit d'une absence totale de méthodologie dans l'élaboration des textes et en dépit d'une science politique sceptique qui avait tous les arguments à sa disposition pour prédire un nouvel avortement de l'entreprise !... Il fallait donc que la volonté d'y parvenir ne fût jamais prise en défaut, même si ce fut au prix d'importants compromis politiques et d'une émasculatation majeure du projet au moment où la délinquance économique et financière avait plus que tout autre besoin que lui soit opposée un corpus cohérent de règles pour être utilement contrée.

Les auteurs s'interrogent sur la nécessité d'un code pénal, « monument » à l'aube du troisième millénaire. Nous croyons toujours, quant à nous, à son utilité symbolique et pratique, à condition qu'on n'ait pas affaire à un code pénal cul-de-jatte.

■ **Frédéric OCQUETEAU**

IHESI et CNRS-GAPP

Nathalie DUCLOS

*Les violences paysannes sous la V<sup>e</sup> République*  
Paris, Economica, 1998, 281 p.

Plus que les autres Français, les agriculteurs ont déployé une étonnante capacité de mobilisation depuis les années cinquante. Leurs contestations, chroniques et souvent spectaculaires, ont ponctué la modernisation de l'agriculture. Pourtant, elles ont longtemps été ignorées des universitaires qui, à peu d'exceptions près, se sont penchés sur des traits plus conventionnels de la participation politique paysanne. Aussi, en étudiant les violences paysannes sous la V<sup>e</sup> République, Nathalie Duclos s'attaque-t-elle à un thème encore largement empreint de l'imagerie populaire des « jacques » et des « croquants ». La violence est-elle l'inévitable expression de la contestation paysanne, le reflet d'un particularisme sociologique immuable ? Ou est-elle un mode historique de la contestation paysanne, voué à disparaître avec l'interdépendance croissante de la société ? Dans la lignée des travaux sur la modernisation, Duclos avance la thèse d'une modération tendancielle de la violence paysanne. Le cas de la Bretagne, plus particulièrement étudié par l'auteur, est révélateur de cette tendance : « Tandis que la violence protestataire des années soixante était assez largement le fait de l'ensemble du monde paysan, celle des années quatre-vingt et quatre-vingt-dix est devenue beaucoup plus résiduelle » (p.33). Ni la persistance de foyers de violence, ni l'émergence de la « coordination rurale » ne viennent ébranler ce constat. Les jacqueries appartiennent à un temps révolu caractérisé par la position autarcique et la sujétion politique de la paysannerie. Par contraste, les mobilisations paysannes d'aujourd'hui sont marquées du sceau de la modernité. Elles s'inscrivent dans le cadre de la politique

nationale et de l'économie capitaliste, en même temps qu'elles en subissent les effets pacificateurs.

Pour démontrer cette thèse, Duclos puise dans deux traditions théoriques souvent présentées comme antagonistes : l'école de la « mobilisation des ressources » (MR) et celle dite de la « privation relative » (PR). Selon l'auteur, ces théories sont en réalité complémentaires : l'une (MR) « s'intéressant surtout aux modalités de formation et de maintien d'une mobilisation », l'autre (PR) spécifiant « les facteurs favorisant l'émergence d'un mouvement violent » (p. 10). De fait, la structure de l'ouvrage reflète cette division théorique du travail, la première partie s'attachant à décrire l'évolution des prédispositions à la violence, la deuxième mettant en lumière les « dilemmes de l'action » des syndicats agricoles. Duclos fait un effort louable pour dépasser la polémique stérile présentant indûment l'école de la PR comme un psychologisme réducteur. Ce croisement de perspectives se traduit en pratique par la consultation de sources riches et variées (données de presse, documents internes, témoignages d'acteurs) et le déploiement de méthodes complémentaires (dénombrement des événements protestataires et entretiens qualitatifs). Malgré cette honnêteté de ton et un travail de recherche considérable, l'auteur ne réussit pourtant pas vraiment à convaincre de l'ampleur de la modération de la violence ni de l'interprétation à en donner.

La fragilité des résultats de Duclos est en grande partie imputable à des choix empiriques discutables et à des carences méthodologiques. On s'interroge tout d'abord sur le choix de la Bretagne comme prisme d'analyse, alors que cette région est marquée par des traits politiques et culturels profondément idiosyncrasiques. La revendication autonomiste bretonne, affirmée

jusque dans le domaine de la représentation syndicale paysanne, incite à interpréter les résultats bretons avec circonspection, a fortiori lorsqu'il s'agit d'extrapolation. Le bref examen de l'intermède de la « coordination rurale » ne suffit d'ailleurs pas à renforcer la validité de la thèse de la pacification à l'échelon national, thèse qui nécessite pour le moins d'adopter une approche comparative. Autre regret, l'auteur décrit peu les fondations méthodologiques sur lesquelles s'appuie le dénombrement des mobilisations paysannes. Quels critères temporels et spatiaux ont guidé l'inclusion d'un événement protestataire et l'exclusion d'un autre ? Sur quelle base les onze années ont-elles été sélectionnées ? Quelles qu'en soient les raisons, ces carences affaiblissent la « lisibilité » des résultats du dépouillement et compromettent le rapprochement de ces résultats avec ceux d'autres études régionales ou sectorielles.

Reste l'interprétation de la « modération tendancielle » de la violence paysanne. L'argument est simple : la violence paysanne est l'expression, stratégiquement modulée par les états-majors syndicaux, des frustrations engendrées par le décalage entre attentes paysannes et réalisations. La démonstration, pourtant, révèle les limites de la thèse de la PR puisque la pacification du répertoire paysan s'est opérée malgré la « pérennisation d'une relative infériorité » (p. 85) économique et sociale des agriculteurs. L'auteur porte involontairement un coup fatal à l'école de la PR en soulignant les effets contraires de cette « infériorité relative », produisant un militantisme radical dans les années soixante puis une résignation croissante dans les années quatre-vingt (p. 89). De même, le fait que les paysans soient devenus « moins permissifs » à l'égard de la violence constitue davantage un indicateur supplémentaire de la pacification qu'une de ses causes. En fin de compte,

l'élément explicatif clé de la violence semble bien être «*l'existence de soutiens ou d'oppositions aux protestations*» (p.165), qu'ils soient médiatiques ou politiques, internes ou étrangers au monde paysan. On est au cœur de la problématique de la MR.

Séduisante, la tentative d'œcuménisme théorique de Nathalie Duclos s'avère finalement décevante. La complémentarité postulée de la MR et de la PR se brise au cours de l'analyse. La raison tient sans doute à ce que la divergence entre ces deux théories ne se résume pas à un simple problème de «priorités» analytiques que l'on pourrait résoudre par une division du travail appropriée. En réalité, l'école de la MR contient une explication sophistiquée de la violence - produit de l'interaction entre l'État et les militants - que l'auteur n'examine guère. En l'absence de véritable synthèse théorique, l'analyse des rapports entre État et activistes paysans apparaît comme la voie la plus prometteuse. C'est dans cette interaction que se façonnent les protestations paysannes. Ce sont donc dans les transformations de cette interaction- solidification puis reformulation du néo-corporatisme, mise en place de structures de décision contraignantes au niveau européen - qu'il faut rechercher la clé des changements du répertoire protestataire paysan.

■ **Christilla ROEDERER**

BRATTON (W.), KNOBLER (P.)  
*Turnaround : How America's Top Cop Reversed the Crime Epidemic*  
New York, Random House, 1998, 329 p.

L'abaissement général de la criminalité dans la plupart des grandes agglomérations américaines est un constat indiscutable. Certaines villes qui ont développé des stra-

tégies policières innovantes sont désormais érigées en exemple à suivre, et ce à l'échelle internationale. New York qui était auparavant considérée comme une capitale du crime et de la violence est maintenant couramment présentée comme une des villes les plus sûres des États-Unis.

L'ancien chef de la police new-yorkaise, William Bratton, propose dans un livre qui connaît un appréciable succès aux États-Unis, *Turnaround*, le récit de sa carrière personnelle, de son expérience professionnelle et de ses démêlés avec Rudolph Giuliani le très médiatique maire de New York.

De 1994 à 1996, Bratton a profondément transformé la stratégie et les méthodes du NYPD (*New York Police Department*) et de ses 38 000 agents, sur un plan organisationnel, philosophique et technique. Durant cette période, la criminalité a régulièrement et fortement baissé à mesure qu'il introduisait un style de management de la police inspiré du secteur privé. Bratton s'est concentré sur les raisons du crime et a mis en œuvre des réponses préventives et proactives en s'attachant à définir des objectifs précis pour tous les agents de son service et en insistant sur la responsabilité personnelle des officiers et des dirigeants. Les résultats, autour desquels la municipalité a su très efficacement communiquer, sont pour le moins frappants. Au début des années quatre vingt dix, on recensait plus de 2 200 meurtres par an, contre moins de 800 en 1997. En deux ans, le nombre d'agressions a baissé de 27 %, celui des meurtres de 39%, et celui des vols de 30 %.

Bratton a commencé sa carrière à Boston où il a observé les éléments les plus condamnables des services de police américains. Dans la liste des critiques qu'il dresse on peut relever la corruption, la brutalité, le népotisme, la politisation, et l'absurdité de certaines pratiques de management. Le



jeune officier s'est forgé une idée d'une éthique et d'une culture policière renouvelées, attentives aux performances personnelles et à la présence effective et visible des policiers dans la ville. Sous l'égide de l'ancien responsable de la police de Boston, Bob di Grazia, il a pris conscience de l'importance des petits désordres et des incivilités qui avaient un très fort impact sur la population en terme de qualité de vie et d'accessibilité des espaces publics.

Bratton est arrivée à New York en 1990, dont le maire était à l'époque David Dinkins, pour prendre la tête du service de sécurité des transports en commun. Il y a fait preuve d'une rare efficacité en transformant totalement l'ambiance d'un réseau métropolitain qui apparaissait inexorablement engagé dans une spirale de déclin. Développant une stratégie de sécurité concentrée sur la moindre effraction et le moindre désordre, Bratton a effectivement réussi sa politique de reconquête du territoire. Dans les relations qu'il avait alors avec la police de la ville il a constaté l'inertie et l'étanchéité à toute innovation du NYPD. Selon lui, la police new-yorkaise se souciait beaucoup moins de faire baisser la criminalité que d'esquiver les critiques de la population, des médias ou des responsables politiques.

En 1994, le nouveau maire, Giuliani, lui a confié le poste de responsable du NYPD. Leur ambition commune était de faire baisser la criminalité de 40 % en trois ans. Pour y parvenir Bratton a introduit une véritable révolution dans une police dépeinte comme une administration timorée, bureaucratique, totalement centralisée, sans visées réalistes, déconnectée de la réalité des quartiers. Il a provoqué un bouleversement dans une organisation routinisée, sûre d'elle même, mais appréciée très négativement par tous les habitants. Le cœur de sa stratégie était de rendre les agents, à tous les niveaux de la

hiérarchie, comptables du succès ou de la faillite de toute action entreprise contre la criminalité.

Bratton, véritable entrepreneur de police, s'est fortement appuyé sur la communication, les technologies de l'information ainsi que sur les acquis de la recherche en criminologie. Il considérait tout d'abord qu'il était absolument essentiel de disposer de tableaux de bord pour suivre avec précision l'impact des diverses tactiques entreprises. À cet effet, il participa à la conception d'un programme novateur, COMPAST (*Computerized Analysis of Crime Strategies*), qui autorise le suivi extrêmement précis des évolutions de la criminalité (statistiques, formes, localisation). Des réunions bi-hebdomadaires réunissant les principaux cadres du service permettaient, à partir des données ainsi traitées, de vérifier et d'évaluer l'action de chacun. Bratton faisait, fondamentalement, le pari de l'intelligence policière. Il permit effectivement au NYPD de créer et de bénéficier d'un système d'informations stratégiques qui a depuis fait école.

Bratton a également souhaité faire appliquer des principes et des théories issus de la recherche en criminologie, tels la certitude de la peine, la « vitre cassée » ou la « tolérance zero ». Sa stratégie s'appuie sur une règle des « trois p » : partenariat, prévention et problème à résoudre. Au fond de l'action de Bratton se trouve l'idée selon laquelle toute infraction à la loi doit être prévenue et, le cas échéant, punie. La question n'est pas celle de la sévérité de la peine, mais bien celle de la très forte probabilité de son application. Considérant le délinquant et le criminel comme des acteurs rationnels, la stratégie préventive et répressive de Bratton consiste à limiter les opportunités qu'ils peuvent trouver pour passer à l'acte, et à augmenter les coûts liés aux conséquences de leurs actes. Une attention particulière



porte sur les récidivistes, pour lesquels la sévérité augmente implacablement avec la répétition des méfaits. Enfin la politique de Bratton passe par le harcèlement permanent des incivilités. Tous les petits désordres dans l'espace public sont traqués par des patrouilles régulières afin de reconquérir des quartiers en y améliorant le sentiment de sécurité des habitants. L'arrestation des responsables de ces troubles mineurs à l'ordre public permet d'en limiter l'expansion, mais autorise également la résolution d'affaires plus graves car ces personnes se trouvent être des sources d'informations de première qualité concernant l'ensemble de la criminalité dans un quartier.

Une question en suspens est de savoir quelle part exacte de la réduction de la criminalité à New York est réellement attribuable à cette stratégie policière. Des changements démographiques, des transformations économiques et des évolutions dans le comportement des habitants, sont également des variables explicatives à prendre en compte. Il n'en reste pas moins que la politique mise en place par Bratton a suscité de nombreuses modifications qui ont eu incontestablement une influence sur la vie quotidienne de la plupart des quartiers new-yorkais.

Le livre de Bratton, dont certains passages relèvent tout de même de l'autocélébration excessive du « meilleur flic d'Amérique », est intéressant car il relate de l'intérieur une

expérience de stratégie policière, encensée ou abhorrée, qui commence à être bien connue. Sa lecture pose le problème, irrésolu, de l'explication complète de la baisse de la criminalité aux États-Unis. L'ouvrage soulève également la question des rapports entre une autorité locale, en l'occurrence un maire très habile politiquement, et un service de police qui en dépend. Les luttes personnelles entre Giuliani, récemment réélu en raison de son bilan positif en matière de lutte contre l'insécurité, et Bratton, qui avait déclaré vouloir se présenter à l'élection municipale, sont assez savoureuses à apprécier. Poussé à la démission par Giuliani, Bratton exprime par moments les rancœurs d'un employé qui s'estime injustement remercié.

Si Bratton semble peu se soucier des conséquences de sa politique sur les registres des droits individuels ou de l'augmentation de la population carcérale, s'il se présente de manière trop appuyée comme la victime innocente d'un maire dont il fait un portrait peu flatteur, il n'en propose pas moins dans *Turnaround* une analyse stimulante de sa pratique et de ses observations. Son livre est à recommander à tous ceux qui souhaitent s'informer sur les pratiques dites de « tolérance zero »<sup>1</sup> car il en expose avec vigueur tous les aspects positifs et en dévoile, en filigrane, toutes les difficultés.

■ **Julien DAMON**

*Université Paris IV*

•••(1) Au sujet de la « zero tolerance », on pourra lire NORMAN (Dennis) (dir.), *Zero Tolerance : Policing a Free Society*, Londres, Institute of Economic Affairs, 1997. Cet ouvrage collectif anglais rassemble les réflexions de quelques responsables policiers, dont William Bratton qui y présente ses thèses et méthodes.



## COLLOQUES ET RENCONTRES

Compte rendu du séminaire  
de Palma de Mallorca

Un séminaire sur l'harmonisation au niveau européen des statistiques de la criminalité, organisé par l'*Instituto de Estudios de Policia de Espana*, a rassemblé du 11 au 15 janvier 1999 à Palma de Mallorca une quarantaine de spécialistes venus de onze pays de l'Union européenne, de l'Europe de l'Est et des États-Unis.

Les pays représentés étaient l'Allemagne, la Belgique, l'Espagne, la Finlande, la France, la Hollande, l'Italie, l'Irlande, le Luxembourg, le Portugal, le Royaume-Uni, la Suède, la Hongrie, la République Tchèque et les États-Unis.

Ce séminaire s'inscrit dans le cadre du programme *Oisin* d'échanges, de formation et de coopération entre les services de police, financé par la Commission européenne. Les représentants des organismes internationaux (Interpol, Europol, Eurostat, la Commission européenne) ont dirigé les débats en précisant les travaux en cours et le cadre de futurs projets.

Les participants étaient pour la plupart des membres des services de police responsables de l'élaboration des statistiques ou des instituts de recherche chargés de leur analyse, qui ne sont pas, en règle générale, indépendants de la police. Lors des deux premiers jours, la présentation rapide des travaux effectués dans chaque pays a permis

la comparaison des moyens mis en œuvre, des pratiques et la définition d'axes de travail pour le reste du séminaire.

L'intervention du représentant du FBI, qui dispose d'un outil opérationnel centralisé de recueil et d'analyse de la criminalité, a mis en lumière le temps et la mobilisation nécessaire à l'établissement d'un système de statistiques harmonisé. Cela repose tout d'abord sur l'adhésion de tous les États au projet et donc à la définition exacte de l'objectif du système. Aux États-Unis où la criminalité n'est comparable ni en intensité, ni en densité à celle connue en Europe, cet instrument a un but opérationnel très clair : aider la police dans son action par une meilleure connaissance du crime.

Or, ce point de vue n'a pas fait l'unanimité au sein des participants. En effet, l'assistance était composée de policiers mais aussi de statisticiens, de chercheurs en sciences sociales. Ces derniers sont enclins à trouver dans les statistiques de quoi expliquer la délinquance par des facteurs socio-économiques et à essayer d'introduire celle-ci dans une réflexion plus générale intégrée au débat public. Toutefois les deux approches ne peuvent s'exclure mutuellement. Les statistiques de la criminalité peuvent tout autant permettre de mesurer l'action de la police que de connaître les causes de la délinquance.

Ainsi, il paraît nécessaire de définir précisément le contexte de la délinquance au niveau des faits mais aussi à un niveau agré-

gé de variables démographiques et socio-économiques. Seule la construction d'indicateurs pertinents peut permettre la mesure et la comparaison de l'évolution de la criminalité en Europe. Ceux-ci doivent couvrir l'étendue de la gamme du crime : de la petite délinquance, proche des préoccupations de la population, au crime organisé, proche des préoccupations des États. Notons que ces deux formes de criminalité ne sont pas indépendantes et que le crime organisé reste difficilement identifiable.

Deux ateliers se sont ainsi créés : l'un portant sur la mise en œuvre d'un système harmonisé de statistiques, l'autre sur la construction d'indicateurs contextuels de la délinquance. Le choix des infractions retenues comme base de travail par chacun des groupes a révélé des intérêts différents chez les participants. Dans le premier atelier, il a été question des homicides volontaires, des vols, des stupéfiants, de trafic d'armes à feu, de trafic d'êtres humains ; dans le second, des cambriolages, des agressions avec blessures, des vols de voiture.

Le Conseil de l'Europe a déjà fait réaliser une étude sur la définition légale des infractions en Europe qui devrait servir de base aux travaux à venir. On a considéré que les sources policières ne pouvaient constituer le seul indicateur de la connaissance du crime et qu'à ce titre, les enquêtes de victimation, utilisées dans la plupart des pays de l'Union, pourraient être des sources particulièrement riches d'informations. Des initiatives d'enquêtes communes ayant déjà vu le jour, elles pourraient être soutenues par les instances européennes. Pour cela, il a été considéré qu'un réseau d'experts réunissant tous les acteurs concernés devrait être créé et institutionnalisé.

La Commission européenne a déjà lancé, dans le cadre du programme Falcone de lutte contre le crime organisé, une étude

pilote concernant l'harmonisation des statistiques relatives aux vols de véhicules en Europe. L'IHESI a été chargé de ce travail. Ce délit, proche des préoccupations des citoyens, peut donner lieu à un trafic organisé, dépassant de loin les frontières de l'Union. Sa connaissance précise concerne directement d'autres acteurs comme les entreprises du secteur privé (assurances, industries automobiles).

Ces acteurs ont compris depuis fort longtemps que le besoin d'informations de qualité devait s'intégrer à une prise de décision réactive et globale. Ils disposent d'informations nominatives importantes qu'ils utilisent à un niveau agrégé mais aussi à un niveau individuel. Le degré de légalité et de confidentialité de l'utilisation des données individuelles risque d'être difficilement contrôlable, aussi le besoin de transparence doit-il susciter une réflexion approfondie.

Dans le cas de données policières, les participants au colloque ont estimé que le traitement devait se faire dans le souci constant du respect des libertés individuelles. Il appartient aux décideurs publics de bien préciser l'utilité, la mise en œuvre et les limites d'un système harmonisé de statistiques, dans un but de transparence. Ce séminaire a montré l'importance de la réappropriation par le citoyen du débat sur la sécurité en Europe, afin que l'Europe politique se construise dans le respect des règles d'un jeu démocratique institutionnalisé. Il a su percevoir à travers la question technique de la constitution de sources et données statistiques au service d'objectifs de lutte internationale contre le crime, le souci des droits de l'homme. C'est une première qu'il convenait de saluer.

■ **Pierre Varly**  
*statisticien - IHESI*

# ABSTRACTS

## THE PRINCIPLE OF PROPORTIONALITY

*Louise CADOUX*

The principle of proportionality, which can be applied by a judge without reference to any law, states that any limit - with the public interest as its justification - in the exercise of public freedoms by the individual must be strictly proportional to the objective to be attained. Extended to the domain of information technology, this principle is made use of by specific legal enactments embedded in the laws on Human Rights and linked to those relating to data protection.

## NEW TECHNOLOGIES, NEW OFFENCES

*Peter GRABOSKY, Russell G. SMITH, Paul WRIGHT*

The unprecedented criminal opportunities provided by Information Technology are fully described in this article. Faced with the global reach of telecommunications and while awaiting any hypothetical international regulation, the best solution remains, in the opinion of the writers, selfhelp and self-regulation.

## TIERS DE CONFIANCE OU DE DÉFIANCE COLLECTIVE SECURITY AND ASYMETRIC DATA ENCRYPTION

*Gaël BOISSEAU*

At present, data encryption is the only way of protecting Internet privacy. It has thus become an important subject of unceasing debate and changes in the Law within the context of globalization. Is security a collective issue and therefore the concern of governments or is it a basic individual right and as such subordinated to the individual's will alone? Confidentiality in an information-based society is the fundamental issue which is outlined and debated in this article.

## INTERNET AND THE RIGHT TO DATA PROTECTION

*Conseil d'Etat/Commission européenne*

Is the current experience of total freedom on the Internet the hallmark of a revolution that has not yet been fully understood or a manifestation of the impossibility of setting up a single legal framework in a global context? For the Council of State which submitted its report to the prime minister last July there is absolutely no need to apply a specific legislative framework to the world wide web. On the contrary, it is the type of service in question (mail, e-commerce etc.) which should specify the legal system to be applied. The conclusions of the Direction general XIII of the European Commission are imminent, with an interesting supplement on the future status of service providers and the requirement to register the territorial origin of websites.

## THE POLICE AND TECHNOLOGICAL INNOVATION

Nicole SOULLIÈRE

An historical analysis of technological progress shows that each technological innovation leads to a profound restructuring of police organisations. A description of the North-American situation would seem to indicate that the introduction of information technology redefines the role of the police officer and the structure of organisations. Finally, the potential for control brought about by these changes is fostering a new approach of power in terms of simulation.

## PROTEIFORM INTELLIGENCE

Nicholas Dorn

Over the last few years, the ad-hoc sharing of information between different state agencies has given way to the exchange of information between institutions in diverse spheres. While this meshing can largely be explained by the gradual advent of the pan-European co-operation of control agencies, it is also due to the revolution in information technology. The ensuing complexity poses the problem of quality and validity of intelligence systems and, according to the writer, contributes not inconsiderably to the social construction of the notion of organised crime.

## THE Y2K BUG : AN INDICATOR OF VULNERABILITY

Daniel Naulleau

The Y2K bug has made us aware of the vulnerability of information systems but beyond the financial losses, a worsening of civil liberties is to be feared. A new vulnerability is emer-

ging which arises from the complexity and incompatibility of systems, networks as well as human factors. We should appraise information systems on a systematic basis and educate people to recognise their exposure to risk. This is necessary if we are not to live under the illusion that the vulnerability of IT systems is only the affair of specialists.

## DATAS INSTITUTIONNAL EXCHANGE AND SECURITY FILES. A MODERN ISSUE

Joël Boyer

With the arrival of the information society, the methods of control and intervention of the CNIL (the IT regulatory body) must change so that information technology does not provide the means to do what the legislator has sought to proscribe. File transfer should remain exceptional and the use and communication of a social security number should be carefully controlled. As concerns the Criminal Investigation Department, the CNIL is in favour of more openness, notably by guaranteeing the right to indirect access. Finally, the increasing use of IT affecting our private lives leads the author to reflect on the right to be anonymous, a necessary feature of a balanced democratic society.

## HOUSE ARREST AND ELECTRONIC TAGGING : A NEW ECONOMY OF CONTROL

Jean Charles Froment

More than just a simple high-tech gadget, the use of an electronic bracelet modifies the economies and the meaning of punishment. First of all, in a positive way, it equates prison with

the deprivation of freedom at a precise moment in the history of punishment but it also brings back the idea of punishment as corporeal, marking the body. But this ideal is quickly demolished since, despite the effectiveness of this new form of punishment, the prison population is not going down? More generally, in the opinion of the writer, this change marks the advent of a society based on control at the expense of one based on punishment, in which political power is spreading and having a socialising, civilising influence.

#### **CAN ZERO TOLERANCE BE APPLIED IN FRANCE ?**

*Sebatian ROCHÉ*

The comparison of delinquency in two countries as different from each other as France and the United States in the level and type of delinquency can make us wonder why the sociological causes of crime debated in each country are so similar. A first line of enquiry is to ask whether the specifically New York response to crime

lies in a break with the attempt to find sociological causes in order to focus more on practical ways of reducing crime. However, given the differences between both countries, one is entitled to ask how appropriate the New York zero tolerance policy is in a French context.

#### **THE MOSAIC OF EXPERT LEGAL OPINION, THE PUBLIC AND PRIVATE SECTORS, MONOPOLY AND COMPETITION**

*Laurence Dumoulin*

The provision on the French market of expert legal opinion is particularly fragmented with a plethora of actors and authorities able to supply the legal establishment with knowledge and skills ranging from engineering science to genetic fingerprinting. While the providers of this expertise can be classified as belonging to either the public or the private sector, today these divisions are breaking down and both sectors blend and interweave, making a complex, kaleidoscopic mosaic.





# ONT CONTRIBUÉ

**Alain BELVEAU**, Commissaire principal, est actuellement chargé de Mission au Bureau des Projets de Police Opérationnelle à la Direction des Transmissions et de l'Informatique.

*Adresse : Direction des Transmissions et de l'Informatique (DTI), 7 rue Nélaton 75015 PARIS. email : alfredst@club-internet.fr*

**Gaël BOISSEAU** est diplômé en science politique et en management de l'information. Il pratique et enseigne l'intelligence stratégique sur l'Internet au sein du groupe HEC et au CNFPT. Ses recherches portent depuis 1993 sur le rôle de l'État au sein des réseaux de télécommunications. Il travaille plus particulièrement sur la gestion de la sécurité.

*Adresse : Groupe HEC, 1 rue de la libération, 78351 Jouy-en-Josas cedex.  
e-mail : boisseau@hec.fr.*

**Joël BOYER** est magistrat de l'ordre judiciaire. Substitut du procureur de la République du tribunal de Nîmes (1987-1989), il a ensuite exercé à la direction des affaires criminelles et des grâces du ministère de la Justice (1989-1993) avant d'être détaché à la CNIL en qualité de chef de service juridique. Il a été

nommé secrétaire général, chargé des affaires juridiques de la CNIL en novembre 1996.

*Adresse : Commission nationale de l'informatique et des libertés, 21 rue Saint-Guillaume, 75340 Paris cedex 07*

**Richard BROUSSE** est chargé d'enseignement à l'université de Paris X, Nanterre en science politique. Il est également membre de l'équipe éditoriale de la revue *Culture et conflits*. Il travaille actuellement sur les industries de sécurité et la construction des menaces.

*Adresse : Université de Paris X, 200 avenue de la République, 92000 Nanterre.*

**Nicholas DORN** est actuellement conseiller de l'unité de coordination anti-drogue du Royaume-Uni au cabinet du *Home Office* et directeur de l'ISDD à Londres (antenne anglaise de l'OEDT). Il a récemment été nommé coordinateur du programme *Eurocrime* (*Institute of Advanced Legal Studies* à l'université de Londres).

Son travail de recherche est désormais centré sur les droits national et européen et la lutte contre le crime organisé. Il a récemment publié *Regulating European Drug problems*, Kluwer, 1998. Au Royaume-Uni, il a mené plusieurs recherches pour le compte des services des douanes et droits indirects de sa Majesté, et a été consultant du Département d'évaluation des indicateurs de performance sur les marchés illégaux de drogues pour le gouvernement britannique.  
*e-mail : ecru@dial.pipex.com*

**Laurence DUMOULIN** est doctorante en science politique. Elle prépare une thèse sur l'expertise comme nouvelle raison politique au CERAT-CNRS/IEP de Grenoble. Elle participe actuellement à une recherche sur « Experts et expertises judiciaires en France. 1791-1939 », et contribue à une étude des « pratiques et politiques de gestion de la violence à l'école ». Elle a publié avec Thierry Delpeuch, « La justice : émergence d'une rhétorique de

l'usager», in WARIN (P.) (dir), *Quelle modernisation des services publics ? Les usagers au cœur des réformes*, Paris, La découverte, 1997, p. 103-129 ; avec Jacques Commaille et Cécile Robert (dir.), *Les approches et les démarches de recherche consacrées à la production normative*, LGDJ, à paraître.

Adresse : CERAT-IEP Grenoble, BP 38, 38040 Grenoble Cedex 9.

e-mail : Dumoulin@iepetud.upmf-grenoble.fr

**Isabelle FALQUE-PIERROTIN**, ancienne élève de l'École nationale d'administration (ENA-1986), est actuellement maître des requêtes au Conseil d'État. Après un détachement auprès du Groupe Bull (1991-1993), elle est directeur-adjoint de cabinet du ministre de la culture et de la francophonie de 1993 à 1995 ; présidente de la mission interministérielle sur Internet (1996) ; expert auprès de l'OCDE pour le développement de la coopération internationale sur Internet (1997) et rapporteur général du rapport du Conseil d'État sur « Internet et les réseaux numériques » rendu au Premier ministre en juillet 1998.

Adresse : Conseil d'État, place du Palais Royal, 75100 Paris 01 SP.

**Jean-Charles FROMENT** est maître de conférences de droit public à l'université P. Mendès France de Grenoble et chercheur au CERDAP (centre d'étude et de recherche sur le droit et l'administration publique). Spécialiste des questions pénitentiaires et de sécurité, il vient de publier *La République des surveillants de prison* (1958-1998), LGDJ, 1998, et travaille actuellement sur un ouvrage relatif à la nouvelle loi sur les polices municipales qui paraîtra à la *Lettre du cadre territorial*, dans une nouvelle collection consacrée aux polices territoriales qu'il dirige désormais.

Adresse : Faculté de droit de Grenoble-CERDAP, BP 47, 38040 Saint Martin d'Hères cedex

**Peter GRABOSKY** est directeur de recherche à l'Institut australien de criminologie (*Australian Institute of Criminology, Canberra*). Il est l'auteur de plusieurs ouvrages et articles sur la délinquance en col blanc, dont le plus récent, *Crime in the digital Age : Controlling Telecommunications and Cyberspace Illegality*, avec Russell Smith. Il est président de la société australienne et néo-zélandaise de criminologie.

Adresse : Institut australien de criminologie, GPO Box 2944, Canberra Act 2601, Australia.  
e-mail : Peter.Grabosky@aic.gov.au

**Jean GUISEL** est, depuis 1996, grand reporter au Point. En charge des questions de Défense et de renseignement, il est responsable de la rubrique cyberspace. À la suite de nombreux ouvrages, il vient de publier *Les pires amis du monde : les relations franco-américaines à la fin du xx<sup>e</sup> siècle*, Stock, 1999, 352 p.

Adresse : Le point, 75 avenue du Maine, 75014 Paris

**Kevin HAGGERTY** a récemment terminé son doctorat à l'université britannique de Colombie en sociologie et anthropologie. Sa thèse *Making Crime count* (Les comptes du crime), est une analyse de la production institutionnelle de statistiques criminelles dans la définition des pratiques de gouvernance. Il est le co-auteur avec Richard Ericson de *Policing the Risk Society*, university of Toronto Press, 1997. Il travaille actuellement à l'université de Toronto sur l'utilisation des empreintes génétiques en pratique judiciaire.

Adresse : Centre of Criminology, university of Toronto.

e-mail : kd.haggerty@utoronto.ca

**Yves HERNANDEZ** est, depuis 1998, adjoint au sous-directeur des télécommunications et de l'informatique. À la direction générale de la gendarmerie nationale (DGGN), il a occupé les fonctions de chef du Bureau des systèmes informatiques de gestion (BSIG) de

1989 à 1991) et de chef du Bureau de la conception et de la coordination (BCC : de 1994 à 1998)

Adresse : Fort de Rosny sous Bois, SDTI, 1 boulevard Théophile Sueur, 93111 Rosny sous Bois.

**Jean-Claude KARSENTY** est diplômé d'études supérieures de sciences économiques. Inspecteur général de l'administration, il est président de la commission de l'informatique et des télécommunications du ministère de l'Intérieur depuis 1994. Il a été auparavant président de la mission interministérielle de lutte contre la toxicomanie auprès du Premier ministre (1985), directeur de l'administration pénitentiaire au ministère de la justice (1990).

Adresse : 15 rue Cambacérès, 75008 Paris

**Paul LAGIER**, commissaire divisionnaire de la police nationale, est actuellement chef du Service central de documentation criminelle à la sous-direction de la police technique et scientifique.

Adresse : Sous-direction de la police technique et scientifique (SCDC), 31 avenue Franklin Roosevelt, 69134 Ecully cedex

**Daniel NAULLEAU**, Maître de Conférence en Informatique à l'Université P. et M. Curie, est président du CREIS (Centre de coordination pour l'enseignement et la recherche en informatique et société) et membre du comité de rédaction de la revue *Terminal* (l'Harmattan). Depuis 25 ans, il enseigne en Informatique et mène parallèlement un travail de

recherche et un enseignement sur les impacts de l'informatisation.

Adresse : ufr Informatique, Université P&M Curie, CREIS, 4 place Jussieu, 75252 Paris cedex 05.

e-mail : Daniel.Naulleau@ufr-info-p6.jussieu.fr

**Sebastian ROCHÉ** est politologue, chargé de recherche au CNRS (CERAT - Institut d'Études Politiques de Grenoble). Il enseigne à l'université de Lyon 3 et à l'université Paris V. Il est l'auteur de *La société incivile*, Paris, Seuil, 1996.

Adresse : CERAT, 1030, avenue centrale, domaine universitaire, BP 45, 38402 Saint Martin d'Hères cedex.

**Russell SMITH** est officier de recherche à l'AIC. Il est spécialisé sur les thèmes de la prévention et du contrôle de la fraude. Il a écrit en collaboration avec Peter Grabosky : *Crime in the digital Age : Controlling Telecommunications and Cyberspace Illegalities*.

e-mail : Peter.Grabosky@aic.gov.au

**Nicole SOULLIÈRE** est doctorante à l'École de criminologie de l'université de Montréal et assistante au Collège canadien de la police à Ottawa.

Adresse : soulliere@globetrotter.qc.ca

**Paul WRIGHT** est ingénieur des télécommunications et officier de recherche au *Western Australia Police Service*. e-mail : Peter.Grabosky@aic.gov.au



# INDEX DES AUTEURS

BASSON Jean-Charles

*Notes et études : Faut-il réprimer les violences scolaires ? A propos du centenaire de la loi du 19 avril 1898*

N°32, p. 175-187

BELVEAU Alain

Table ronde : *Information et sécurité*

N°34, p. 109-124

BERLIOZ Gilbert

*DES CCPD aux CLS : Articulation, superposition ou disjonction de deux logiques ?*

N°33, p. 89-104

BLANC Alain

*Décloisonnement et réinsertion : poursuivre l'ouverture*

N°31, p. 53-77

N°32, p. 237-261

BOISSEAU Gaël

*Tiers de confiance ou de défiance ?*

*La sécurité collective face à la cryptographie asymétrique*

N°34, p. 31-55

BOURGOIN Nicolas

*Le suicide en prison*

N°31, p. 229-238

BOYER Joël

*Le point de vue de la CNIL*

N°34, p. 135-147

BROUSSE Richard

TABLE RONDE : *Information et sécurité*

N°34, p. 109-124

BUI-TRONG Lucienne

*NOTES ET ÉTUDES : LES violences urbaines à l'échelle des RG. État des lieux pour 1998*

N°33, p. 215-224

BUI-TRONG Lucienne

*Notes et études (entretien avec) : Sur quelques secrets de fabrication*

N°33, p. 225-233

CADOUX Louise

*Point de vue : Le principe de proportionnalité*

N°34, p. 7-12

CASEY John J. Jr

*Les Fondamentaux de la sécurité : Gérer son business. La vie de l'usager d'héroïne*  
DANS LA RUE

N°32, p. 213-236

CHARRAS Igor

*L'État et les « stupéfiants » : archéologie d'une politique publique répressive*

N°32, p. 7-28

CHAUVENET Antoinette

*Guerre et paix en prison*

N°31, p. 91-109

CODINE JEAN-PASCAL

TABLE RONDE : *Information et sécurité*

N°34, p. 109-124

COLONEL HERNANDEZ

TABLE RONDE : *Information et sécurité*

N°34, p. 109-124

COMBESSIE Philippe

*Le pouvoir en prison : comme dans toute entreprise ?*

N°31, p. 111-121

CONSEIL D'ÉTAT, COMMISSION EUROPÉENNE

*Internet et le droit à la sécurité*

N°34, p. 57-67

CRAWFORD Adam

*Partenariat et responsabilité à l'ère managériale. Retour sur l'expérience britannique*

N°33, p. 51-87

CRETIEZ Xavier

NOTES ET ÉTUDES : *Lire la violence politique en Corse*

N°33, p. 195-214

DELORME Claire

*L'usage des drogues en milieu carcéral : approche épidémiologique*

N°31, p. 195-210

DELUMEAU Jean

Notes et études : *Peurs d'hier et peurs d'aujourd'hui*

N°32, p. 151-164

DEMONCHY Christian

*Architecture et évolution du système pénitentiaire*

N°31, p. 79-89

DERRAC Michel

*La Douane dans la lutte contre les stupéfiants*

N°32, p. 103-116

DONZELOT Jacques

*Magistrature sociale et souci du territoire. Les groupes locaux de traitement de la délinquance (GLTD)*

N°33, p. 149-174

DORN Nicholas

*Les nouvelles formes de renseignement policier*

N°32, p. 137-150

DORN Nicholas

*Du renseignement au partage des informations : l'intelligence protéiforme*

N°34, p. 91-108

DUBOUCHET LOUIS

*Des CCPD aux CLS : Articulation, superposition ou disjonction de deux logiques ?*

N°33, p. 89-104

DUMOULIN Laurence

*La mosaïque de l'expertise judiciaire : entre public et privé, monopole et concurrence*

N°34, p. 223-251

DUPONT Benoît

CHRONIQUE INTERNATIONALE : *Police, demande sociale et internet*

N°33, p. 235-244

ERICSON Richard V.

*La police dans la société du risque et de l'information*

N°34, p. 169-202

ESTÈBE Philippe

*L'émergence des politiques locales de tranquillité publique. L'exemple des pays de Loire*

N°33, p. 129-148

FAUGERON Claude

POINT DE VUE : *Réformer la prison ?*

N°31, p. 7-18

FRANQUET Jacques

*Drogues et toxicomanie dans le Nord. Les réponses policières*

N°32, p. 117-128

FRESSE Alexandra  
Notes et études : *Face aux inquiétudes, quelles stratégies ?*  
N°32, p. 165-174

FROMENT Jean-Charles  
*Les paradoxes de l'action collective des surveillants de prison depuis 1945*  
N°31, p. 151-170

FROMENT Jean-Charles  
*La prison à domicile sous surveillance électronique : une nouvelle économie du pouvoir de punir ?*  
N°34, p. 149-168

GOLDSTEIN Herman  
*Les fondamentaux de la sécurité : Améliorer les politiques de sécurité : une approche par les problèmes*  
N°31, p. 259-285

GRABOSKY Peter  
*Nouvelles technologies, nouveaux délits*  
N°34, p. 13-29

GRAPENDAAL Martin  
*Drogue et délinquance dans un contexte de tolérance. La situation à Amsterdam*  
N°32, p. 63-84

GUÉRIN Olivier  
*Quelle politique pénale ? L'exemple du tribunal de Lille*  
N°32, p. 129-136

GUILLONNEAU Maud  
*Les agressions de détenus envers les surveillants*  
N°31, p. 171-181

GUILLOT Yves  
TABLE RONDE : *Information et sécurité*  
N°34, p. 109-124

GUISNEL Jean  
TABLE RONDE : *Information et sécurité*  
N°34, p. 109-124

HAGGERTY KEVIN D.  
*La police dans la société du risque et de l'information*  
N°34, p. 169-202

HERZOG-EVANS Martine  
*Les particularités du droit pénitentiaire*  
N°31, p. 19-34

INGOLD Rodolphe  
LES FONDAMENTAUX DE LA SÉCURITÉ : *Gérer son business. Un commentaire du texte de E. PREBBLE et J. J. CASEY*  
N°32, p. 213-236

JOURNÈS Claude  
NOTES ET ÉTUDES : *Politiques de sécurité et syndicalisme policier en France et en Grande-Bretagne*  
N°31, p. 239-257

KARIM BEN DIANE Marc  
*L'usage des drogues en milieu carcéral : approche épidémiologique*  
N°31, p. 195-210

KARSENTY Jean-Claude  
TABLE RONDE : *Information et sécurité*  
N°34, p. 109-124

KENSEY Annie  
*Les agressions de détenus envers les surveillants*  
N°31, p.171-181

KOPP Pierre  
*Analyse économique des relations entre drogue et délinquance*  
N°32, p.29-45

LABROUSSE Alain

*L'approvisionnement des marchés des drogues dans l'espace Schengen*

N°32, p. 85-102

LAGIER Paul

TABLE RONDE : *Information et sécurité*

N°34, p. 109-124

LAGRANGE Hugues

*Du diagnostic à l'action : l'échelle pertinente du territoire*

N°33, p. 175-194

LÉON Hervé

*L'émergence des politiques locales de tranquillité publique*

L'exemple des pays de Loire

N°33, p. 129-148

LEUW Ed

*Drogue et délinquance dans un contexte de tolérance. La situation à Amsterdam*

N°32, p. 63-84

LHUILIER Dominique

*Surveillants de prison : identité professionnelle et crise de légitimité*

N°31, p. 135-150

MACÉ Éric

*La médiation : paradigmes et référentiels des politiques publiques de sécurité*

N°33, p. 7-20

MARCHETTI Anne-Marie

*Le travail en détention : un révélateur de la condition carcérale*

N°31, p. 183-193

MATHIEU Lilian

*Des significations de la sexualité en milieu carcéral*

N°31, p. 211-228

MONJARDET Dominique

*Professionnalisme et médiation de l'action policière*

N°33, p. 21-49

NAULLEAU Daniel

*Le bogue de l'an 2000 : un révélateur de la vulnérabilité de nos libertés*

N°34, p. 125-134

NELEN Hans

*Drogue et délinquance dans un contexte de tolérance. La situation à Amsterdam*

N°32, p. 63-84

OCQUETEAU Frédéric

*La sécurité privée en France. État des lieux et questions pour l'avenir*

N°33, p. 105-127

PAOLI Letizia

*Chronique internationale : Éléments pour une compréhension de la mafia en Italie*

N°32, p. 189-212

PARKER Howard

*Epidémies d'héroïne, carrières et réponses publiques au Royaume-Uni. 1980-1998*

N°32, p. 47-61

PREBLE Edward, CASEY John J.

*Les Fondamentaux de la sécurité : Gérer son business. La vie de l'usager d'héroïne dans la rue*

N°32, p. 213-236

ROCHÉ Sebastian

*La tolérance zéro est-elle applicable en France ?*

N°34, p. 203-233

ROSTAING Corinne

*La dynamique des relations dans les prisons de femmes*

N°31, p. 123-133



ROTILY Michel

*L'usage de drogues en milieu carcéral :  
approche épidémiologique*

N°31, p. 195-210

SMITH Russell G.

*Nouvelles technologies, nouveaux délits*

N°34, p. 13-29

SOULLIÈRE Nicole

*Polices et innovations technologiques*

N°34, p. 69-99

TOURNIER Pierre

*Les composantes de l'inflation carcérale*

N°31, p. 35-51

WELZER-LANG Daniel

*Des significations de la sexualité en milieu  
carcéral*

N°31, p. 211-228

WRIGHT Paul

*Nouvelles technologies, nouveaux délits*

N°34, p. 13-29

WYVEKENS Anne

*Magistrature sociale et souci du territoire.*

*Les groupes locaux de traitement de la  
délinquance (GTLD)*

N°33, p. 149-174



# INDEX DES NOTES BIBLIOGRAPHIQUES

BACHMANN C., LE GUENNEC N.

*Autopsie d'une émeute. Histoire exemplaire  
du soulèvement d'un quartier*

Paris, Albin-Michel, 1997, 233 p.

N°31, p. 301-303

par Jean-Paul Grémy

BRATTON W. KNOBLER P.

*Turnaround : How America's Top Cop  
Reversed the Crime Epidemic*

New York, Random House, 1998, 329 p.

N°34, p. 263-265

par Julien Damon

BRIDGEMAN C., HOBBS L.

*Preventing Repeat Victimisation : the police  
officer's guide*

Londres, Home Office Police Research  
Group, juin 1997

N°33, p. 249-250

par Jean-Paul Grémy

CHALOM M.

*Le policier et le citoyen*

Montréal Liber, 1998, 164 p.

N°34, p. 253-259

par Jean-Louis Loubet del Bayle

CRAWFORD A.

*The Local Governance of crime : Appeals to  
Community and Partnership*

Oxford, Clarendon, 1997

N°33, p. 256-262

par Jérôme Ferret

CUSSON M.

*Criminologie actuelle*

Paris, PUF, 1998, 254 p.

N°33, p. 251-254

par Frédéric Ocqueteau

DUCLOS N.

*Les violences paysannes sous la V<sup>e</sup>*

*République*

Economica, 1998, 281 p.

N°34, p. 261-263

par Christilla Roederer

ERICSON R. V., HAGGERTY K. D.

*Policing The Risk Society*

Oxford University Press, 1997, 487 p.

N°33, p. 245-248

par Maurice Punch

ESTERLE-HÉDIBEL M.

*La bande, le risque et l'accident*

L'Harmattan, coll. logiques sociales, 1997

N°31, p. 304-306

par Alain Quéval

FAGET J.

*La médiation, essai de politique pénale*

Éditions Érès-Trajets, 1997, 210 p.

N°33, p. 248-249

par Frédéric Ocqueteau

FAUGERON Cl., CHAUVENET A., COMBESSIE Ph.

*Approches de la prison*

De Boeck, collection perspectives crimino-  
logiques, avril 1997, 368 p.

N°32, p. 263-266

par Marianne Cattani

- FORST M. L. (dir.)  
*The Police and the Homeless*  
 Charles C. Thomas Publisher, Springfield,  
 1997, 233 p.  
 N°32, p. 269-271  
 par Julien Damon
- FOURNIER M.  
*Entretiens avec Denis Szabo. Fondation et  
 fondements de la criminologie*  
 Montréal, Liber, 1998, 228 p.  
 N°34, p. 253-259  
 Par Jean-Louis Loubet del Bayle
- GEISSER V.  
*Ethnicité républicaine : les élites d'origine  
 maghrébine dans le système politique fran-  
 çais*  
 Paris, Presses de Sciences-Po, 1997, 261 p.  
 N°31, p. 300-301  
 par Catherine Vionne
- INGOLD R., TOUSSIRT M.  
*Le cannabis en France*  
 Anthropos, 1998, 192 p.  
 N°32, p. 271-272  
 par Patrick Mignon
- KORF D.  
*Dutch Treat. Formal Control and illicit Drug  
 Use in the Netherlands*  
 Amsterdam, Thesis Publishers, 1995, 342 p.  
 N°32, p. 272-277  
 par Fabien Jobard
- LEPOUTRE D.  
*Cœur de banlieue, codes, rites et langages*  
 Paris, Odile Jacob, 1997, 362 p.  
 N°31, p. 306-310  
 par Françoise Impériali

- MARCHETTI A.-M.  
*Pauvretés en prison*  
 Ramonville Saint-Agne, éditions Érès,  
 Collection Trajets, 1997, 222 p.  
 N°31, p.287-294  
 par Manuela Ivone Cunha
- NORMANDEAU A.  
*La police professionnelle de type commu-  
 nautaire*  
 Montréal, éditions du Méridien, 2 tomes,  
 1998, 326 p., 358 p.  
 N°34, p. 253-259  
 par Jean-Louis Loubet del Bayle
- PONCELA P., LASCOUMES P.  
*Réformer le code pénal ; où est passé l'archi-  
 tecte ?*  
 Paris, PUF, 1998, 309 p.  
 N°34, p. 259-261  
 par Frédéric Ocqueteau
- REVUE FRANÇAISE DES AFFAIRES SOCIALES  
 « Insertion, intégration : concepts et pra-  
 tiques »  
 Ministère de l'emploi et de la solidarité, la  
 documentation française, 51<sup>e</sup> année, n°2,  
 avril-juin 1997, 291 p.  
 N°33, p. 254-256  
 par Abdelhag Rharade
- REVUE FRANÇAISE DES AFFAIRES SOCIALES  
 « La santé en prison : un enjeu de santé  
 publique »  
 janvier-mars 1997  
 N°31, p. 295-299  
 par Arnaud Lerch
- ROCHÉ S.  
*Sociologie politique de l'insécurité ; vio-  
 lences urbaines, inégalités et globalisation*  
 Paris, PUF, 1998, 283 p.  
 N°31, p. 311-313  
 par Frédéric Ocqueteau

ROSTAING C.

*La relation carcérale. Identités et rapports sociaux dans les prisons de femmes*

Paris, PUF, Collection le lien social, 1997

331 p.

N°31, p. 287-294

par Manuela Ivone Cunha

WELZER-LANG D., MATHIEU L., FAURE M.

*Sexualités et violences en prison*

Observatoire national des prisons, Aléas

éditeur, 1997 (1<sup>re</sup> ed. 1996), 280 p.

N°32, p. 266-269

par Léonore Le Caisne



- N°0 Actes du colloque des 2,3/11 1989  
novembre 1989
- N°1 *Les Français et l'insécurité*,  
avril-juin 1990
- N°2 *L'offre publique de sécurité*,  
juillet-septembre 1990
- N°3 *Le marché de la sécurité privée*,  
nov. 1990-janv. 1991
- N°4 *La mesure de la délinquance*,  
février-avril 1991
- N°5 *Jeunesse et sécurité*,  
mai-juillet 1991
- N°6 *La gestion de crise*,  
août-octobre 1991
- N°7 *Polices en Europe*,  
nov. 1991-janv. 1992
- N°8 *Police et démocratie à l'Est*,  
février-avril 1992
- N°9 *La police de l'environnement*,  
mai-juillet 1992
- N°10 *La sécurité des réseaux*,  
août-octobre 1992
- N°11 *Gendarmeries et  
polices à statut militaire*,  
nov. 1992-janv. 1993
- N°12 *Police et médias*,  
février-avril 1993
- N°13 *Systèmes de police comparés  
et coopération (I)*,  
mai-juillet 1993
- N°14 *Systèmes de police comparés  
et coopération (II)*,  
août-octobre 1993
- N°15 *La violence à l'école*,  
1<sup>er</sup> trimestre 1994
- N°16 *Collectivités locales et sécurité*,  
2<sup>e</sup> trimestre 1994
- N°17 *Ordre public et histoire*,  
3<sup>e</sup> trimestre 1994
- N°18 *Le nouveau code pénal*,  
4<sup>e</sup> trimestre 1994
- N°19 *Sécurité sans frontières*,  
1<sup>er</sup> trimestre 1995
- N°20 *Médias et violence*,  
2<sup>e</sup> trimestre 1995
- N°21 *Les technologies de sécurité*,  
3<sup>e</sup> trimestre 1995
- N°22 *Les métiers de l'urgence*,  
4<sup>e</sup> trimestre 1995
- N°23 *Délinquances quotidiennes*,  
1<sup>er</sup> trimestre 1996
- N°24 *Entreprise et sécurité*,  
2<sup>e</sup> trimestre 1996
- N°25 *Routes, espace incertain*,  
3<sup>e</sup> trimestre 1996
- N°26 *Football, ombres au spectacle*,  
4<sup>e</sup> trimestre 1996
- N°27 *Maintien de l'ordre*,  
1<sup>er</sup> trimestre 1997
- N°28 *Violences en famille*,  
2<sup>e</sup> trimestre 1997
- N°29 *Un péril «jeunes» ?*  
3<sup>e</sup> trimestre 1997
- N°30 *Le renseignement*,  
4<sup>e</sup> trimestre 1997
- N°31 *Prisons en société*,  
1<sup>er</sup> trimestre 1998
- N°32 *Drogue*,  
2<sup>e</sup> trimestre 1998
- N°33 *Les partages de la sécurité*,  
3<sup>e</sup> trimestre 1998
- N°34 *Risque et information*,  
4<sup>e</sup> trimestre 1998
- N°35 *Le lien familial*,  
1<sup>er</sup> trimestre 1999