Document generated on 01/22/2025 10:37 a.m.

Criminologie

Les morphologies de la sécurité après le 11 septembre : hiérarchies, marché et réseaux

Benoît Dupont

Volume 38, Number 2, Fall 2005

La police en pièces détachées

URI: https://id.erudit.org/iderudit/012665ar
DOI: https://doi.org/10.7202/012665ar

See table of contents

Publisher(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (print)
1492-1367 (digital)

Explore this journal

Cite this article

Dupont, B. (2005). Les morphologies de la sécurité après le 11 septembre : hiérarchies, marché et réseaux. *Criminologie*, *38*(2), 123–155. https://doi.org/10.7202/012665ar

Article abstract

The 9/11 attacks have highlighted the capacity of terrorist networks to strike and inflict extensive damages, as well as the helplessness of traditional vertical state institutions to confront this new threat. One of the solutions offered by security practitioners is to enlist the networked mode of organization in order to make the fight against terrorism and organized crime more effective. However, as we will show in the first section, the discourse on the prominence of networks preceded the 9/11 events, allowing a quick implementation of those recommendations in the US, Europe and Canada. Far from being an isolated phenomenon, the institutional and temporal reach of the network paradigm will be examined in the second section. This description and the contextual framework provided earlier will shed a factual light to the third section, which will initiate a theoretical discussion on the value of the network concept to understand the governance of security post 9/11.

Tous droits réservés © Les Presses de l'Université de Montréal, 2005

This document is protected by copyright law. Use of the services of Érudit (including reproduction) is subject to its terms and conditions, which can be viewed online.

https://apropos.erudit.org/en/users/policy-on-use/

érudit

This article is disseminated and preserved by Érudit.

Érudit is a non-profit inter-university consortium of the Université de Montréal, Université Laval, and the Université du Québec à Montréal. Its mission is to promote and disseminate research.

https://www.erudit.org/en/

Les morphologies de la sécurité après le 11 septembre : hiérarchies, marché et réseaux

Benoît Dupont

Professeur adjoint, École de criminologie
Chercheur au CICC (Centre international de criminologie comparée)
Université de Montréal
benoit.dupont@umontreal.ca

RÉSUMÉ • Les attentats du 11 septembre ont mis en lumière la capacité d'action et de destruction des réseaux terroristes et l'impuissance des institutions étatiques traditionnelles verticales face à cette nouvelle forme de menace. L'une des solutions proposées par les praticiens de la sécurité est de recourir à l'organisation en réseau afin de rendre plus efficace la lutte contre le terrorisme et le crime organisé. Cependant, comme nous le montrerons dans la première partie, le discours sur la prééminence des réseaux précédait les attaques du 11 septembre 2001, ce qui a permis une mise en œuvre rapide aux États-Unis, en Europe et au Canada. Loin de constituer un phénomène particulier, les dimensions diachronique et synchronique des réseaux de sécurité seront abordées dans la deuxième partie. Cette description et cette mise en contexte fourniront un éclairage factuel à la troisième partie, qui amorcera un débat théorique sur la valeur du concept de réseau pour comprendre la gouvernance de la sécurité après le 11 septembre.

ABSTRACT • The 9/11 attacks have highlighted the capacity of terrorist networks to strike and inflict extensive damages, as well as the helplessness of traditional vertical state institutions to confront this new threat. One of the solutions offered by security practitioners is to enlist the networked mode of organization in order to make the fight against terrorism and organized crime more effective. However, as we will show in the first section, the discourse on the prominence of networks preceded the 9/11 events, allowing a quick implementation of those recommendations in the US, Europe and Canada. Far from being an isolated phenomenon, the institutional and temporal reach of the network paradigm will be examined in the second section. This description and the contextual framework provided earlier will shed a factual light to the third section, which will initiate a theoretical discussion on the value of the network concept to understand the governance of security post 9/11.

> Le pouvoir des flux prend le pas sur les flux de pouvoir. La présence ou l'absence dans le réseau et la dynamique de chaque réseau par rapport aux autres sont la source essentielle de la domination et du changement dans la société en réseau, dans la mesure où la morphologie sociale l'emporte sur l'action sociale (Castells, 2001 : 575).

Les attentats du 11 septembre ont mis en lumière la capacité d'action et de destruction du réseau terroriste Al Qaeda, et l'impuissance des institutions étatiques états-uniennes face à cette nouvelle forme de menace. Les rapports officiels d'analyse des dysfonctionnements des services de police et de renseignement ont soulevé le problème de l'inertie bureaucratique et de l'absence de collaboration entre des agences gouvernementales ossifiées dans des particularismes culturels et des luttes d'allure picrocholine. Un des exemples frappants de ce manque de coordination est le nombre de bases de données qui contenaient des informations sur 15 des 19 terroristes directement impliqués : pas moins de 12 fichiers gérés par 9 agences gouvernementales ont été recensés, et, néanmoins, aucune alerte n'a pu être lancée à temps (GAO, 2003). Pour leur part, les membres d'Al Qaeda, organisés en cellules semi autonomes et néanmoins parfaitement coordonnées, se servaient du réseau informatique mondial pour effectuer en ligne leurs réservations de billets à l'aide de cartes de crédit et de numéros de voyageurs réguliers, contournant ainsi les systèmes automatiques d'alerte déclenchés par des comportements « suspects » prédéterminés. Devant une telle asymétrie de moyens, la question posée de manière récurrente fut celle de l'adaptation des structures policières dans la lutte qui les oppose à des formes de criminalité et de terrorisme entrées résolument dans l'ère de la mondialisation.

L'histoire des institutions policières met en lumière l'influence du modèle militaire d'organisation du travail, qui par son système pyramidal de commandement et son code disciplinaire rigide, permet d'exercer un contrôle permanent sur chaque membre de l'organisation. Ce choix s'explique par la volonté de limiter le pouvoir discrétionnaire des agents, source potentielle de déviances, mais aussi par le désir illusoire de rendre l'intervention policière aussi efficace que celle des unités militaires. Les services de police du monde entier consacrèrent ainsi la majeure partie du XX^{e} siècle à l'implantation d'un modèle fortement hiérarchisé et autarcique, privilégiant l'intervention d'urgence et limitant les contacts avec l'environnement immédiat afin de ne pas distraire la vigilance des

agents et les détourner de leur mission première. Les limites de ce modèle devinrent évidentes dès les années 1970, sous la pression d'une criminalité acquisitive exponentielle et de profonds changements sociaux (mondialisation des échanges économiques et culturels, intégration des femmes et des minorités visibles dans la sphère politique, éclatement et dématérialisation des attributs de l'identité). La réponse des services de police à ces changements prit la forme d'un discours proclamant une foi retrouvée dans le service à la communauté et la proximité dans les relations avec les citoyens. Derrière la rhétorique communautaire et le foisonnement de déclarations de principes, bien peu d'actions durables permirent de conclure à un réel changement des pratiques policières (Brodeur, 2003). Certains chercheurs notèrent même une recrudescence des stratégies paramilitaires dans la lutte contre la criminalité (Kraska, 2001). Simultanément, le secteur privé de la sécurité sut répondre à la demande de protection des individus et des entreprises, et il connaît, depuis plusieurs décennies, une croissance soutenue (Ocqueteau, 2004). Le marché offre aujourd'hui une palette infinie de prestataires qui proposent leurs services ou leurs technologies à des commanditaires privés, communautaires ou même publics (Bayley et Shearing, 2001).

La notion de privatisation et la dichotomie artificielle qu'elle introduit entre une hiérarchie étatique d'un côté et un marché ouvert de l'autre occulte cependant le décloisonnement institutionnel et la nature complexe des interactions qu'entretiennent les acteurs de la sécurité. Ces derniers, loin de pouvoir être catégorisés selon un système binaire, doivent plutôt être placés sur un continuum aux extrémités duquel figureraient la police et les entreprises de sécurité privée à contrat, et dont le segment central accueillerait les organisations hybrides. La pluralité et la diversité des acteurs que ce continuum permet de représenter introduit incidemment la question de leurs relations. La connaissance des organisations opérant dans un même champ ne peut en effet être entière sans que ne soit étudiée l'architecture générale de leurs liens d'interdépendance.

Dans cette perspective, le concept de réseau et les outils méthodologiques conçus pour son étude paraissent offrir un pouvoir explicatif fort pour comprendre la gouvernance de la sécurité[1]. Trois usages du terme

1. La gouvernance de la sécurité peut être définie comme la « constellation d'institutions, formelles ou informelles, gouvernementales ou privées, commerciales ou bénévoles qui participent au contrôle social et à la résolution des conflits, et qui tentent de mitiger les menaces (immédiates ou anticipées) qui découlent de la vie en collectivité » (Dupont *et al.*, 2003). Elle englobe également les processus de coordination à l'œuvre au sein de cette constellation.

« réseau » doivent être distingués. Tout d'abord, les réseaux de nos vies quotidiennes consistent en des dispositifs spatiaux et technologiques réticulaires facilitant la circulation des personnes, des biens ou de l'information. Ensuite, l'usage métaphorique du terme « réseau » connaît une popularité proportionnelle au rôle central pris par les réseaux concrets dans l'économie mondialisée. Finalement, les sciences sociales attribuent au concept de réseau une signification beaucoup plus abstraite. Manuel Castells, par exemple, définit le réseau comme « un ensemble de nœuds interconnectés. Un nœud est un point d'intersection d'une courbe par elle-même. La réalité d'un nœud dépend du réseau auquel il appartient » (2001 : 576). Emmanuel Lazéga, pour sa part, définit un réseau social comme « un ensemble de relations d'un type spécifique (par exemple, de collaboration, de soutien, de conseil, de contrôle ou d'influence) entre un ensemble d'acteurs » (1994 : 293). Cette troisième signification servira de point de référence à notre réflexion.

Les travaux de nombreux anthropologues ont bien mis en évidence l'ancienneté de la forme d'organisation en réseau (Stinchcombe, 1989). Cependant, les réseaux organisationnels ont été longtemps surpassés en efficacité par les hiérarchies centralisées et les marchés. C'est la révolution informationnelle de la fin du XX^{e} siècle qui leur aurait permis de surmonter les problèmes de coordination et d'échelle qui les handicapaient, les amenant à exploiter pleinement la flexibilité et l'adaptabilité qui les caractérisent (Castells, 2000 : 15). La puissance évocatrice du concept, dans un monde complexe dont les frontières s'estompent, a alors favorisé la propagation d'arguments apologétiques proclamant la supériorité des réseaux sur les autres morphologies sociales. Cette convergence de facteurs a servi de tremplin aux incantations normatives de ceux qui appellent à l'abandon des hiérarchies, tout en dénonçant les dysfonctionnements du marché. Aux rigidités bureaucratiques, le réseau opposerait ainsi un fonctionnement fluide et réactif, gage d'efficacité et d'efficience, basé sur la confiance personnelle et institutionnelle qui lie ceux qui le constituent. Cette flexibilité ne reposerait pas uniquement sur des arbitrages aveugles et compétitifs de maximisation des profits, comme on peut en rencontrer dans les situations de marché, mais se manifesterait aussi bien à des fins économiques que dans des contextes d'offres de services publics ou d'entraide communautaire. Les membres du réseau s'appuieraient alors sur des valeurs communes et une forte interdépendance pour s'autoréguler et éviter les situations de domination et d'exclusion produites par les dysfonctionnements du

marché. Ces avantages attribués aux réseaux doivent cependant être modulés : de nombreux réseaux criminels ou terroristes (ou *dark networks*, Raab et Milward, 2003) tirent leur efficacité tout autant de la confiance régnant entre leurs membres que de la terreur qu'ils inspirent à ceux qui gênent leurs activités. Par ailleurs, s'ils présentent, en effet, un degré de coordination supérieur au marché, les réseaux restent bien souvent des entités qui se forment de manière spontanée, autour de besoins ponctuels, et qui répondent mal aux injonctions des politiques publiques et à leurs exigences évaluatives.

Dans le champ de la sécurité, les attentats du 11 septembre ont, semble-t-il, joué le rôle de catalyseurs. Le contraste saisissant, diffusé sur tous les écrans du monde, entre, d'une part, le pouvoir destructeur d'un réseau international de quelques centaines de terroristes, et, d'autre part, la défaillance des plus puissants services de sécurité de la planète, n'a pas manqué de produire des effets dont il est encore difficile d'évaluer la portée. Toutefois, le démembrement méthodique des barrières séparatrices entre sécurité intérieure et sécurité nationale, sécurité publique et sécurité privée, renseignement criminel et renseignement de sécurité, données publiques et données privées, paraît être un « fait accompli ».

Sous la pression d'intérêts divers, la rhétorique de la mise en réseau et de l'échange massif d'information est devenue le nouveau mantra des services de police et de renseignement. Nous montrerons dans la première partie de cet article comment elle existait en germe avant les attaques du 11 septembre, et comment elle était utilisée aux États-Unis, en Europe et au Canada. Loin de constituer un phénomène isolé, les dimensions diachronique et synchronique des réseaux de sécurité seront abordées dans la deuxième partie. Cette description et cette mise en contexte fourniront un éclairage factuel à la troisième partie, qui amorcera un débat théorique sur la valeur du concept de réseau pour comprendre la gouvernance de la sécurité après le 11 septembre. Cette démarche exploratoire qui prend le parti d'examiner tour à tour quelques manifestations propres à un phénomène, avant de se questionner successivement sur ses particularités historique, fonctionnelle et théorique ne peut prétendre à l'exhaustivité, et cette limite doit être clairement établie. En effet, les observations dont on dispose relèvent encore plus de l'intuition agrémentée de faits concordants que d'un appareil empirique solidement étayé et méthodologiquement robuste, tout du moins en ce qui concerne le champ de la sécurité. Par ailleurs, devant l'ampleur du

phénomène étudié[2], et l'« insaisissabilité » qui en découle, on a jugé préférable de procéder par touches successives, en ayant recours à la métaphore picturale de l'expressionnisme. Au détriment d'une interprétation cohérente se déployant dans une progression élégante, on privilégiera la mise en lumière de perspectives complémentaires dont les agencements restent encore à préciser.

1. La sécurité intérieure mise en réseau ou la rhétorique postterroriste

Quelques jours après les attaques contre New York et Washington, une coalition tacite de journalistes, de chercheurs, d'entrepreneurs et de hauts fonctionnaires du Pentagone proclama l'inefficacité des structures verticales face aux menaces asymétriques non étatiques que posent les groupes terroristes contemporains[3]. Afin d'affronter celles-ci, ils préconisèrent notamment, de façon plus ou moins explicite, la mise en réseau des institutions militaires, policières et de renseignement, seule capable, selon eux, de surmonter la pesanteur bureaucratique à laquelle fut attribué l'effet de surprise. Comme le déclara l'un d'entre eux au *Washington Post*: « Nous utilisons un tank pour arrêter un tank. Nous devons utiliser un réseau pour détruire un réseau » (Arquilla et Ronfeldt, 2001, cité dans Garreau, 2001). Quelques mois plus tard, une publication professionnelle destinée aux cadres de la fonction publique fédérale reprenait ces propos et sommait ses lecteurs d'adopter les modes de pensée et d'action des réseaux (Friel, 2002).

La guerre des réseaux

Cette coalition trouve ses racines dans les travaux d'un pôle de chercheurs associés à la *Rand Corporation*, qui explorent depuis plusieurs

2. On en jugera simplement à travers les trois volumes consacrés par Manuel Castells au sujet, qui totalisent plus de 1400 pages, sans citer les travaux consacrés depuis plusieurs décennies par les sciences dites « dures » à la théorie des graphes ou aux propriétés nodales de certains phénomènes physiques et biologiques (Barabasi, 2002).

3. Des articles dans le *Washington Post* (Garreau, 2001) et la revue *Business 2.0* (Stewart 2001) firent ainsi écho aux travaux de Ronfeldt et Arquilla sur le concept de *Netwar*, et sur ses implications pour l'organisation de la riposte. Le Réseau international d'analyse des réseaux sociaux (International Network for Social Network Analysis) consacra également un numéro spécial de son journal officiel *Connections* aux réseaux terroristes, et aux stratégies permettant de les neutraliser (2001).

années le concept de *Netwar*, ou guerre des réseaux, et l'ont patiemment diffusé au sein des organisations militaires avant que les événements du 11 septembre ne contribuent à en faire un concept grand public. Un autre pôle plus informel de chercheurs universitaires et indépendants s'est constitué sur ce thème autour des activités du Réseau international d'analyse des réseaux sociaux (Stewart, 2001). Tous soulignent à l'unisson la profonde mutation de la nature des conflits, rendue possible par la révolution informatique. La diffusion des moyens de communication aurait rendu possible l'émergence de réseaux d'acteurs non étatiques plus « agiles » et flexibles que les hiérarchies gouvernementales qui les affrontent. Les cas utilisés pour appuyer cette thèse incluent le mouvement zapatiste au Chiapas (Ronfeldt et Arquilla, 2001), les manifestations antimondialisation de Seattle (de Armond, 2001), les activités des principales organisations criminelles transnationales (Klerks, 2001 ; Williams, 2001) ou encore celles des groupes terroristes islamistes (Zanini et Edwards, 2001).

Comme le concèdent bien volontiers Ronfeldt et Arquilla (2001 : 4), le cadre conceptuel qu'ils ont contribué à forger doit une grande part de son succès à l'impuissance des structures gouvernementales à contrer les adversaires terroristes et criminels insaisissables. Il offre en effet une motivation à saveur scientifique aux dirigeants des agences de sécurité militaires et civiles afin que ces derniers constituent leurs propres réseaux locaux et internationaux de coordination et d'échange d'information. Cette vision du monde horizontale, asymétrique et centrée sur des réseaux reconfigurables en fonction de besoins ponctuels a été abondamment relayée par les plus hautes instances du Pentagone[4]. Elle a, par ailleurs, constitué le socle conceptuel d'un ensemble de programmes technologiques destinés à détecter les manifestations latentes des réseaux clandestins menaçant les États-Unis. Simultanément, on a assisté à la création du *Department of Homeland Security* (DHS), une structure chargée de « mobiliser et de coordonner les ressources du gouvernement fédéral, des États et des collectivités locales, du secteur privé et de la population » (DHS, 2004), qui relève aussi de l'application d'une telle logique. En effet, le DHS forme avant tout le noyau d'un réseau d'organisations et d'institutions dans un pays où la prolifération des organes d'application de la loi est un acquis constitutionnel.

4. Sur l'usage, par Donald Rumsfeld, de la dialectique du réseau pour combattre les réseaux terroristes, voir Duffield (2002 : 156).

Si la reconfiguration inachevée des agences qui constituent le DHS est encore trop récente pour se prononcer définitivement sur la généralisation du mode d'organisation en réseau, les déclinaisons technologiques de la rhétorique du réseau se prêtent mieux à une telle analyse. Appliquant les recommandations décrites précédemment, l'Amiral Poindexter fut chargé par le Pentagone de mettre sur pied un système informatique axé sur l'exploitation massive des données personnelles (*datamining*). Il s'agit en fait ici d'outils perfectionnés d'analyse de réseaux, ou plus précisément, d'outils prétendant repérer des réseaux d'acteurs terroristes à partir de données massives en apparence anodines telles que les habitudes de consommation de certains produits et services (aviation, transport, santé, éducation, etc.). Cette approche est déjà utilisée depuis un certain nombre d'années dans la lutte contre la fraude bancaire ou fiscale, mais elle était jusqu'ici limitée à l'identification de suspects isolés. L'innovation introduite par le programme originel *Total Information Awareness*, et les héritiers plus « discrets » qui lui ont succédé après son élimination sous la pression des mouvements de défense des libertés individuelles, consiste à dépister les réseaux et les liens non apparents qui unissent leurs membres. Cette nouvelle approche requiert un accès à des quantités de données beaucoup plus importantes, des modèles prédictifs suffisamment robustes et des ressources informatiques capables d'accommoder les deux premières conditions. L'objectif n'est plus de trouver l'aiguille dans la botte de foin, mais de pouvoir « localiser et suivre en permanence un dangereux groupe d'aiguilles dissimulées dans une botte d'aiguilles absolument identiques » (Senator, 2002).

L'industrie privée du renseignement et la mise en réseau de l'information

L'optimisation de ces programmes se fait en étroite collaboration avec une constellation de fournisseurs privés qui disposent d'une très longue expérience dans ce domaine. L'un d'entre eux put ainsi affirmer : « Le 11 septembre nous a montré que les capacités de traitement de l'information du gouvernement américain se trouvent au même niveau que celles dont nous disposions en 1973 » (Morgan, cité dans O'Harrow, 2005 : 58). Par ailleurs, le recours à des sous-traitants privés permet au gouvernement d'échapper à l'inertie administrative cruellement mise en évidence par la Commission d'enquête du 11 septembre (9/11 Com-

mission, 2004). Cet engagement du secteur privé vaut tant pour la collecte des données primaires nécessaires à cet exercice que pour la conception des outils de traitement et de diffusion de l'information. Une industrie prospère des technologies du renseignement a ainsi vu le jour autour de la capitale fédérale grâce aux milliards de dollars alloués par le Congrès aux budgets de la sécurité nationale et intérieure (Murphy, 2001).

Quelques exemples suffiront à donner une idée de l'étendue des partenariats envisagés. Faisant face à une croissance exponentielle du nombre des déclarations de transactions suspectes faites par les établissements financiers, le *Department of Homeland Security* s'est tourné vers l'entreprise anglaise *World-Check*[5], qui met à la disposition de ses 800 clients une base de données couvrant 250 000 personnes et entreprises jugées « à risque » en raison de leurs actions directes ou en liens avec des groupes criminels organisés, terroristes ou des activités de blanchiment. Cette base de données est considérée comme plus complète que celles dont dispose actuellement le DHS, principalement en raison de critères d'inclusion moins rigoureux (Lichtblau, 2004). Le projet pilote MATRIX (Multi-State Anti-Terrorism Information Exchange), également réalisé pour le DHS par la société privée Seisint[6], vise pour sa part à faciliter l'accès des services de police à des données publiques éparses telles que les fichiers d'immatriculation des véhicules, d'enregistrement d'entreprises (et de faillites), de permis d'exercer délivrés par les différents ordres de gouvernement, des hypothèques enregistrées, etc., qui viennent ainsi s'agglomérer aux données criminelles (casier judiciaire) et personnelles (opérations bancaires, habitudes de consommation) plus traditionnelles. Le projet MATRIX donnait accès, à la mi-2004, à environ 3,9 milliards de dossiers informatisés distincts (Krouse, 2004 : 4).

Onze des seize États états-uniens qui avaient manifesté un intérêt pour ce programme se sont cependant rapidement retirés, notamment en raison de préoccupations quant à l'intégrité des données transmises. Cette préoccupation marginale pour le respect des législations locales

5. <www.world-check.com>.

6. Cette entreprise est une filiale du conglomérat Reed-Elsevier, spécialisée dans la publication de revues et de bases de données scientifiques. Quelques semaines après le 11 septembre, elle aurait dressé une liste de 120 000 personnes présentant un facteur de risque terroriste élevé (*HTF*, en anglais) à partir des données contenues dans des fichiers publics et d'une formule non précisée de « calcul » de ce quotient. D'après l'*American Civil Liberties Union*, un certain nombre d'arrestations auraient été menées sur la foi de cette liste (ACLU, 2004).

et nationales sur le respect de la vie privée semble être l'une des constantes de ces partenariats. La compagnie ChoicePoint[7], par exemple, agissant sous contrat pour le ministère de la Justice états-unien dut s'expliquer auprès de la Justice mexicaine et colombienne pour avoir illégalement vendu les fichiers électoraux et des données personnelles sur des millions de citoyens sud-américains (Burkeman et Tuckman, 2003). Ces données sont utilisées par les services de l'immigration, des douanes, la DEA et le FBI pour vérifier l'identité d'éventuels suspects.

Les liens commerciaux d'échanges d'information tissés entre le secteur public et le secteur privé seront amenés à se multiplier, bénéficiant d'un régime légal de plus en plus propice. Le *USA Patriot Act* de 2001 et l'*Intelligence Reform and Terrorism Prevention Act* de 2004 contiennent, en effet, des dispositions permettant la banalisation de l'accès aux données privées (respectivement art. 215 et 1016 des lois citées). Cette dissolution des barrières légales qui limitaient les flux de données résulte principalement du constat fait par les pouvoirs publics et les groupes de réflexion qui les conseillent de l'avance technologique prise par les entreprises d'agrégation des données, qui ont conçu des outils sophistiqués de profilage des consommateurs utilisés pour mieux cibler les campagnes de marketing direct (Markle Foundation Task Force, 2003). Venant ainsi éclipser la vision orwellienne d'un *Big Brother* étatique omnipotent, la surveillance contemporaine semble plutôt se dessiner sous les traits d'un essaim de « petits frères » entreprenants.

Les modes de mobilisation du secteur privé, loin de se limiter à des relations contractuelles, font également appel à la conscription des bases de données privées. Les législations antiterroristes mentionnées plus haut comprennent également des dispositions prescriptives qui étendent l'emprise des services de police et de renseignement sur des données qui leur étaient auparavant uniquement accessibles sur obtention d'un mandat de perquisition ou d'une autorisation d'interception. À titre d'exemple, les informations que détiennent les compagnies aériennes sur leurs passagers sont dorénavant accessibles aux autorités de protection du transport aérien (Singel, 2004). Au Canada, la *Loi sur les douanes* (L.R. (1985), ch. 1 (2e suppl.)), inclut dans son article 107.1 la possibilité pour les autorités frontalières d'exiger la transmission de ces données. Celles-ci sont recueillies par les compagnies afin d'offrir un service aussi personnalisé et confortable que possible aux voyageurs, mais per-

7. <www.choicepoint.com>.

mettent indirectement aux gouvernements de suivre leurs déplacements de manière beaucoup plus détaillée que par le passé. Elles livrent également une foule de détails d'ordre financiers, religieux et médicaux sur les passagers sans que les procédures judiciaires habituelles soient requises et que les contrôles afférents en matière de respect de la vie privée soient appliqués. On retrouve des exigences similaires de transmission et de déclaration dans le domaine bancaire, sous couvert de la lutte contre le blanchiment et le financement du terrorisme (Gagnon et Bacher, 2004).

L'internationalisation des réseaux de sécurité

Les exemples tirés des États-Unis se justifient par le caractère exemplaire des initiatives décrites : l'ampleur des ressources et des technologies mises au service de la rhétorique des réseaux de sécurité laisse entrevoir une adoption rapide de ce modèle à l'échelle de la planète. Contrairement aux vagues précédentes d'innovations policières estampillées « *made in USA* », qui connurent une diffusion désordonnée sans véritable effort de promotion de la part de leurs « concepteurs », l'approche en réseau exige l'établissement de liens aussi nombreux que possible. Engagées dans une guerre totale contre un terrorisme protéiforme international, les agences de renseignement et de sécurité états-uniennes n'ont d'autre option que de déployer leurs propres réseaux à l'échelle de la planète afin que l'information circule aussi librement que les individus de l'ère mondialisée. Cette doctrine s'impose ainsi aux assemblages de sécurité des pays alliés des États-Unis, qui font l'objet de pressions plus ou moins subtiles incitant au partage total de leurs données, incluant celles en possession des entreprises locales. La mise en réseau sécuritaire est ainsi parfois moins l'aboutissement d'une volonté commune que le résultat d'un jeu de pouvoir dont l'enjeu est le maintien des flux économiques et financiers (Lyon, 2004). Des logiques locales sont toutefois également à l'œuvre, démontrant le caractère symptomatique de cette dialectique du réseau dans le champ de la sécurité.

En Europe, de telles logiques avaient précédé les événements du 11 septembre de quelques années, s'étant plutôt imposées au fil de la construction de l'Union et de la disparition progressive des frontières nationales. Didier Bigo (1996) et James Sheptycki (2002) ont, par exemple, étudié l'émergence de réseaux de sécurité par le biais de la

constitution d'instances semi officielles de coopération policière, ou l'intensification et la systématisation des échanges d'information dans les zones transfrontalières, et particulièrement dans le secteur de la Manche. Marc Alain (2001) a également montré que ces réseaux constituent des enjeux de pouvoir importants au niveau national pour leurs membres, le privilège d'accès ou l'exclusion traduisant une situation de force ou de faiblesse dans les États disposant de services de police et de gendarmerie concurrents. Les deux grandes organisations internationales de coopération policière que sont INTERPOL et EUROPOL peuvent également être décrits comme des réseaux de sécurité, leur fonction principale consistant à faciliter les échanges d'informations entre organisations membres au moyen de systèmes informatiques décentralisés. À cet égard, le développement de ces systèmes par les organisations internationales et leur mise à disposition des services de police nationaux entreraient dans une stratégie de renforcement des capacités techniques de ces derniers, mais également de neutralisation des résistances au partage de l'information (Gerspatcher et Pujas, 2004).

Au Canada, le rapport « En quête de sécurité » de la Commission du droit emploie le terme de « réseaux de services de police publics et privés » pour désigner les nouvelles formes de partenariats entre secteur public et secteur privé (2002 : 17). Richard Ericson et Kevin Haggerty (1997) ont ainsi analysé avec un luxe de détails les liens formels et informels entre policiers et assureurs dans leur ouvrage sur la police dans la société du risque. Ils soulignent cependant que l'utilité de ces liens demeure largement abstraite, voire inexistante pour les acteurs de première ligne que sont les agents de la paix, et que des comportements de résistance en résultent. Un sondage administré en 2003 par Marcel-Eugène LeBeuf auprès des policiers municipaux, provinciaux et fédéraux de niveaux hiérarchiques variés révèle quant à lui une fréquence élevée d'échanges d'information entre organisations publiques de sécurité. Contrairement à ce que l'on pourrait penser, la majeure partie des échanges ne repose pas sur des technologies à fort potentiel d'accessibilité comme les bases de données, mais découle plutôt de contacts personnels directs. Cela explique qu'un facteur essentiel identifié par les répondants soit la connaissance du destinataire, autrement dit la confiance, ce qui n'empêche pas de nombreuses initiatives technologiques de mise en commun de l'information de voir le jour aux niveaux régional, provincial et national, à l'instar des projets OPTIC en Ontario ou PIMITS dans les provinces de l'Atlantique (LeBeuf et Paré, 2003).

On peut d'ailleurs émettre l'hypothèse que cette limite des réseaux technologiques a nourri la prolifération ces dernières années au Canada d'équipes intégrées d'application de la loi. Ces dernières regroupent physiquement de manière temporaire ou permanente les policiers de différents services travaillant sur une même menace criminelle ou terroriste. Principalement actives dans les domaines de la lutte contre le crime organisé (Escouade Carcajou puis équipes régionales mixtes), le terrorisme (Équipes intégrées de la sécurité nationale), le télémarketing frauduleux (projet COLT) ou la protection de la frontière Canada-USA (Équipes intégrées de la police des frontières), ces unités constituent de véritables nœuds de concentration et de dissémination de l'information, et des techniques d'enquête, pour les organisations qui en sont membres (GRC, 2003). On observe d'ailleurs une tendance similaire aux États-Unis, où le nombre des équipes intégrées de lutte contre le terrorisme (*Joint Terrorism Task Forces*) est passé de 35 en 2001 à 84 en 2003 (Markle Foundation Task Force, 2003 : 87).

Le discours d'un noyau de réformateurs influents appelant à un changement de paradigme organisationnel, et la débauche d'actions qui en résultent sont guidés par la volonté de combattre à « armes égales » les réseaux criminels et terroristes. Cette approche essentiellement focalisée sur la grande criminalité et les menaces contre la sécurité nationale doit cependant être replacée dans un contexte synchronique et diachronique beaucoup plus large.

2. La mise en réseau de la sécurité : un processus qui transcende le 11 septembre

Comme le suggèrent les exemples européens et canadiens cités précédemment, les stratégies de mise en réseau dépendent en grande partie de facteurs politiques locaux, de besoins nés de l'ouverture des frontières ou encore de la mobilité accrue des délinquants. Les événements du 11 septembre auront considérablement accéléré ce processus en incitant la seule puissance militaire et policière mondiale à déployer des stratégies visant à surmonter la fragmentation administrative et l'isolement qui la caractérisait. Avant de se pencher sur les implications théoriques et normatives de cette évolution, un changement d'angle est nécessaire afin de bien saisir l'ampleur de cette tendance qui dépasse largement la conflagration terroriste de 2001.

Tout d'abord, il faut souligner que l'histoire des réseaux policiers précède l'avènement de l'informatique et des moyens de transport modernes. Quelques cas particulièrement éloquents nous permettrons d'analyser les précédents initiés en ce domaine par quelques visionnaires. Ensuite, la morphologie du réseau, loin d'être réservée aux agences d'application de la loi, semble avoir été adoptée, dans le discours ou en pratique, par de nombreux autres secteurs de la fonction publique. Il est donc utile de replacer l'évolution que connaissent les services de police et de renseignement dans le contexte beaucoup plus large de la réforme du secteur public et des modalités d'intervention de l'État, au détriment d'approches d'inspiration « conspirationniste ». Pour terminer, on rappellera qu'en même temps qu'elle se trouve enrôlée dans la lutte contre le terrorisme et le crime organisé, la dialectique du réseau fait également l'objet d'un intérêt marqué de la part de criminologues explorant son potentiel pour la prévention de la criminalité. Leur ambition est de montrer que les réseaux de sécurité peuvent aussi bien être déployés par le haut qu'émerger par le bas.

Généalogie incomplète des réseaux de sécurité

Si le rythme de formation des réseaux semble connaître une accélération marquée depuis quelques années, cette structure organisationnelle ne représente pas en tant que telle une découverte pour le monde de la sécurité. Intuitivement, de nombreux services de « haute police » avaient dès le début du XIX^{e} siècle établi des mécanismes d'échange d'information. Comme nous le verrons dans le cas de la société Pinkerton, la sécurité privée ne fut pas en reste.

La légende de Joseph Fouché et de ses réseaux d'informateurs, issus de toutes les strates de la société et enveloppant la France et l'Europe dans une surveillance totale se prêterait à merveille à notre démonstration, si les aveux mêmes du ministre de la Police générale et des historiens qui ont disséqué son parcours n'étaient venus tempérer ce mythe de toute-puissance (Madelin, 1903 ; Tulard, 1998 ; Brodeur, 2003). C'est donc à travers l'exemple de l'Union policière allemande, fondée en 1851 à l'initiative du président de la police de Berlin, Karl Ludwig Friedrich von Hinckeldey, que débutera notre exploration de l'usage de formes primitives de réseaux internationaux par les organisations policières. Devant la menace révolutionnaire qui menaçait d'embraser toute

l'Europe, les polices souveraines de la Confédération germanique[8] mirent en commun leurs ressources de « haute police » (Brodeur, 2003) et établirent un système d'échange de renseignements par le biais de rencontres annuelles portant sur les activités des principaux opposants politiques allemands, français, italiens, polonais ou hongrois (Deflem, 1996). Des agents représentant l'Union policière furent également postés à Londres, New York, Paris et Bruxelles, sans toutefois que des liens privilégiés de collaboration puissent être établis avec les autorités locales, réticentes à l'égard de cette ingérence dans la vie politique.

Parallèlement, à partir de 1852, la police autrichienne publia et distribua aux autres membres de l'union un bulletin d'information bimensuel sur les personnes recherchées et leurs modes opérationnels : le *Central-Polizei-Blatt*. Très rapidement, ce bulletin fut expédié à l'ensemble des polices européennes (à l'exception de la Russie et de l'Italie), qui ne manquèrent pas en retour de faire parvenir leurs propres bulletins à Vienne (Liang, 1992 : 32). Il faut noter qu'au-delà des frontières germaniques, ces pratiques semblaient moins motivées par une stratégie de partage du renseignement que par un échange peu coûteux de bons procédés. Ainsi, on peut se poser la question de l'utilité pour la police viennoise de disposer de bulletins français contenant exclusivement des informations sur des criminels de droit commun peu susceptibles de menacer le régime austro-hongrois. À l'instar des mécanismes de coopération policière qui lui succédèrent, l'Union policière s'est constituée à l'initiative de bureaucrates policiers qui jugeaient trop contraignant le recours à la machinerie lourde des traités internationaux (Deflem, 2002).

D'autres initiatives visant à améliorer l'intégration des services de police européens virent le jour au début du XX^{e} siècle, d'abord en réponse aux assassinats perpétrés par les groupes anarchistes[9], puis dans le cadre de phénomènes criminels tels que la « traite de Blanches[10] »,

---

8. Les services membres de l'Union policière représentaient les royaumes d'Autriche, de Prusse, de Saxe, d'Hanovre, de Bavière, de Wurtemberg et de Bade.

9. Conférence de Rome, en décembre 1898, à la suite de l'assassinat en septembre à Genève de l'impératrice d'Autriche, Elisabeth (« Sissi »), ou Protocole secret de guerre internationale contre l'anarchisme signé en 1904 par l'Allemagne, l'Autriche-Hongrie, la Russie, la Suède, la Bulgarie, le Danemark, l'Espagne, le Portugal, la Roumanie et la Turquie (Liang, 1992 : 173).

10. Conférences de 1904 et 1910 en France, de Buenos Aires en 1905, de Madrid en 1909, de Sao Paolo en 1912, de Washington en 1913, de Monaco en 1914, de Buenos Aires en 1920 et de New York en 1922 et 1923 (Deflem, 1996 et 2002).

pour finalement aboutir à la création de la Commission internationale de police criminelle à Vienne en 1923, ancêtre d'Interpol.

Si les initiatives décrites plus haut furent stimulées par le besoin croissant des services de police d'opérer au-delà de leurs frontières nationales, d'autres réseaux de sécurité furent assemblés afin de remédier à la fragmentation institutionnelle interne de certains systèmes policiers. Aux États-Unis, l'agence de détectives privés Pinkerton prospéra ainsi en occupant les interstices laissés vacants par des organisations policières locales impuissantes devant la mobilité des délinquants profitant des moyens de communication et de transport modernes. Bien avant la création du *Federal Bureau of Investigation*, elle facilita la circulation et l'exploitation du renseignement policier à travers tout le pays, et parfois au-delà des frontières. Au début du XX^{e} siècle, Pinkerton disposait ainsi de 20 succursales dans les principales villes états-uniennes, chacune possédant un exemplaire du fichier criminel actualisé en permanence par les bureaux de New York et de Chicago. Ces informations étaient également mises à la disposition des services de police locaux qui en faisaient la demande, en échange d'un accès à leurs propres fichiers locaux (Morn, 1982 : 152). Les frères Pinkerton jouèrent un rôle central dans la professionnalisation du travail policier, par leur rôle actif dans la création de l'Association internationale des chefs de police (IACP), leurs inlassables démarches en faveur de la création d'un fichier national d'empreintes digitales et la formation d'employés qui prirent les rênes de services de police municipaux (Morn, 1982 : 166). Le bureau de New York entretenait des contacts réguliers avec les services de police de Londres, Paris, Berlin, et de nombreux pays sud-américains, et n'hésitait pas à envoyer des agents dans le monde entier à la poursuite de criminels célèbres, activité qui générait une importante publicité gratuite dans la presse. Ce réseau de services de police locaux, unis par une entreprise privée et ses interfaces internationales, conférait *de facto* à Pinkerton le statut de police nationale aux yeux de nombreux gouvernements étrangers (Marquis, 1993 : 62 ; Nadelmann, 1997 : 57)[11]. Plusieurs années avant la création d'agences fédérales d'application de la loi, le secteur de la sécurité privée, dégagé des contraintes politiques et légales qui s'imposaient aux organisations policières, occupa ainsi un rôle d'intermédiaire ou de « courtier » entre celles-ci.

11. C'est en 1908 que l'*Attorney General*, Charles Joseph Bonaparte, créa au sein du ministère de la Justice une unité embryonnaire permanente constituée d'enquêteurs, le *Bureau of Investigation*.

Ce rôle de nœud central s'estompa dès le début du XX[e] siècle avec la création et le renforcement d'instances fédérales, qui, à leur tour, éprouvèrent rapidement le besoin de travailler en réseau. On mentionnera seulement le « réseau de neutralité », chargé d'empêcher dès 1909 les incursions de rebelles le long de la frontière avec le Mexique (Nadelmann, 1997 : 78). Celui-ci était composé d'agents représentant les douanes, l'immigration, les marshals, l'inspection postale, le département d'État, le renseignement Militaire, le Bureau d'enquêtes (qui deviendra le FBI), le service secret, les services de police texans et les agences gouvernementales mexicaines. Malgré les nombreuses frictions et les conflits ouverts qui émaillèrent le fonctionnement de ce premier réseau, son succès semble avoir justifié son maintien en fonctionnement jusqu'à la Première Guerre mondiale et son utilisation dans la lutte contre les activités des services de renseignement allemands au Mexique.

Ces quelques exemples, choisis parmi tant d'autres, concernent essentiellement des réseaux interpersonnels en étoile, dans lesquels des individus visionnaires bâtissent un réseau social où l'intérêt personnel et collectif se chevauchent constamment. La structure centralisée de ces réseaux les rend incapables de survivre à la disparition de leur fondateur. C'est avec le progrès technologique des moyens de communication que la banalisation des échanges a pu étendre le champ d'action des réseaux et accroître leur capacité de connexion. Mais loin d'être un phénomène restreint aux institutions de contrôle social, les pratiques de mise en réseau touchent l'ensemble des services publics.

Les ramifications de l'État horizontal

La crise de l'État providence et les efforts faits pour lui trouver un cadre théorique et normatif de remplacement se sont soldés par un transfert de responsabilités du secteur public vers le secteur privé dans les domaines de l'éducation, de la santé, des transports, etc. Déléguant les fonctions de mise en œuvre (le *rowing*) à des opérateurs privés plus efficients, l'État aurait recentré ses activités sur les fonctions de coordination (le *steering*) (Osborne et Gaebler, 1992).

Ces nouvelles modalités de gouvernance requièrent la participation de nombreux acteurs dans la conception et l'application des politiques publiques, et l'existence de jeux de pouvoirs et de dépendances complexes entre ces acteurs. Ce constat a ouvert la voie à l'étude des réseaux

comme nouvelle forme de l'action gouvernementale (Le Galès, 1995 ; Rhodes, 1997 ; Pierre et Peters, 2000), rejoignant sur ce terrain la longue lignée des travaux menés dans la sphère des échanges économiques (Powell, 1990 ; Tshuma, 2000). Sur le plan normatif, le fonctionnement en réseau et le jargon qui l'accompagne semblent coloniser toutes les sphères de la fonction publique, offrant une alternative aux pesanteurs et aux clivages des bureaucraties verticales, tout en atténuant les excès du recours au marché.

Sur le plan théorique, Rod Rhodes et ses collaborateurs ont montré que le concept de réseau d'action publique (*policy network*) devait beaucoup aux travaux de la science politique états-unienne, qui approfondit dès le début des années 1950 les relations triangulaires symbiotiques entre agences gouvernementales, comités parlementaires et groupes d'intérêts sectoriels. Leurs propres travaux sur les réseaux d'action publique anglais se nourrirent parallèlement des recherches européennes sur les relations interorganisationnelles (Rhodes, 1997). L'apport majeur de ce groupe de chercheurs, à partir de monographies détaillées menées dans divers secteurs de l'action publique, fut de proposer une typologie de facteurs tels que les divers niveaux d'interdépendance entre acteurs, leur degré d'intégration et les disparités quant aux ressources à leur disposition. Ils mirent ainsi en évidence l'existence de réseaux au cœur desquels la relation de dépendance pouvait aussi bien favoriser les acteurs privés que publics, résultat d'une volonté ou d'une capacité variable de l'État d'exercer son emprise (Marsh et Rhodes, 1992). Loin d'être circonscrit au monde anglo-saxon, ce concept paraît disposer d'un potentiel explicatif tout aussi fort dans des contextes où l'action publique a traditionnellement opéré selon un mode centralisé (Le Galès, 1995).

La mise en lumière de la pertinence empirique du concept de réseau pour analyser certaines formes de l'action publique doit cependant éviter l'écueil d'une vision trop séquentielle. Hiérarchies, marché et réseaux se sont effectivement succédé comme modes dominants de prestation des services publics. Toutefois, ils coexistent aujourd'hui en dépit de leurs irréductibles contradictions, ce qui contribue à l'éclosion de nombreux dilemmes organisationnels concernant le dosage optimal de ces trois morphologies. Nous reviendrons sur cet aspect ultérieurement.

Ce détour par la science policière et administrative ne prétend aucunement à l'exhaustivité. Tout au plus souhaite-t-il rappeler l'enchâssement des organisations policières et de renseignement dans des structures

gouvernementales beaucoup plus vastes, dont les modes de gestion transcendent les particularismes fonctionnels. S'il demeure pertinent de se pencher sur les évolutions de chaque administration et de sa constellation de partenaires en adoptant une grille de lecture disciplinaire (la police étant, par exemple, principalement étudiée par des criminologues et des sociologues équipés d'outils conceptuels précis), des comparaisons intersectorielles nous semblent également porteuses d'un fort potentiel de relativisation des changements radicaux décrits dans certaines recherches, ou des interprétations trop étroites auxquelles ces observations peuvent donner lieu. Il en va ainsi de l'établissement d'un lien causal entre la constitution des réseaux policiers et une volonté diffuse de resserrer les mailles du filet pénal ou de faciliter l'exclusion des pauvres et des étrangers (Bigo, 1996 ; Wacquant, 1999). Ce raisonnement, aussi noble que soient ses intentions, néglige de prendre en compte la nouvelle orthodoxie bureaucratique de la mise en réseau, qui s'étend aussi bien au domaine de la sécurité qu'à ceux de la santé, de l'éducation, de l'énergie ou du transport. Si on doit se questionner sur les menaces que font peser de telles pratiques sur les valeurs démocratiques, il paraît exagéré de voir là la stratégie délibérée d'une rationalité punitive dominante. À cet égard, un certain nombre de chercheurs anglo-saxons explorent depuis quelques années le potentiel des structures en réseau pour la prévention de la criminalité et une gouvernance optimale de la sécurité.

La gouvernance nodale de la sécurité et la prévention du crime

Depuis le début des années 1970, le rejet d'un mode de contrôle social institutionnel uniquement axé sur l'action répressive de la police a ouvert la voie à des approches de prévention sociale et situationnelle mettant à contribution une myriade d'acteurs publics, hybrides et privés (Cusson, 2002). Impuissante à endiguer les phénomènes de criminalité acquisitive ou d'incivilités, la police elle-même s'est convertie à cette nouvelle philosophie en tentant le passage d'un modèle professionnel réactif à un modèle communautaire proactif. Ces initiatives traduisent la prise de conscience qu'une organisation, aussi étendus soient ses pouvoirs légaux et son mandat, ne peut répondre seule à des problèmes sociaux d'une telle complexité. Les alliances qu'elle tisse avec d'autres acteurs disposant

de ressources financières, humaines ou symboliques, afin de mutualiser celles-ci dans une démarche de résolution des problèmes conduisent alors à un mode de gouvernance multilatérale du crime et de la sécurité.

Les programmes de prévention lancés en France (Donzelot *et al.*, 2003), en Angleterre (Crawford, 1997), au Canada (Brodeur, 1999) ou en Australie (O'Malley et Sutton, 1997) ces trente dernières années insistent tous sur cette nécessité du partenariat, dont les bénéfices attendus semblent illimités. Quelques évaluations invitent cependant à la prudence quant à l'utilisation d'une telle approche. Les jeux de pouvoir inter-institutionnels et l'affrontement des rationalités concurrentes (Espeland, 1998) mis en évidence par ces études montrent bien à quel point les structures en réseau peuvent aussi bien être mobilisées pour la coopération que pour la domination, pour l'inclusion que pour l'exclusion. Comme nous l'avons déjà mentionné, la coexistence des hiérarchies et des réseaux se prête à des dilemmes et des conflits organisationnels dont l'arbitrage s'avère difficile, particulièrement lorsqu'il met aux prises des acteurs aux ressources variables. Les exemples abondent, dans des contextes nationaux divers, de comportements d'instrumentalisation de ces partenariats par les institutions policières au détriment d'acteurs politiques et sociaux locaux (Ferret, 2004 ; Cherney, 2004). De plus, Crawford montre comment les stratégies d'évitement ou de neutralisation des conflits, rendues centrales du fait de la fréquence des prises de décisions communes, peuvent mener à une dilution des objectifs et une éviscération des moyens déployés pour les atteindre (Crawford, 1997 : 133-144).

Afin d'apporter une réponse à ce constat d'échec relatif, Clifford Shearing et ses collègues se proposent de concevoir la production de sécurité comme le résultat d'un processus de gouvernance nodale. Cette forme de gouvernance consiste en un processus d'adaptation sociale qui met en présence des nœuds institutionnels, privés et communautaires dotés de mentalités, technologies, ressources et structures propres (Johnston et Shearing, 2003). Les communautés les plus défavorisées, disproportionnellement affectées par les effets de la criminalité, sont considérées comme des nœuds à part entière, disposant de capacités locales susceptibles d'être mobilisées par l'entremise de structures autogérées de résolution des problèmes. Par leur intégration dans des réseaux d'acteurs publics et privés qui mettent à leur disposition les ressources qui leur font défaut, ces structures (ou nœuds) participent alors à une gouvernance par le bas qui répond à leurs besoins et réduit

le déficit démocratique des stratégies traditionnelles de prévention. Des résultats encourageants ont été obtenus par des projets pilotes implantés dans des communautés affaiblies en Afrique du Sud et en Argentine (Shearing et Wood, 2003). On retrouve une philosophie similaire d'autonomisation (*empowerment*) par l'intégration dans les réseaux locaux de revitalisation des quartiers animés par les *Community Development Corporations* états-uniens (Donzelot *et al.*, 2003). La gouvernance nodale est-elle un concept réservé à des États trop faibles pour maintenir leur monopole sur les fonctions régaliennes de sécurité et de justice, ou peut-elle aussi constituer un outil approprié d'analyse des transformations de la gouvernance de la sécurité dans les sociétés modernes avancées ? Cette question ne pourra trouver sa réponse que dans l'étude empirique des pratiques actuelles de mise en réseau et de partenariat dans le champ de la sécurité. Le déficit actuel de ce type de recherches[12] nous amène, dans une troisième partie, à soulever un certain nombre de questions qui nous paraissent centrales dans une telle perspective.

3. Questions de recherche

Malgré les exemples à notre disposition et la reconnaissance tacite par de nombreux chercheurs de l'existence d'une densité relationnelle forte dans le champ de la sécurité, on peut être surpris de la faible pénétration des méthodes d'analyse de réseaux dans le domaine des études policières. Cette réticence ne concerne pas la criminologie dans son ensemble, puisque l'étude de certaines formes de criminalités complexes fait un usage intensif de ces outils (voir, par exemple, Lemieux, 2003 ; Morselli, 2003 ; Tarrius, 2003). On doit plutôt y voir, en ce qui concerne les recherches sur la police et la sécurité privée, la domination de la pensée juridique et de la conception wébérienne de l'État, qui peinent parfois à ajuster l'idée de monopole à une réalité beaucoup moins contrastée et élégante sur le plan théorique (Ocqueteau, 2004). Quoiqu'il en soit, l'urgence de substituer un savoir scientifique aux anecdotes journalistiques qui transpirent sur les réseaux de haute police, la confirmation de l'intérêt de cette approche par les recherches antérieures en sociologie et en science politique, couplées au besoin normatif d'explorer les

12. Notons cependant les exceptions que représentent les travaux de Gatto et Thoenig (1993), Crawford (1997), Newburn (2001), Crawford et Lister (2004).

ressources que peuvent offrir cette morphologie organisationnelle pour une gouvernance plus démocratique de la sécurité, nous amènent à suggérer trois pistes prioritaires de réflexion. La contribution de recherches centrées sur les réseaux de sécurité plutôt que sur des approches mono-institutionnelles ne peut, en effet, se limiter à une simple description de la pluralité des acteurs ou de la complexité de leurs relations. La coordination de ces réseaux et leurs mécanismes de régulation paraissent alors offrir des angles d'attaque plus prometteurs.

L'applicabilité des méthodes d'analyse de réseaux dans le champ de la sécurité ou comment dépasser le stade de la métaphore ?

Sans rentrer dans les détails, rappelons que les outils mis à notre disposition par l'analyse de réseaux visent à décrire et à modéliser par induction la structure relationnelle des réseaux, en faisant appel le plus souvent aux mathématiques et à la théorie des graphes (Degenne et Forsé 1994 ; Lazega, 1994 ; Wasserman et Faust, 1994). Il est souvent reproché à l'analyse de réseaux son caractère « a-théorique », et sa propension à la description « statique » de réseaux d'amplitude limitée ou modérée, alors que la réalité sociale laisse entrevoir une évolution constante de ces structures et l'existence de chevauchements et de croisements entre les dimensions individuelles et organisationnelles des réseaux. S'il est légitime d'émettre de tels doutes sur les apports de cette méthodologie, ceux-ci ne peuvent suffire à rejeter sans autre forme de débat les tentatives de remédier aux faiblesses relevées. À décharge, il est utile de préciser que les limites actuelles des méthodes d'analyse de réseaux relèvent en partie de l'objectif ambitieux qu'elles se sont fixé de cartographier des phénomènes sociaux fluides et ambigus. La richesse des données requises, les efforts à déployer pour les recueillir et la faiblesse des ressources disponibles permettent difficilement de procéder à des études de grande ampleur ou longitudinales. Cela explique d'ailleurs en partie pourquoi un grand nombre des recherches les plus novatrices en ce domaine relève de la sociologie des organisations et de l'économie, disciplines bénéficiant du soutien financier de grandes entreprises ou de puissants mécènes privés directement intéressés à leurs résultats.

Cette démarche méthodologique et théorique semble pourtant particulièrement pertinente dans le contexte actuel post-11 septembre, où les frontières internes et externes du système d'action que représente la

sécurité intérieure ont été pulvérisées. La souplesse des méthodes associée à l'analyse de réseaux recèle un potentiel stimulant de suivi des changements en cours (Lazega, 1994). S'appuyant sur les connaissances amassées au cours des quarante dernières années par les sociologues de la police et de la sécurité sur la structure et la culture des organisations de sécurité, et prolongeant une typologie provisoire distinguant les réseaux technologiques, locaux, institutionnels et internationaux (Dupont, 2004), ces outils devraient permettre d'étudier les réseaux de sécurité comme de nouveaux acteurs collectifs dont l'émergence, la dynamique, les dysfonctionnements, et la disparition dérivent de variables dépendantes encore peu formalisées.

Il faudra d'abord procéder au recensement empirique des acteurs (en accordant une attention particulière aux organisations hybrides), déterminer la nature et mesurer la fréquence des interactions entre ces derniers et, par induction, déterminer les positions et les rôles que chaque nœud joue dans l'économie générale du réseau. Cet exercice de cartographie des structures et de leurs relations devrait idéalement pouvoir être répété dans des contextes géographiques, temporels et fonctionnels variés, afin de comparer les observations. Cette première étape menée à bien, on disposera alors d'un point de référence pour analyser les transformations qui affectent les réseaux et les facteurs qui influent sur celles-ci. On pense, par exemple, à des études possibles sur les conditions d'émergence ou de mutation de certains réseaux, au fonctionnement des réseaux de sécurité en temps de crise, à l'influence des trajectoires professionnelles individuelles sur la structure des réseaux, ou encore aux dispositifs adaptatifs actionnés en réponse à l'apparition de contraintes légales, budgétaires ou technologiques. Les conflits entre réseaux concurrents et les choix faits par les acteurs de se joindre à eux, de les déstabiliser ou de quitter certains réseaux pourraient également s'avérer être des sujets féconds.

Le recours aux méthodes d'analyse de réseaux suppose un accès privilégié aux organisations et à leurs membres, et s'expose inévitablement à une résistance de ces derniers à être connus (Loubet del Bayle, 1992 ; Brodeur et Monjardet, 2003). Cette résistance n'est cependant pas uniforme, et la multiplicité des points d'accès à un réseau permet de contourner les refus opposés par certains acteurs. Les cultures organisationnelles, ainsi que les contraintes légales, contractuelles et commerciales connaissent de fortes variations à l'intérieur d'un même réseau, créant pour les chercheurs des occasions de collecte des données. De

plus, la diversification des méthodes privilégiées, qu'il s'agisse du recours à des questionnaires, d'observations, de l'analyse de documents d'archives ou de presse, ou d'expérimentations en milieux contrôlés ou ouverts (Wasserman et Faust, 1994), permet de moduler la « visibilité » des activités de recherche, et, par conséquent, la résistance qu'elles sont susceptibles d'engendrer. Celle-ci est d'autant plus forte que les organisations ou les individus étudiés perçoivent les recherches dont ils font l'objet comme des évaluations masquées de leur efficacité.

Le mythe de l'efficacité des réseaux

L'efficacité des réseaux est souvent attribuée à leur capacité d'apporter une valeur ajoutée substantielle à leurs membres, du seul fait de l'existence d'interconnexions entre ceux-ci (Duffield, 2002 : 158). Ces interconnexions peuvent se traduire concrètement par un accès à des ressources humaines, informationnelles, techniques, ou à une mutualisation des coûts et des risques. Une équation mathématique relativement simple, formulée par Robert Metcalfe, l'inventeur du protocole de mise en réseau informatique *Ethernet*, est souvent citée pour illustrer la supériorité des réseaux sur d'autres formes d'organisation sociale, notamment le marché. La « loi de Metcalfe » stipule ainsi que l'utilité d'un réseau est proportionnelle au carré du nombre de ses utilisateurs ou points de connexion, soit N^2-N (puisqu'un nœud ne peut se connecter à lui-même). Cette utilité exponentielle contraste ainsi avec les modèles traditionnels de l'offre et de la demande qui assignent une valeur supérieure à la rareté. Les réseaux qui intéressaient Metcalfe étaient cependant uniquement constitués de machines (télécopieurs ou ordinateurs), et d'étendre l'application de sa « loi » à d'autres formes de réseaux, notamment organisationnels, semble pour le moins abusif. Les êtres humains et les organisations sont, en effet, loin de disposer des mêmes aptitudes infinies à communiquer simultanément entre eux.

L'efficacité des réseaux sociaux ou organisationnels dépend de facteurs beaucoup plus complexes que le simple nombre de leurs membres. Du point de vue des nœuds qui forment un réseau, ce sont leurs positions à l'intérieur de celui-ci et la densité de relations non redondantes avec les autres membres ou des acteurs extérieurs qui vont procurer ou non un avantage compétitif et influencer leurs stratégies (Coleman, 1988 ; Granovetter, 1983). À l'échelle du réseau, les structures mani-

festes (formelles) et latentes (informelles) qui modèlent celui-ci vont faciliter ou, au contraire, rendre plus difficile la collaboration entre membres (Rowley, 1997). Qui plus est, certaines particularités organisationnelles propres au champ de la sécurité, telles que le culte du secret (Brodeur, 2003) et la compartimentation qui en résultent, vont rendre plus difficile la circulation de l'information et réduire les occasions de manifestation des interprétations alternatives. La mise en réseau va ici contribuer à la propagation et au renforcement de mythes désuets, au détriment d'idées critiques rejetées sans examen de leur valeur intrinsèque, la fameuse « pensée de groupe ». Comme on le voit, la simple mise en réseau ne suffit pas à conférer une efficacité supérieure sur les hiérarchies ou le marché, et contient en germe de nombreux facteurs de dysfonctionnement. L'étude approfondie des conditions d'émergence, de renforcement ou d'atténuation de ces facteurs devrait faire avancer les connaissances sur le fonctionnement des mécanismes de coordination, par destination ou incidence, des réseaux de sécurité.

Le rôle de la confiance dans le bon fonctionnement des réseaux semble ici déterminant. L'un des avantages que possèdent les réseaux criminels sur leurs « adversaires » policiers réside dans la confiance absolue qui unit chacun de leurs membres. Qu'elle découle d'une origine ethnique partagée, d'une adhésion à des croyances religieuses ou des causes politiques extrémistes, ou encore de la participation à des rites de passage violents, cette confiance permet de réduire les coûts de transaction à l'intérieur du réseau. Les contextes de réseaux interorganisationnels formels qui nous occupent ici se prêtent beaucoup moins bien à la création et à la « diffusion » de la confiance. Celle-ci ne se gagne pas par décret, et dépend plutôt de facteurs contingents tels que la taille des réseaux, leur degré d'homogénéité, les rapports de force qui les traversent, leur histoire ou encore le niveau de consensus quant aux objectifs qu'ils se sont fixés. De surcroît, il faut distinguer plusieurs formes de confiance, selon le degré de fragilité ou de résilience (Smith Ring, 1997), ou selon la nature personnelle ou institutionnelle de ses manifestations.

Le phénomène de « *blue drain* » (Shearing et Stenning, 1982), qui voit des policiers retraités de haut rang entamer une seconde carrière dans la sécurité privée peut, à cet égard, être interprété comme une stratégie délibérée de leur nouvel employeur d'augmenter leur capital social et de faciliter les relations avec les institutions policières (Erickson, 2001). De même, dans le cadre d'un sondage sur l'échange de l'information

entre services de police canadiens, Marcel-Eugène LeBeuf et Simon Paré (2003) ont souligné le rôle primordial que joue la confiance personnelle et la propension des policiers interrogés à restreindre la transmission d'informations aux individus qu'ils connaissent. Dans la même veine, on peut ici émettre l'hypothèse que l'échec des services de sécurité états-uniens à contrecarrer les attentats du 11 septembre ne dérive pas seulement de l'absence de mécanismes formels de collaboration[13], mais aussi d'un déficit de la confiance intra et interorganisationnelle qui empêcha le traitement des fragments d'information disponibles (9/11 Commission, 2004). Si l'étude de l'efficacité des réseaux de sécurité va de pair avec celle de la confiance qui alimente leurs échanges, elle est également intimement liée à la question de l'érosion des formes traditionnelles d'imputabilité qu'elle suppose.

Réseaux de sécurité et imputabilité

Comme l'a souligné Lucia Zedner (2003), l'aspiration à la sécurité et les moyens employés pour concrétiser celle-ci sont indissociables de six paradoxes, qui sapent les principales valeurs démocratiques que sont la liberté, l'équité, ou encore la justice. Les mécanismes d'imputabilité peuvent alors être considérés comme des moyens de régulation de ces paradoxes et de leurs manifestations. Chaque morphologie réclame cependant un régime de contrôle adapté qui tienne compte de ses propriétés structurelles. Le fait que ces trois morphologies s'imbriquent en un processus de métissage permanent ne facilite bien entendu pas les choses. Les réseaux de sécurité, du fait de leurs capacités de distribution des ressources et des tâches entre nœuds appartenant à des sphères organisationnelles variées, peuvent, par exemple, se soustraire avec plus ou moins d'aisance aux mécanismes hiérarchiques de contrôle. Le mandat de ces derniers se limite en règle générale à un acteur ou une classe d'acteurs (services de police, agences de sécurité privée, organisations hybrides, etc.). Cette fragmentation du contrôle ne convient plus lorsque les acteurs utilisent la mise en réseau pour s'émanciper des contraintes d'imputabilité en sous-traitant ou en déléguant à leurs partenaires certaines activités interdites. Le recours à la torture par le gouvernement

13. La CIA avait ainsi créé, dès 1986, le *Counter Terrorism Center*, une unité de liaison et de « fusion » du renseignement composée d'agents représentant les principaux services de police et de renseignement (Hersh, 2004).

états-unien dans sa lutte contre le terrorisme, et la division minutieuse du travail en ce domaine constitue un exemple extrême des dérives auxquelles peuvent prêter les réseaux de sécurité.

Astreintes au respect des règles de procédure judiciaire élémentaires par les tribunaux états-uniens, les agences responsables de la lutte contre le terrorisme ont établi un réseau international et clandestin de torture qui délègue les pratiques les plus extrêmes à des services amis du Moyen-Orient, tout en fournissant les individus à interroger, les questions à leur poser et les moyens logistiques de transport d'un pays à un autre (Hersh, 2004). Ce réseau, constitué d'une quarantaine de centres de détention « clandestins » mis en place par le gouvernement des États-Unis à Guantanamo, en Afghanistan, en Irak et ailleurs, auxquels viennent s'insérer les services de sécurité d'une dizaine de pays aux traditions démocratiques discutables tels que la Syrie, le Pakistan, la Jordanie, l'Arabie Saoudite ou l'Ouzbékistan, représente un effort délibéré de diluer l'efficacité des mécanismes de contrôle (Human Rights Watch, 2004). L'attitude ambivalente du FBI qui profite des renseignements ainsi extraits tout en ayant donné l'ordre à ses agents de ne pas assister aux interrogatoires les plus « musclés » afin de ne pas vicier d'éventuelles procédures criminelles, illustre bien les problèmes que posent l'exploitation de contraintes légales variables par les réseaux de sécurité. Les mises en réseaux de bases de données publiques et privées décrites plus haut répondent à la même volonté de contourner les règles traditionnelles d'imputabilité en transférant certaines responsabilités ou données à des acteurs non imputables, même si les conséquences de cette manœuvre sont moins choquantes.

Comme on le voit, les liens lâches entre nœuds du réseau permettent de brouiller aux yeux des acteurs extérieurs la véritable nature des transactions opérées à l'intérieur. De véritables espaces d'incertitude, dénués de toute forme de régulation externe et soustraits aux mécanismes internes d'imputabilité peuvent alors être aménagés par les membres d'un réseau afin d'optimiser leur liberté d'action. Dans la mesure où la complexité des réseaux de sécurité décrits ici s'oppose à une intégration hiérarchique des mécanismes d'imputabilité, le recours à des mécanismes de métarégulation, c'est-à-dire de régulation de la régulation, semble être une option plus réaliste. Cette approche commence juste à faire l'objet de recherches dans d'autres domaines de la gouvernance (Grabosky, 1995 ; Parker, 2002 ; Braithwaite, 2003). Elle ouvre cependant des

perspectives intéressantes de conceptualisation de l'imputabilité dans le contexte des réseaux de sécurité, qui ne pourront être tenus à la reddition de comptes que par des réseaux d'imputabilité.

Conclusion

Les critiques des arguments avancés dans cet article pourront faire valoir que le travail en réseau a toujours constitué un ressort essentiel du travail policier et de renseignement, comme en attestent d'ailleurs les exemples historiques mentionnés précédemment. Cependant, nous avons espéré démontrer dans la première partie à quel point les événements du 11 septembre 2001 et les technologies de l'information jusque-là disponibles, mais sous-exploitées par les services de police, avaient provoqué une accélération de la mise en réseau des prestataires de sécurité. Ces réseaux restent organisés autour de l'État, dont les multiples services de sécurité se sont révélés moins bien coordonnés qu'assumés. Mais fréquemment on assiste aussi à l'inclusion d'entreprises privées et d'organisations hybrides dans des structures qui fonctionnent selon un mode plus horizontal que vertical, et de manière décentralisée. L'étude de l'influence de ce phénomène reste encore trop largement intuitive, reposant sur les informations glanées çà et là par des journalistes d'investigation inquiets des retombées sur les libertés individuelles, elles-mêmes amplement relayées par des universitaires plus militants que scientifiques. Une approche empirique systématique est cependant possible et souhaitable, afin de dépasser les dimensions factuelles ou administratives des articles sensationnalistes ou des rapports officiels laconiques. La boîte à outils méthodologique de l'analyse de réseaux offre à cet égard des ressources éprouvées pour lancer une exploration théorique des reconfigurations actuelles de la gouvernance de la sécurité. Les questions de l'efficacité respective des trois morphologies organisationnelles principales que sont la hiérarchie, le marché et le réseau, et des mécanismes d'imputabilité adaptés à chacune d'elles semblent prioritaires. L'un des défis sera cependant de reconnaître et de prendre en compte la coexistence et l'imbrication de ces trois morphologies, dont la manifestation chaotique s'accorde souvent mal aux désirs d'élégance conceptuelle des chercheurs.

Références

9/11 Commission (National Commission on Terrorist Attacks upon the United States) (2004). *Final report.* New York : W. W. Norton & Company.

Alain, M. (2001). 'The trapeze artist and the ground crew' police cooperation and intelligence exchange mechanisms in Europe and North America : A comparative empirical study. *Policing and Society, 11*, 1-27.

American Civil Liberties Union (2004). *ACLU unveils disturbing new revelations about MATRIX surveillance program.* Washington DC : Communiqué de presse du 20 mai.

Arquilla, J. & Ronfeldt, D. (2001). The advent of netwar (revisited). In J. Arquilla et D. Ronfledt (ed.), *Networks and netwars* (1-25). Santa Monica : Rand.

Barabasi, A. L. (2002). *Linked : the new science of networks.* Cambridge : Perseus Publishing.

Bayley, D. & Shearing, C. (2001). *The new structure of policing : Description, conceptualization, and research agenda.* Washington DC : National Institute of Justice.

Bigo, D. (1996). *Polices en réseau : L'expérience européenne.* Paris : Presses de Science Po.

Braithwaite, J. (2003). Meta risk management and responsive regulation for tax system integrity. *Law & Policy, 25*, 1-16.

Brodeur, J.-P. (1999). Police et prévention au Canada et au Québec. *Les Cahiers de la sécurité intérieure, 37*, 161-181.

Brodeur, J.-P. (2003). *Les visages de la police.* Montréal : PUM.

Brodeur, J.-P. & Monjardet, D. (2003). Connaître la police. In J.-P. Brodeur et D. Monjardet (ed.), *Connaître la police* (9-21). Paris : La Documentation française.

Burkeman, O. & Tuckman, J. (2003, 5 mai), Firm in Florida election fiasco earns millions from files on foreigners. *The Guardian*, p. 12.

Castells, M. (2000). Materials for an exploratory theory of the network society. *British Journal of Sociology, 51*, 5-24.

Castells, M. (2001). *La société en réseau : L'ère de l'information.* Nouvelle édition. Paris : Fayard.

Cherney, A. (2004). *Agency and resistance in the governance of security.* Canberra : Australian National University, Manuscrit de l'auteur.

Coleman, J. (1988). Social capital in the creation of human capital. *American Journal of Sociology, 92*, S95-S120.

Commission du droit du Canada (2002). *En quête de sécurité : Le rôle des forces policières et des agences privées.* Ottawa : CDC.

Crawford, A. (1997). *The local governance of crime.* Oxford : Oxford University Press.

Crawford, A. & Lister, S. (2004). *The extended policing family : Visible patrols in residential areas.* York : Joseph Rowntree Foundation.

Cusson, M. (2002). *Prévenir la délinquance : Les méthodes efficaces.* Paris : PUF.

De Armond, P. (2001). Netwar in the emerald city : WTO protest strategy and tactics. In J. Arquilla & D. Ronfledt (ed.), *Networks and netwars* (201-235). Santa Monica : Rand.

Deflem, M. (1996). International policing in 19th century Europe : The Police Union of German states, 1851-1866. *International Criminal Justice Review*, *6*, 36-57.

Deflem, M. (2002). *Policing world society : Historical foundations of international police cooperation.* Oxford : Oxford University Press.

Degenne, A. & Forsé, M. (1994). *Les réseaux sociaux*. Paris : Armand Colin.

Department of Homeland Security (2004). *Securing our homeland : US Department of Homeland Security strategic plan.* Washington DC : DHS.

Donzelot, J., Mével, C. & Wyvekens, A. (2003). *Faire société : La politique de la ville aux États-Unis et en France.* Paris : Le Seuil.

Duffield, M. (2002). War as a network enterprise : The new security terrain and its implications. *Cultural Values*, *6* (1-2), 153-165.

Dupont, B. (2004). Policing in the age of networks. *Policing & Society*, *14*, 76-91.

Dupont, B., Grabosky, P. & Shearing, C. (2003). The governance of security in weak and failing states. *Criminal Justice*, *3*, 331-349.

Erickson, B. (2001). Good networks and good jobs : The value of social capital to employers and employees. In N. Lin, K.S. Cook & R.S. Burt (ed.), *Social capital : Theory and research* (127-158). New York : Aldine de Gruyter.

Ericson, R. & Haggerty, K. (1997). *Policing the risk society*. Oxford : Clarendon Press.

Espeland, W. (1998). *The struggle for water : Politics, rationality and identity in the American Southwest.* Chicago : University of Chicago Press.

Ferret, J. (2004). The State, policing and 'old continental Europe' : Managing the local/national tension. *Policing & Society*, *14*, 49-65.

Friel, B. (2002). Hierarchies and networks. *Government Executive Magazine*, 1er avril. Page consultée le 12-29-2004 au <http://www.govexec.com/features/0402/0402s2.htm>.

Gagnon, C. & Bacher, J.-L. (2004). Le dispositif canadien de lutte contre le blanchiment d'argent. *Revue internationale de criminologie et de police, 57*, 428-437.

Garreau, J. (2001, 17 septembre). Disconnect the dots. *Washington Post*, p. C1.

Gatto, D. & Thoenig, J.-C. (1993). *La sécurité publique à l'épreuve du terrain.* Paris : L'Harmattan.

Gendarmerie royale du Canada. (2003). *Integrated policing and law enforcement : why and why now ?* Ottawa : GRC.

General Accounting Office. (2003). *Terrorist watch list should be consolidated to promote better integration and sharing*. Washington DC : USGAO.

Gerspacher, N. & Pujas, V. (2004). *International police organisation : The missing link to cooperate effectively ?* Grenoble : Institut d'études politiques, manuscrit des auteurs.

Grabosky, P. (1995). Using non-governmental resources to foster regulatory compliance. *Governance*, *8*, 527-550.

Granovetter, M. (1983). The strength of weak ties : a network theory revisited, *Sociological Theory*, *1*, 201-233.

Seymour Hersh. (2004). *Chain of command*. New York : Harper Collins.

Human Rights Watch. (2004). *The United States' « disappeared » : The CIA long-term's 'ghost detainees'*. New York : Human Rights Watch.

International Network for Social Network Analysis. (2001). Terrorist networks. *Connections*, *24* (3). Page consultée le 12-29-2004 au <http://www.sfu.ca/~insna/Connections-Web/Volume24-3/Cover24-3.htm>.

Johnston, L. & Shearing, C. (2003). *Governing security : Explorations in policing and justice*. Londres : Routledge.

Klerks, P. (2001). The network paradigm applied to criminal organisations : Theoretical nitpicking or a relevant doctrine for investigators ? Recent developments in the Netherlands. *Connections*, *24* (3), 53-65.

Kraska, P. (2001). *Militarizing the American criminal justice system : The changing roles of the armed forces and the police*. Boston : Northeastern University Press.

Krouse, W. J. (2004). *The Multi-State Anti-Terrorism Information Exchange (MATRIX) pilot project*. Washington DC : Congressional Research Service.

Lazega, E. (1994). Analyse de réseaux et sociologie des organisations. *Revue française de sociologie*, *35*, 293-320.

LeBeuf, M.-E. & Paré, S. (2003). *Échange de l'information entre les services policiers canadiens – l'état actuel des connaissances*. Ottawa : Gendarmerie royale du Canada.

Le Galès, P. (1995). Les réseaux d'action publique entre outil passe-partout et théorie de moyenne portée. In P. Le Galès & M. Thatcher (ed.), *Les réseaux de politique publique,* (13-27). Paris : L'Harmattan.

Lemieux, V. (2003). *Les réseaux criminels*. Ottawa : Gendarmerie royale du Canada.

Liang, H.-H. (1992). *The rise of modern police and the European state system from Metternich to the Second World War*. Cambridge : Cambridge University Press.

Lichtblau, E. (2004, 12 décembre). Homeland Security Department experiments with new tool to track financial crime. *New York Times*, p. 48.

Loubet del Bayle, J.-L. (1992). *La police : Approche socio-politique*. Paris : Montchestien.

Lyon, D. (2004). Globalizing surveillance : Comparative and sociological perspectives. *International Sociology*, *19*, 135-149.

Madelin, L. (1903). *Fouché*. (Tome 1). Paris : Plon.

Markle Foundation Task Force (2003). *Creating a trusted information network for homeland security*. Washington DC : Markle Foundation.

Marquis, G. (1993). *Policing Canada's century : A history of the Canadian Association of Chiefs of Police*. Toronto : University of Toronto Press.

Marsh, D. & Rhodes, R. (ed.) (1992). *Policy networks in British government*. Oxford : Clarendon Press.

Morn, F. (1982). *The eye that never sleeps : A history of the Pinkerton National Detective Agency*. Bloomington : Indiana University Press.

Morselli, C. (2003). Career opportunities and network-based privileges in the Cosa Nostra. *Crime. Law and Social Change*, *39*, 383-418.

Murphy, V. (2001, 12 octobre). Spook Valley. *Forbes Magazine*, p. 12-16.

Nadelmann, E. (1997). *Cops across borders : The internationalization of US criminal law enforcement*. University Park : The Pennsylvania State University Press.

Newburn, T. (2001). The commodification of policing : Security networks in the late modern city. *Urban Studies*, *38*, 829–848.

Ocqueteau, F. (2004). *Polices entre État et marché*. Paris : Les Presses de Science Po.

O'Harrow, R. (2005). *No place to hide*. New York : Free Press.

O'Malley P. & Sutton, A. (ed.) (1997). *Crime prevention in Australia : Issues in policy and research*. Leichhardt : The Federation Press.

Osborne, D. & Gaebler, T. (1992). *Reinventing government*. Reading : Addison-Wesley.

Parker, C. (2002). *The open corporation : Effective self-regulation and democracy*. Cambridge : Cambridge University Press.

Pierre, J. & Peters, B. G. (2000). *Governance, politics and the state*. Londres : Macmillan.

Powell, W. (1990). Neither market nor hierarchy : Network forms of organization. *Research in Organizational Behavior*, *12*, 295-336.

Raab, J. & Milward, H. B. (2003). Dark networks as problems. *Journal of Public Administration Research and Theory*, *13* (4), 413-439.

Rhodes, R. (1997). *Understanding governance*. Maidenhead : Open University Press.

Ronfeldt, D. & Arquilla, J. (2001). Emergence and influence of the zapatista social netwar. In J. Arquilla & D. Ronfledt (ed.), *Networks and netwars* (171-199). Santa Monica : Rand.

Rowley, T. (1997). Moving beyond dyadic ties : A network theory of stakeholder influences. *The Academy of Management Review*, *22*, 887-910.

Senator, T. (2002, 30 juillet au 2 août). Evidence extraction and link discovery program. Communication faite lors de la conférence *Darpatech 2002 Symposium*. Anaheim.

Shearing, C. & Stenning, P. (1982). *Private security and private justice : The challenge of the 80s*. Montreal : The Institute for Research on Public Policy.

Shearing, C. & Wood, J. (2003). Governing security for common goods. *International Journal of the Sociology of Law*, *31*, 205-225.

Sheptycki, J. (2002). *In search of transnational policing*. Avebury : Ashgate.

Singel, R. (2004). Airlines ordered to expose data, *Wired News*. Page consultée le 11-12-2004 au <http://www.wired.com/news/privacy/0,1848,65699,00.html>.

Smith Ring, P. (1997). Processes facilitating reliance on trust in inter-organizational networks. In M. Ebers (ed.), *The formation of inter-organizational networks* (113-145). Oxford : Oxford University Press.

Stewart, T. (2001). America's secret weapon. *Business 2.0*, 58-68.

Stinchcombe, A. (1989). An outsider's view of network analyses of power. In F. Petrucci & S. Potter (ed.), *Networks of power* (119-133). New York : Aldine de Gruyter.

Tarrius, A. (2003). Nouvelles circulations transnationales des migrants dans l'« espace Schengen ». La mise à l'épreuve des logiques intégratives et des frontières politiques. *Les Cahiers de la Sécurité Intérieure*, *52*, 65-87.

Tshuma, L. (2000). Hierarchies and government versus networks and governance : Competing regulatory paradigms in global economic regulation. *Social & Legal Studies*, *9*, 115-142.

Tulard, J. (1998). *Joseph Fouché*. Paris : Fayard.

Wacquant, L. (1999). *Les prisons de la misère*. Paris : Raisons d'agir.

Wasserman, S. & Faust, K. (1994). *Social network analysis : Methods and applications*. Cambridge : Cambridge University Press.

Williams, P. (2001). Transnational criminal networks. In J. Arquilla & D. Ronfledt (ed.), *Networks and netwars* (61-97). Santa Monica : Rand.

Zanini, M. & Edwards, S. (2001). The networking of terror in the information age. In J. Arquilla & D. Ronfledt (ed.), *Networks and netwars* (29-60). Santa Monica : Rand.

Zedner, L. (2003). Too much security ? *International Journal of the Sociology of Law*, *31*, 155-184.