L'économie de la sécurité

OCDE

L'économie de la sécurité

OCDE

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

En vertu de l'article 1er de la Convention signée le 14 décembre 1960, à Paris, et entrée en vigueur le 30 septembre 1961, l'Organisation de Coopération et de Développement Économiques (OCDE) a pour objectif de promouvoir des politiques visant :

- à réaliser la plus forte expansion de l'économie et de l'emploi et une progression du niveau de vie dans les pays membres, tout en maintenant la stabilité financière, et à contribuer ainsi au développement de l'économie mondiale ;
- à contribuer à une saine expansion économique dans les pays membres, ainsi que les pays non membres, en voie de développement économique ;
- à contribuer à l'expansion du commerce mondial sur une base multilatérale et non discriminatoire conformément aux obligations internationales.

Les pays membres originaires de l'OCDE sont : l'Allemagne, l'Autriche, la Belgique, le Canada, le Danemark, l'Espagne, les États-Unis, la France, la Grèce, l'Irlande, l'Islande, l'Italie, le Luxembourg, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède, la Suisse et la Turquie. Les pays suivants sont ultérieurement devenus membres par adhésion aux dates indiquées ci-après : le Japon (28 avril 1964), la Finlande (28 janvier 1969), l'Australie (7 juin 1971), la Nouvelle-Zélande (29 mai 1973), le Mexique (18 mai 1994), la République tchèque (21 décembre 1995), la Hongrie (7 mai 1996), la Pologne (22 novembre 1996), la Corée (12 décembre 1996) et la République slovaque (14 décembre 2000). La Commission des Communautés européennes participe aux travaux de l'OCDE (article 13 de la Convention de l'OCDE).

Also available in English under the title:
The Security Economy

© OCDE 2004

Les permissions de reproduction partielle à usage non commercial ou destinée à une formation doivent être adressées au Centre français d'exploitation du droit de copie (CFC), 20, rue des Grands-Augustins, 75006 Paris, France, tél. (33-1) 44 07 47 70, fax (33-1) 46 34 67 19, pour tous les pays à l'exception des États-Unis. Aux États-Unis, l'autorisation doit être obtenue du Copyright Clearance Center, Service Client, (508)750-8400, 222 Rosewood Drive, Danvers, MA 01923 USA, ou CCC Online : *www.copyright.com*. Toute autre demande d'autorisation de reproduction ou de traduction totale ou partielle de cette publication doit être adressée aux Éditions de l'OCDE, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

Avant-propos

Le secteur de la sécurité est un pan important et en pleine expansion de l'activité économique. Ces dernières années, un sentiment de hausse de la criminalité, la menace d'attentats terroristes et la libéralisation croissante de la circulation des biens, des capitaux et des hommes, ont provoqué un accroissement des budgets des pouvoirs publics, des entreprises et des consommateurs consacrés aux biens et services de sécurité. Cette évolution promet d'avoir de profondes répercussions économiques et sociétales à longue échéance. Pour les responsables politiques, l'enjeu est de trouver le moyen de satisfaire le besoin apparent de renforcement de la sécurité sans entraver inutilement l'efficience économique et les droits des citoyens des sociétés libérales.

Mi-2003, j'ai proposé à différents hauts responsables des pays membres de l'OCDE d'explorer le phénomène de la « nouvelle économie de la sécurité ». Il était clair à mes yeux que ce concept général restait partiellement incompris, car il était au fond la résultante de la convergence de nouvelles tendances de nos sociétés. Des technologies toujours plus performantes apportent à nos économies des outils utilisables dans de nouveaux produits et services, dont par exemple la surveillance, le stockage et la récupération de gros volumes de données et d'informations. Des bases de données relationnelles plus volumineuses couplées à une forte capacité de calcul créent de nouvelles possibilités de suivi et de contrôle de l'information sur les produits et services – et sur les individus et l'environnement mondial lui-même. Tout aussi clairement, les questions de sécurité nationale pouvaient selon toute probabilité constituer un axe important de l'intérêt des pouvoirs publics et des entreprises. Ce que nous voulions dans le cadre du Programme de l'OCDE sur l'avenir, c'était offrir une plate-forme de discussion de l'avenir de l'économie de la sécurité, de ses composantes et de ses moteurs, dans le secteur tant public que privé.

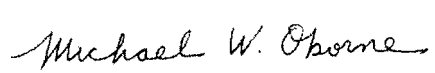
Une première étape a consisté à élaborer le contexte du concept. Pour disposer très tôt des éléments nécessaires, nous avons rédigé un document de délimitation du champ thématique définissant et inventoriant les types de problèmes qui émergent de cette convergence de technologies et de nouveaux besoins sécuritaires. Nous sommes ensuite passés à l'élaboration de la réunion du Forum, base à partir de laquelle nous avons lancé les appels à présentations orales et rapports écrits. Le Forum s'est tenu le 8 décembre 2003 au siège de l'OCDE à Paris.

La réunion s'est articulée en quatre sessions. La première d'entre elles a permis de passer en revue les moteurs sociaux, économiques et institutionnels de la demande

croissante de sécurité, et de dessiner les tendances et les évolutions qui devraient déterminer son ampleur et son orientation futures. La seconde session a examiné l'offre de sécurité, détaillant l'état de plusieurs technologies essentielles d'identification, d'authentification et de surveillance et explorant leur probable évolution au cours de la décennie à venir. Au cours de la troisième session, ce sont les répercussions économiques à plus long terme de l'économie émergente de la sécurité qui ont été abordées : quels arbitrages faudra-t-il consentir au cours des prochaines années entre un surcroît de sécurité d'un côté et l'efficience économique de l'autre ? Quel[s] rôle[s] les pouvoirs publics et les entreprises pourraient-ils jouer pour contribuer à résoudre ces dilemmes ? La quatrième et dernière session a été consacrée aux implications sociétales à moyen et long terme de l'usage croissant de technologies de sécurité. Plus précisément, elle a abordé l'avenir de la « société de la surveillance » et ce qui peut être fait pour orienter le développement et l'utilisation de technologies d'identification et de surveillance sur des pistes que la société considère, tout bien pesé, comme les plus bénéfiques globalement.

Barrie Stevens a conçu et organisé la réunion, et rédigé les deux premiers chapitres du rapport. Jack Radisch a déterminé le champ initial du concept et des questions à aborder, la partie recherche étant confiée à Marit Undseth et le soutien logistique à Concetta Miano. Le volume a été révisé par Randall Holden.

Cet ouvrage est publié sous la responsabilité du Secrétaire général de l'OCDE.



Michael W. Oborne
Directeur,
Questions multidisciplinaires,
Programme de l'OCDE sur l'avenir

L'ÉCONOMIE DE LA SÉCURITÉ – ISBN 92-64-10773-8 – © OCDE 2004

Table des matières

Chapitre 1. **L'économie de la sécurité émergente : une introduction**
par *Barrie Stevens* 7

Chapitre 2. **Les facteurs de la demande de biens et services de sécurité**
par *Barrie Stevens* 19

Chapitre 3. **Biométries**
par *Bernard Didier* 39

Chapitre 4. **RFID : le concept et l'incidence**
par *Steve Hodges* et *Duncan McFarlane* 61

Chapitre 5. **Localisation par satellite : GALILEO**
par *René Oosterlinck* 87

Chapitre 6. **Produits de sécurité : anatomie de la carte d'identité électronique italienne**
par *Alfio Torrisi* et *Luigi Mezzanotte* 103

Chapitre 7. **Économie de la sécurité : arbitrages économiques**
par *Tilman Brück* 113

Chapitre 8. **Les technologies de la surveillance : tendances et répercussions sociales**
par *David Lyon* 141

Annexe : **Liste des participants** 167

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 1

L'économie de la sécurité émergente : une introduction

par
Barrie Stevens
Secrétariat de l'OCDE, Unité consultative auprès du Secrétaire général

Ces dernières années, la « sécurité » est devenue une question tout à fait centrale. Confronté à une multitude de menaces potentielles allant du terrorisme et des virus informatiques à la fraude et au crime organisé, le monde est perçu par beaucoup comme de plus en plus dangereux. De ce fait, la sécurité retient davantage l'attention et la demande de biens et de services dans ce domaine connaît une progression constante, ce qui donne naissance à une palette large et diversifiée d'activités économiques tant publiques que privées, qui composent l'économie de la sécurité émergente.

Le vocable « économie de la sécurité » est, comme le concept qu'il dénote, relativement neuf. Il tente de décrire le kaléidoscope des activités dont l'objet est de prévenir ou d'atténuer le risque d'atteintes délibérées à la vie et aux biens. Dans son acception la plus large, il peut englober la défense et le contre-espionnage, les forces de police, les polices privées, le gardiennage armé et les fournisseurs de technologies de sécurité ; dans un sens plus étroit, il peut se limiter aux dépenses privées de sécurité des personnes et des entreprises. Pour les besoins de la présente publication, nous considérerons l'économie de la sécurité comme le domaine recouvrant essentiellement le secteur de la sécurité et ses interfaces avec les activités sécuritaires des pouvoirs publics et de leurs instances.

Le secteur de la sécurité regroupe des centaines de milliers d'entreprises et d'individus dont l'objectif est de vendre une protection contre les actes malveillants menaçant la vie, les biens et autres actifs, et l'information. Les produits et services offerts sont très variés : alarmes incendie et intrusion ; systèmes de fermeture et coffres-forts ; contrôle électronique d'accès et biométrie ; surveillance électronique des articles et conseils en sécurité ; fourniture de véhicules blindés, d'équipements de gardiennage et de clôtures de sécurité. Le secteur de la sécurité a longtemps fonctionné – en grande partie au moins – séparément des forces civiles et militaires chargées de l'application de la loi et de la sécurité nationale. Ces dernières années, il semble se fondre davantage avec ces autres intervenants. Les entreprises de sécurité plaçaient le plus gros de leurs produits et services auprès des particuliers et des entreprises ; aujourd'hui, les pouvoirs publics sont aussi devenus des clients importants. Ils ont en outre œuvré au renforcement d'une réglementation sur la sécurité qui touche les intervenants privés de plusieurs autres secteurs d'activité. En raison de sa forte diversité, de son atomisation et du manque de véritables points d'unification de l'interface avec la clientèle, il

n'est peut-être pas surprenant que d'aucuns jugent prématuré de parler d'un « secteur de la sécurité ». D'autres estiment cependant qu'aussi flous que puissent être les contours du secteur de la sécurité aujourd'hui, ils se préciseront très probablement dans un avenir assez rapproché. De telles divergences de vues ne sont pas inhabituelles lorsqu'on parle d'un secteur « émergent » important.

Même si l'on retient sa définition relativement restrictive, l'économie de la sécurité ne se laisse pas aisément quantifier. Toutes les mesures sécuritaires qui sont prises ne se traduisent pas en dépenses, ce qui rend leur évaluation ardue. De surcroît, il s'avère difficile, dans de nombreux cas, de mesurer la valeur ajoutée sécuritaire en raison de son intégration à une kyrielle de biens et de services. Il est par ailleurs difficile de trouver des données fiables sur les dépenses sécuritaires, et les estimations sont souvent, dans ce domaine, très approximatives. Ainsi, les évaluations de la taille du secteur de la sécurité privée et de son évolution dans le temps doivent pour la plupart se fonder sur les éléments fournis par les associations professionnelles et les rapports de consultants spécialisés. Dans quelques pays, on dispose d'informations sur les dépenses sécuritaires du secteur public, mais ces renseignements souffrent des mêmes problèmes de délimitation que les dépenses sécuritaires privées.

Malgré ces difficultés de mesure, il semble que le secteur de la sécurité s'annonce comme un acteur économique important et en croissance. Pour sa partie privée, les estimations disponibles aboutissent à un chiffre d'affaires mondial de 100 à 120 milliards d'USD. Les États-Unis en représenteraient la plus grande part, mais d'autres pays de l'OCDE ont eux aussi un secteur de la sécurité de taille non négligeable. Celui de l'Allemagne, par exemple, avoisinerait 4 milliards d'USD, et ceux de la France et du Royaume-Uni 3 milliards d'USD. Si le 11 septembre 2001 n'a pas déclenché de vague majeure de dépenses de sécurité, les données disponibles à plus long terme dessinent une solide croissance du chiffre d'affaires, de l'ordre de 7 à 8 pour cent annuels, très supérieurs aux taux annuels moyens de croissance économique.

Les principaux facteurs de la demande

Quels sont les moteurs d'une expansion aussi rapide ? La croissance de la demande mondiale de biens et services de sécurité est, jusqu'à un certain point, mue par le progrès technologique. Mais comme le montre le chapitre 1, toute une série de facteurs sociaux, économiques et institutionnels divers en sont les principaux moteurs.

Ces facteurs sont souvent liés à une demande multiple, impliquant les pouvoirs publics, les entreprises et les particuliers, qui recherchent davantage de prévention, de détection et de protection contre des infractions telles que

la fraude et les agissements de l'économie souterraine, le vol ou le vandalisme, mais aussi contre des infractions liées aux stupéfiants et contre la criminalité violente. Il est intéressant de noter que, d'après les statistiques, la criminalité « ordinaire » (par opposition à la criminalité « organisée ») affiche en fait un taux en diminution, dans de nombreux pays, depuis le milieu des années 90. Le crime organisé, lui, a au contraire progressé en maints endroits. Le tableau global de la criminalité serait donc en fait très contrasté, et la perception qu'ont les gens du niveau de l'activité criminelle serait un ingrédient majeur de leur sentiment d'insécurité et de leur conviction que, dans ce cas, la technologie n'est pas toujours la solution.

Même si certaines catégories de crimes sont en recul dans certains pays, le fardeau global de la criminalité sur l'économie semble colossal. De récentes tentatives de quantification de son coût au niveau national l'estiment à 20 pour cent du PIB aux États-Unis, et à environ 7 pour cent du PIB au Royaume-Uni. Cet exercice prend en compte non seulement les coûts réels des dépenses de prévention de la criminalité et des dépenses pénitentiaires, mais aussi les coûts immatériels tels que les dommages physiques et le stress psychologique.

Après les événements du 11 septembre notamment, le risque de dommages de grande ampleur dus aux actes de terrorisme et la menace d'armes de destruction massive sont aussi apparus comme des facteurs importants alimentant la demande croissante de sécurité.

La mondialisation est devenue un autre vecteur important des préoccupations sécuritaires. Ainsi, l'expansion du commerce extérieur stimule le transport des personnes et des marchandises. La croissance des transports de marchandises et de personnes par air, rail, route et mer accroît le risque de failles sécuritaires qui facilitent le vol et la contrebande organisée, ce qui donne incite les pouvoirs publics à redoubler d'efforts pour resserrer la surveillance transfrontalière. La progression de l'immigration affaiblit la capacité des pays d'empêcher les menaces clandestines, tout en alimentant dans certains cas le sentiment local d'insécurité. L'internationalisation croissante des activités de production a mondialisé, spécialisé et fragmenté les filières de communication et d'approvisionnement, donnant ainsi naissance à des vulnérabilités particulières. Dans le même temps, les entreprises et les gouvernements s'efforcent de mener leurs opérations de façon plus efficiente et de gérer la sécurité de manière plus efficace par rapport aux coûts ; dans certains cas (la création aux États-Unis du ministère de la Sécurité intérieure en est un exemple frappant), une restructuration institutionnelle a contribué à stimuler la demande. Dans l'intervalle, des technologies nouvelles et toujours plus sophistiquées de surveillance et d'identification arrivent sur le marché à des prix toujours plus abordables.

Les projections et prévisions émanant de différentes sources semblent indiquer que ces moteurs continueront de stimuler les activités liées à la sécurité au cours des années à venir. L'accroissement de la mobilité devrait placer les pouvoirs publics et les entreprises face à des défis particuliers en matière de sécurité et d'efficience. Le commerce mondial devrait continuer de progresser plus vite que la croissance économique à moyen terme, et s'accompagner de taux d'expansion élevés dans différents secteurs du transport tels que le fret aérien. Pareillement, les pressions migratoires devraient perdurer au cours des prochaines décennies. Les Nations unies, par exemple, ont établi des projections de flux nets annuels moyens dépassant le million d'individus vers les États-Unis, 200 000 personnes vers l'Allemagne et 170 000 vers le Canada. Et l'essor accru du commerce électronique offrira toute latitude à la cybercriminalité. Enfin, il reste la question, en particulier dans les pays de l'OCDE, de l'impact futur du vieillissement de la société sur les perceptions générales du risque et la demande de biens et services de sécurité.

Les technologies d'identification et de surveillance de demain

Dans ce contexte d'expansion globale de l'économie de la sécurité, les technologies utilisées pour assurer les fonctions de sécurité ont aussi tiré parti de cette croissance substantielle. On estime par exemple que le marché des produits de surveillance et d'identification approche aujourd'hui les 15 milliards d'USD. Ces produits constituent la colonne vertébrale des systèmes de sécurité d'entreprise et assurent le contrôle des accès, la surveillance périmétrique et la reconnaissance biométrique. Les produits de sécurité informatique représentent un marché estimé à 4 milliards d'USD et utilisent jetons, cartes et biométrie pour assurer la sécurité frontale des systèmes en vérifiant les accès des utilisateurs. Les projections de croissance effectuées pour les 7 à 10 années à venir sont aussi très prometteuses. En termes globaux, le secteur de la sécurité devrait conserver son taux de croissance de 7 à 8 pour cent par an, mais les perspectives de certains segments de ce marché sont particulièrement favorables : c'est notamment le cas de la biométrie, des technologies d'identification par radiofréquences (RFID) et de la sécurité informatique.

Parmi les technologies qui ont surgi ces dernières années et dont on attend qu'elles jouent un rôle sécuritaire essentiel à l'avenir figurent la RFID et la biométrie ; on peut y adjoindre la navigation et le suivi par satellite, le chiffrement et les télécommunications. Par ailleurs, certaines technologies de surveillance plus anciennes gagnent en visibilité en raison de leur fusion avec les technologies de l'information et des communications (TIC) : la télévision en circuit fermé en est un exemple frappant.

La biométrie

La biométrie est devenue, depuis la fin des années 90, une solution de plus en plus viable pour sécuriser l'accès aux locaux, aux ordinateurs et aux réseaux. La numérisation du doigt, du visage, de l'iris, de la rétine ou de la voix est déjà employée dans différentes applications allant de l'identification des citoyens et de l'accès réseau à la surveillance et la téléphonie. Dans l'avenir, ces applications devraient s'étendre très vite, et comme le souligne Bernard Didier au chapitre 2, des efforts importants seront probablement nécessaires pour faire progresser leurs performances, par exemple en améliorant les techniques de détection des artéfacts biométriques (fausses empreintes, faux iris, etc.) et de développement de la surveillance par l'identification à distance. Il faudra néanmoins trouver des solutions efficaces si l'on veut vaincre les résistances du public en matière de prise d'empreintes ou de respect de la vie privée.

Les systèmes d'identification par radiofréquences

La popularité des technologies de RFID s'est considérablement accrue ces dernières années. Le commerce en particulier utilise des technologies de type appareils de traçage et étiquettes intelligentes associées à des détecteurs de transmission et des lecteurs intelligents pour obtenir des informations sur l'emplacement des marchandises et le comportement des consommateurs. Différents systèmes sont à l'œuvre : surveillance électronique d'articles (EAS), capture de données portables, mise en réseau de systèmes et systèmes de positionnement – mais à une échelle très réduite car la technologie RFID reste trop onéreuse pour un usage massif, par exemple, dans la grande distribution. Un large éventail de dispositifs pilotes verront probablement le jour au cours des prochaines années pour différents types de traçage : vêtements, marchandises dangereuses, biens de consommation sous emballage, devises ou patients. Dans le chapitre 3, Steve Hodges souligne également les usages potentiels de la RFID dans des magasins « sans caisses », pour la gestion des stocks à domicile ou pour la localisation des produits dans la chaîne d'approvisionnement. Il faudra cependant surmonter différents obstacles, dont notamment l'ampleur des investissements nécessaires pour mettre en place des systèmes de RFID et le problème épineux du respect de la vie privée.

La localisation et la surveillance par satellite

Comme le montre René Oosterlinck au chapitre 4, les applications de ces technologies ont connu une expansion importante ces dernières années. Elles sont actuellement utilisées pour une multitude de fonctions connexes : technologies de navigation à l'intention du trafic maritime et des automobiles, observation des mouvements des navires et du transport terrestre des

marchandises, gestion des flottes de véhicules et suivi des véhicules à des fins de facturation de l'usage des infrastructures routières. Avec le lancement de nouveaux satellites et la mise en service, dans le courant de la présente décennie, de systèmes satellitaires très poussés tels que Galileo, les utilisations actuelles devraient s'amplifier et de nouvelles applications émerger.

Les cartes à « technologie hybride »

Des cartes mémoire optiques ultramodernes dotées d'hologrammes permettant une authentification visuelle rapide entrent en service ; elles contiennent souvent des fonctionnalités de sécurité à base d'images microscopiques associées à des puces multiapplicatives donnant accès, par exemple, à des services publics électroniques. Dans le chapitre 5, Alfio Torrisi et Luigi Mezzanotte montrent l'utilisation qui est faite de ces technologies en Italie pour tenter de doter tous les citoyens, dans les cinq ans, d'une carte d'identité sécurisée.

Pour résumer, l'élément crucial de l'essor des technologies de la sécurité sur le moyen et le long terme ne sera probablement pas la technologie, mais bien plutôt le degré de leur acceptation par le public, la reconnaissance effective de leurs avantages et la priorité accordée par les consommateurs à leurs craintes sécuritaires.

Conséquences économiques à plus long terme

Comme l'ont démontré les événements de ces dernières années, la sécurité des économies locales, nationales et régionales subit des menaces nombreuses et variées dont le tribut peut en outre s'avérer très lourd. On estime aujourd'hui, en dehors de la perte tragique de vies humaines, que le coût économique des attentats terroristes du 11 septembre 2001 a avoisiné 120 milliards d'USD. Ce chiffre inclut non seulement les sinistres concernant les biens matériels et infrastructures, mais aussi les répercussions sur l'emploi, les marchés financiers, la continuité opérationnelle des entreprises, etc. Les principaux secteurs d'activité ont ensuite commencé à se saisir du problème des grandes menaces auxquelles ils sont exposés. Par exemple, le secteur du transport maritime considère qu'un attentat terroriste bien coordonné visant son système provoquerait des dommages chiffrables à des dizaines de milliards d'USD. Néanmoins, des agissements moins dramatiques peuvent aussi avoir un coût très élevé. À titre d'illustration, aux États-Unis, le coût de la fraude au niveau des seuls droits à prestations représentait, selon les estimations, 750 millions de dollars à la fin des années 90 ; et l'usurpation d'identité coûterait chaque année quelque 2 milliards de dollars aux banques et autres établissements de crédit. Plus de deux cinquièmes des entreprises

britanniques ont récemment signalé des violations de leur sécurité, qui représenteraient des dommages cumulés de plusieurs milliards de GBP.

L'amélioration de la sécurité a cependant un coût, qui prend généralement l'une ou l'autre des formes suivantes : soit l'investissement que nécessite la mise en place des dispositions de sécurité utiles, soit l'impact négatif que peuvent avoir ces dernières sur le fonctionnement du secteur ou de l'ensemble de l'économie.

Confrontés aux dommages potentiels colossaux que représentent des menaces sérieuses, les pouvoirs publics et les entreprises sont dans l'obligation d'envisager des investissements potentiellement énormes. Pour revenir à l'exemple du transport maritime, on estime à nettement plus de 600 millions d'USD le fardeau financier initial imposé aux armateurs par les mesures de sécurité négociées à l'Organisation maritime internationale (OMI). Presque partout, les entreprises investissent davantage pour protéger leurs actifs et leurs systèmes d'information. Aux États-Unis par exemple, on estime que le coût total des mesures de sécurité intérieure assumé par le secteur privé à la suite des attentats du 11 septembre atteindra une dizaine de milliards d'USD par an, après avoir été probablement beaucoup plus élevé au début, c'est-à-dire en 2003, avec des dépenses comprises entre 46 et 76 milliards d'USD. Par ailleurs, les gouvernements et l'administration en général ont accru leurs dépenses globales de sécurité de manière parfois très notable. Le budget américain consacré à la sécurité intérieure a doublé entre les exercices budgétaires 2002 et 2003, où il a nettement dépassé les 30 milliards d'USD : le financement de la sécurité aérienne atteint désormais 4.8 milliards d'USD et celui de la sécurité frontalière 10.6 milliards d'USD. Que ces investissements soient financés par la fiscalité ou le secteur privé, leur impact sur l'économie n'est pas négligeable.

Le resserrement de la sécurité peut aussi être synonyme d'un allongement des délais de livraison ou de perturbations de filières d'approvisionnement internationales et de systèmes de livraison en flux tendus réglés avec soin. À la suite des préoccupations sécuritaires croissantes de ces dernières années, les partenaires commerciaux ont dû faire face à un accroissement des coûts de transport, de manutention, d'assurance et de passage en douane. Ces coûts « frictionnels » tendent à renchérir les échanges et amoindrir les flux commerciaux. Selon des simulations de l'OCDE, les mesures prises à la suite du 11 septembre pourraient accroître le coût des échanges d'un pour cent, ce qui représente une perte mondiale de richesse d'environ 75 milliards d'USD annuels.

Comme l'indique Tilman Brück au chapitre 6, il existe d'autres arbitrages potentiels, par exemple entre sécurité et mondialisation, ou entre sécurité et progrès technologique. Il faut aussi penser à d'autres effets importants,

indirects et secondaires, de l'insécurité, qui sont pour la plupart mal compris et difficiles à quantifier.

Ces facteurs doivent bien entendu être mis en perspective. À court et moyen terme, les coûts peuvent être élevés, mais dans la mesure où ils préviennent des dommages et des perturbations d'envergure, ils sont porteurs d'effets positifs à long terme considérables. La question est de savoir comment équilibrer de manière optimale les mesures de sécurité et l'efficience. Les nouvelles technologies peuvent y contribuer, et la littérature abonde d'études de cas illustratives. Les auteurs d'une étude sur un nouveau système de gestion électronique des manifestes proposé par les douanes américaines ont estimé à 22 milliards d'USD sur 20 ans les économies que ce système engendrerait pour les seuls importateurs américains, et à plus de 4 milliards d'USD sur la même période celles dont bénéficierait l'administration américaine.

Il reste cependant des possibilités de réévaluation des rôles respectifs des secteurs public et privé. Le principal argument motivant l'intervention des pouvoirs publics est le caractère « bien public » de la sécurité. Les agents ne prennent pas nécessairement en compte l'externalité positive que leur investissement sécuritaire revêt pour autrui. Du coup, le niveau effectif de sécurité n'est en général pas optimisé. De telles conséquences regrettables peuvent être atténuées par une réglementation ou une coordination accompagnée d'un dispositif crédible de mise en œuvre. Mais les questions de l'ampleur de l'implication des pouvoirs publics, des modalités de leur intervention et des mesures à privilégier restent posées.

Étant donné les externalités négatives liées aux grands cataclysmes, des fonds publics sont peut-être en mesure d'aider le secteur privé à améliorer la sécurité, à condition d'éviter les écueils classiques du subventionnement. Lorsqu'une réglementation publique semble être l'outil le plus adapté, l'implication des entreprises touchées est essentielle. D'ailleurs, on a remarqué ces dernières années que les compagnies aériennes ou les institutions financières avaient été contraintes d'endosser une responsabilité bien plus forte en matière de sécurité. Il en a souvent résulté, chez les acteurs du secteur privé, le sentiment d'un transfert accru des risques au secteur privé, avec une prise en charge par les entreprises de coûts qui peuvent être significatifs sans être toujours visibles. Néanmoins, même si un transfert des coûts sécuritaires entre les porteurs publics et privés du risque peut éventuellement se justifier amplement, il faut opérer des choix difficiles quant à l'instrument le mieux adapté, comme par exemple l'impôt ou la réglementation. Clairement, il faudra réfléchir davantage à la manière d'adapter aux conditions et préférences en vigueur les politiques publiques touchant à la sécurité de l'économie.

Il semble qu'il y ait dans le domaine de la sécurité un fort potentiel de coopération entre les secteurs public et privé, en particulier pour les dispositifs volontaires du secteur privé bénéficiant du soutien des pouvoirs publics. Ces dispositifs peuvent, par exemple, prendre la forme d'initiatives visant à assurer l'intégrité de filières d'approvisionnement entières au moyen d'accords alliant chargeurs, intermédiaires et transporteurs, les pouvoirs publics se posant à la fois en partenaires actifs de l'accord (par exemple les services des douanes et de l'immigration) et en facilitateurs (par exemple en externalisant l'assurance, la validation et la certification auprès d'entités privées agréées).

Conséquences sociétales à plus long terme

La généralisation et la technicité accrue des technologies de sécurité suscitent plusieurs évolutions parallèles. Tout d'abord, la surveillance devient de plus en plus *intense*. Elle connaît aussi une *privatisation* accrue : aux États-Unis, par exemple, les dépenses consacrées à la sécurité privée seraient le double de celles consacrées à l'application de la législation, et ont plus que quintuplé entre 1980 et 2000. En outre, les technologies de sécurité sont toujours plus *automatisées*, de plus en plus *intégrées* avec des bases de données contenant des informations personnelles, et aussi de plus en plus *mondialisées*.

Les chapitres susmentionnés détaillent l'utilisation croissante des technologies de surveillance et annoncent une croissance future considérable de ce secteur. L'efficacité accrue des technologies tient au moins en partie à leur mise en relation avec des bases de données consultables et à l'emploi de technologies informatiques très performantes pour les opérations de vérification, de tri et d'identification. La télévision en circuit fermé est un bon exemple : ses systèmes de reconnaissance faciale sont algorithmiques (ou codés de manière mathématique) afin de permettre à des ordinateurs d'opérer des tris et des classements en fonction de caractéristiques faciales, d'expressions ou de profils comportementaux. Ainsi, comme le souligne David Lyon au chapitre 7, ces processus de « catégorisation sociale » et de « discrimination » connaissent en ce XXI^{e} siècle une automatisation croissante. Il est intéressant de noter que ces techniques de tri ne se sont pas développées seulement dans le domaine de l'application de la loi et de l'administration, mais aussi dans celui du marketing. Ainsi, les techniques de surveillance catégorisent les gens (souvent à leur insu), qu'ils soient considérés comme des malfaiteurs ou des consommateurs potentiels. Il en résulte un essor de l'utilisation des profils de risques et un poids accru du « profilage prédictif ».

Simultanément, dans les entreprises publiques comme privées, dans les organes de l'État comme la société civile, les pratiques de surveillance convergent et des bases de données de plusieurs origines – services publics,

police, services de renseignement, entreprises, consommateurs – semblent devoir connaître une intégration croissante. Par ailleurs, en raison de l'entrelacement des réseaux de données publiques et commerciales, le potentiel de surveillance globale (aux aéroports et aux ports, par le biais des données que recueillent les multinationales, etc.) se renforce considérablement.

Il en découle d'importantes questions sur la façon dont la société dans son ensemble choisira de répondre à la généralisation des technologies de surveillance et d'identification dans les années à venir. Jusqu'à maintenant, par exemple, les libertés sécuritaires et démocratiques ont en général été considérées comme des choix mutuellement exclusifs plutôt que potentiellement complémentaires. Les questions qui se posent en matière de respect de la vie privée sont importantes, mais le thème de la responsabilité et de la transparence l'est tout autant pour l'avenir : comment les systèmes de surveillance et de traçage sont-ils contrôlés ? Qui crée les catégories ? Quelles sont les conséquences, pour le commun des mortels, de la catégorisation sociale et du profilage des risques ? Et les pouvoirs publics resteront-ils considérés comme l'instance réglementaire de prédilection alors qu'existent en fait de nombreuses possibilités, pour des organisations et des agences locales, de s'autoréglementer dans le cadre d'un dispositif légal établi ?

Le tableau qui se dessine pour l'avenir n'est pas entièrement négatif. Certaines organisations sont de fait beaucoup plus précautionneuses à l'endroit des renseignements personnels et sensibles, la conscience de la vulnérabilité des données personnelles va croissant, et des conventions internationales restreignant considérablement les transferts internationaux de données personnelles ont récemment vu le jour. Pour de nombreux observateurs, les progrès des technologies d'identification et de surveillance semblent inexorables ; l'action peut-être la plus efficace est donc d'orienter leur évolution et leur emploi selon des modes que la société considère en général comme les plus bénéfiques. L'équilibre atteint entre les technologies en question, l'évaluation par la société de leurs avantages et inconvénients, et la réponse du législateur sera à ce titre déterminant.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 2

Les facteurs de la demande de biens et services de sécurité

par

Barrie Stevens
Secrétariat de l'OCDE, Unité consultative auprès du Secrétaire général

Le secteur de la sécurité est en train d'émerger en tant qu'acteur économique important en pleine croissance. Il regroupe des centaines de milliers d'entreprises et d'individus dont l'objectif est de vendre de la *sécurité*, c'est-à-dire les moyens de protéger la vie, les biens et l'information. Les produits et services qu'il propose vont des plus simples alarmes incendie et intrusion aux dispositifs biométriques les plus avancés. Selon certaines estimations, le chiffre d'affaires du secteur dépasse les 100 milliards d'USD. La plus grande part provient des États-Unis, mais d'autres pays de l'OCDE ont également un secteur de la sécurité important ; par exemple, celui de l'Allemagne est estimé à environ 4 milliards d'USD, et ceux du Royaume-Uni et de la France à environ 3 milliards chacun. Au niveau mondial, le taux de croissance de ce secteur a oscillé entre 7 et 8 pour cent chaque année – une performance très supérieure à celle de la croissance économique.

Cette expansion remarquable des activités du secteur de la sécurité est façonnée par des facteurs sociaux, économiques et institutionnels nombreux et très variés. La criminalité et la perception qu'en a la population, ainsi que le désir de la prévenir et de s'en protéger, jouent un rôle important. La crainte des conséquences des actions terroristes a aussi pesé ces dernières années. Des forces économiques plus vastes sont également à l'œuvre. La mondialisation intensifie les mouvements d'individus, de biens et de services sur la planète, en apportant à de nombreuses populations une prospérité accrue, mais aussi des risques plus forts de contrebande, de vol, de trafic de stupéfiants, de contrefaçon, d'immigration illégale, de perturbation des réseaux mondiaux d'approvisionnement, etc. Simultanément, les entreprises et les gouvernements recherchent des moyens de mener leurs opérations de façon plus efficiente et de gérer la sécurité de manière plus rentable, tandis que des technologies nouvelles et toujours plus pointues de surveillance et d'identification arrivent sur le marché à des prix toujours plus abordables.

L'ambition du présent chapitre est de proposer un panorama plus systématique de ces facteurs et d'explorer leur signification en tant que moteurs de la demande de biens et services de sécurité. Les projections citées ici ne cherchent aucunement à prévoir l'avenir, mais simplement à donner une idée du potentiel de croissance induit par nombre des facteurs susceptibles de déterminer l'environnement de la sécurité au cours des années à venir.

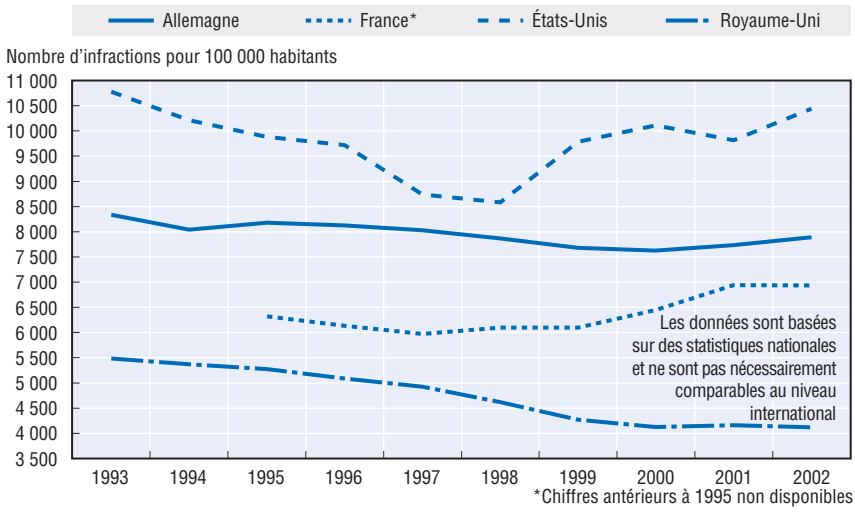
1. Une préoccupation croissante à l'égard des activités criminelles

Quel que soit le mode de mesure, le fardeau cumulé que représente la criminalité pour l'économie est énorme. Des études récentes ont estimé son coût national à environ 20 pour cent du PIB aux États-Unis et à 7 pour cent du PIB au Royaume-Uni. Ces estimations englobent les coûts réels des dépenses de prévention de la criminalité et des dépenses pénitentiaires, mais aussi les coûts immatériels des dommages physiques ou du stress psychologique.

Trois thèmes se détachent du point de vue de la relation entre les tendances de la criminalité et la demande de biens et services de sécurité. Tout d'abord, l'insécurité fait partie intégrante des sociétés modernes, et le besoin de sécurité est donc très subjectif. Il est fréquent qu'aucune mesure de prévention ou de protection, aussi forte soit-elle, ne calme l'anxiété fondamentale des gens. En second lieu, il s'ensuit de ce constat que la *perception* par les individus de la criminalité, de ses conséquences et de sa gravité a toutes les chances d'avoir autant d'importance que son niveau effectif. Et troisièmement, si les taux de criminalité constatés ces dernières années dans la plupart des pays de l'OCDE révèlent quelques grandes tendances communes, certaines évolutions restent inégales à la fois selon le pays et selon la catégorie criminelle.

A priori, il ne semble pas déplacé de soupçonner l'existence d'un lien fort entre les taux de la criminalité ordinaire (par opposition à la criminalité

Figure 1. **Tendances du niveau de la criminalité déclaré dans quelques pays de l'OCDE, 1993-2002**



Source : OCDE, tiré d'Interpol, 2003.

organisée) d'un côté et la demande de biens et services de sécurité de l'autre. Au niveau global, cependant, cette relation est tout sauf simple, et les variations des niveaux globaux de la criminalité ne semblent pas constituer un indicateur satisfaisant des tendances générales des dépenses de sécurité. Comme nous l'avons indiqué plus haut, les marchés des biens et services de sécurité ont crû très vite – alors que dans plusieurs pays de l'OCDE, les statistiques criminelles connaissaient un pic au début des années 90 (après une hausse significative au cours des années 80) pour ensuite chuter.

Des ventilations plus détaillées des données concernant la criminalité fournissent ici ou là des indices intéressants sur la relation en question. Les chiffres globaux des États-Unis, par exemple, montrent un recul de l'ensemble des types d'infractions, cambriolages compris, depuis le début ou le milieu des années 90. Néanmoins, la ventilation selon le lieu indique que les cambriolages chez les particuliers ont en fait augmenté au cours de la même période. Ce constat peut contribuer à expliquer l'usage croissant de la vidéosurveillance, d'alarmes et d'autres systèmes de sécurité dans les foyers américains malgré le déclin général des taux de criminalité.

En raison de la complexité des statistiques de la criminalité et des problèmes bien connus de sous-déclaration, de sur-déclaration ou d'écarts entre les infractions déclarées et les infractions recensées, on pourrait aussi soutenir, bien sûr, que les statistiques officielles ne reflètent pas la perception qu'a le citoyen ordinaire de l'insécurité face à la recrudescence des infractions liées aux stupéfiants, de la violence urbaine et de différentes autres formes de délinquance ou de crime. Ce point n'est pas toujours corroboré par les enquêtes menées auprès des particuliers. La *British Crime Survey* (enquête britannique sur la criminalité), par exemple, suit les tendances des craintes vis-à-vis de différentes sortes de crimes et délits (cambriolages, agressions, viols), ainsi que l'évaluation par chacun de sa sécurité personnelle. Globalement, les tendances décrites par cette enquête épousent très bien le déclin général des taux de la criminalité enregistré au cours des années 90.

Pour l'avenir, on ne peut que spéculer sur l'effet potentiel des évolutions socioéconomiques plus larges sur le niveau de la criminalité et sur la perception qu'en auront les citoyens. La hausse des revenus mènera-t-elle à un amoindrissement des conséquences de la criminalité ? La proportion croissante des personnes âgées dans les populations des pays de l'OCDE changera-t-elle fondamentalement l'attitude de la société vis-à-vis de la sécurité (en suscitant par exemple davantage de complexes résidentiels et de centres urbains barricadés) ?

En ce qui concerne le crime organisé, les données disponibles laissent à penser que les recettes annuelles actuelles des activités criminelles illicites

sont énormes. Le NIC (*National Intelligence Council*, ou Conseil national de renseignement) en fait l'estimation suivante :

- 100-300 milliards d'USD pour le trafic de drogues.
- 9 milliards d'USD pour le vol de véhicules (rien qu'aux États-Unis et en Europe).
- 7 milliards d'USD pour le passage d'êtres humains en contrebande.
- 1 milliard d'USD pour le vol de biens couverts par la propriété intellectuelle.

On ne décèle pourtant pas de tendance générale et uniforme concernant le niveau de la criminalité organisée. En Europe, par exemple, certains pays signalent une hausse de ce niveau et un accroissement du nombre de groupes criminels organisés, tandis que d'autres observent une certaine stabilisation, voire un recul. La criminalité transnationale pose des problèmes particuliers. Même si les informations à son sujet restent parcellaires, il semblerait qu'elle soit en hausse. Comme nous l'avons noté plus haut, la coopération transfrontalière grandissante des organisations criminelles provient en partie de l'interdépendance croissante des économies nationales et des trafics transfrontaliers d'êtres humains et de marchandises. L'accélération future de la mondialisation s'accompagnera de débouchés nouveaux pour le crime transnational, sauf si des mesures adaptées – notamment une coopération et une coordination internationales améliorées – sont prises.

2. L'évolution des modalités de l'action terroriste

On a vu apparaître ces dernières années des formes de terrorisme qui présentent des différences notables avec ce que l'on pourrait appeler le terrorisme « traditionnel » : leur objectif est souvent de combattre durablement l'ensemble d'un système économique, social, politique ou culturel ; elles ont acquis une dimension plus mondiale ; et comme l'ont montré les événements du 11 septembre 2001, de Bali ou d'Istanbul, les attentats visent souvent à tuer autant de civils que possible – accentuant en cela une tendance qui avait vu le jour dès les années 80. On a ainsi observé que le nombre d'attentats terroristes transfrontaliers avait chuté de près de 60 % entre les années 80 et les années 90, mais que le nombre de victimes – tués ou blessés – avait augmenté de 20 %.

Ainsi, les lieux très fréquentés tels que le métro, les gares ferroviaires, les centres commerciaux et les grands bâtiments sont devenus des cibles privilégiées. En outre, les formes plus récentes du terrorisme s'efforcent d'exploiter la dépendance des sociétés modernes vis-à-vis d'infrastructures vitales touchant à l'énergie, à l'eau, aux transports, à la santé, aux services financiers et aux systèmes d'information. La destruction ou à tout le moins la perturbation durable d'infrastructures de cette nature peut avoir un coût humain et économique considérable. La protection des lieux publics et des

infrastructures vitales est donc devenue une tâche prioritaire non seulement pour les pouvoirs publics, mais aussi pour les exploitants d'installations essentielles, ce qui n'a pas manqué de stimuler les services de surveillance, de prévention et de protection.

3. La mobilité croissante des personnes et des biens

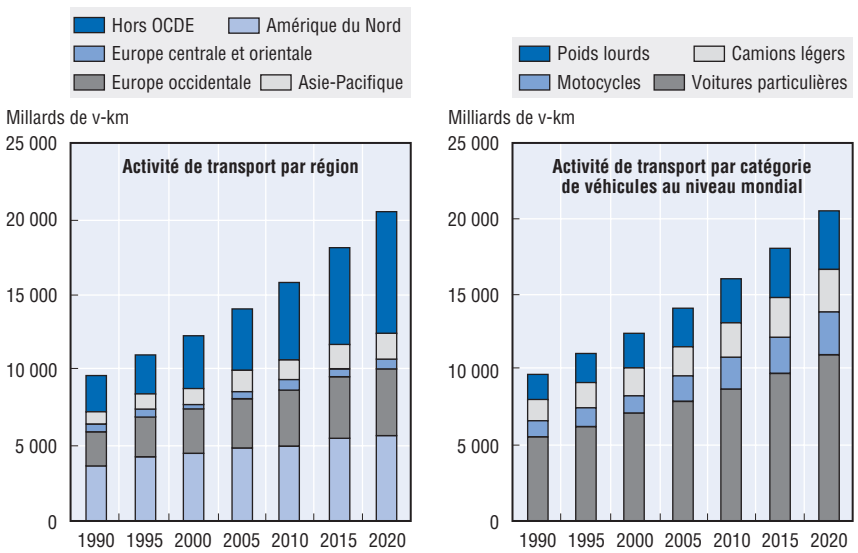
Le processus de mondialisation des décennies récentes a été largement alimenté par la croissance des transports et des communications à tous les niveaux – local, régional, national et international.

La hausse rapide et soutenue des mouvements mondiaux de personnes et de marchandises a aiguillonné l'activité économique et contribué de manière importante à la prospérité de maintes sociétés. Le revers de la médaille, cependant, est que ces mêmes canaux sont vulnérables au vol, à la fraude, au trafic d'êtres humains et d'animaux ou aux opérations terroristes, ce qui contraint les pouvoirs publics et les entreprises à surveiller ces mouvements plus étroitement.

a) La mobilité des individus

L'expansion du transport de voyageurs sous toutes ses formes a été colossale, mue du côté de la demande par la croissance économique, un

Figure 2. **Distance parcourue par les véhicules à moteur (v-km), 1990-2020**



Source : Perspectives de l'environnement de l'OCDE, 2001.

L'ÉCONOMIE DE LA SÉCURITÉ – ISBN 92-64-10773-8 – © OCDE 2004

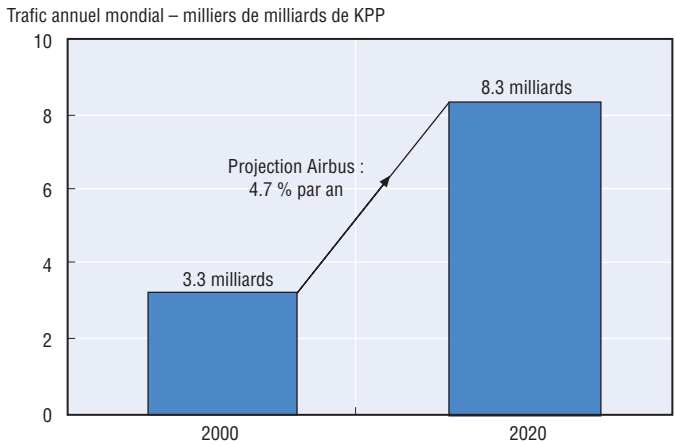
revenu disponible plus élevé et des périodes de loisirs plus longues, et du côté de l'offre par la chute des prix des transports et le progrès technologique.

Comme l'illustre la figure 2 ci-dessus, le trafic routier des particuliers a connu une expansion remarquable. D'autres formes de transport de voyageurs ont elles aussi progressé : le transport aérien, par exemple, a affiché une croissance particulièrement rapide qui s'est traduite par une expansion annuelle moyenne de 9 % depuis 1960. Cette croissance, à un rythme toutefois moins soutenu, devrait perdurer à l'avenir. Les constructeurs aéronautiques tels qu'Airbus prévoient un doublement au moins du trafic aérien entre aujourd'hui et 2020, sous l'effet notamment de la hausse des revenus, des progrès de l'efficacité des transporteurs et de la baisse des tarifs.

C'est dans la région asiatique, où la progression des vols interrégionaux devrait être rapide, que l'on attend la plus forte croissance du trafic aérien international de passagers, ainsi qu'entre l'Asie et l'Amérique du Nord et entre l'Asie et l'Europe. Le trafic limité à l'Europe devrait aussi connaître une hausse rapide liée au renforcement et à l'élargissement de l'intégration économique dus à l'adhésion de nouveaux pays à l'UE. Ces tendances sont une indication des pressions auxquelles les pouvoirs publics, les agences, les transporteurs et les exploitants d'aéroports seront soumis ces prochaines années dans leurs activités de traitement d'un trafic passager international en hausse.

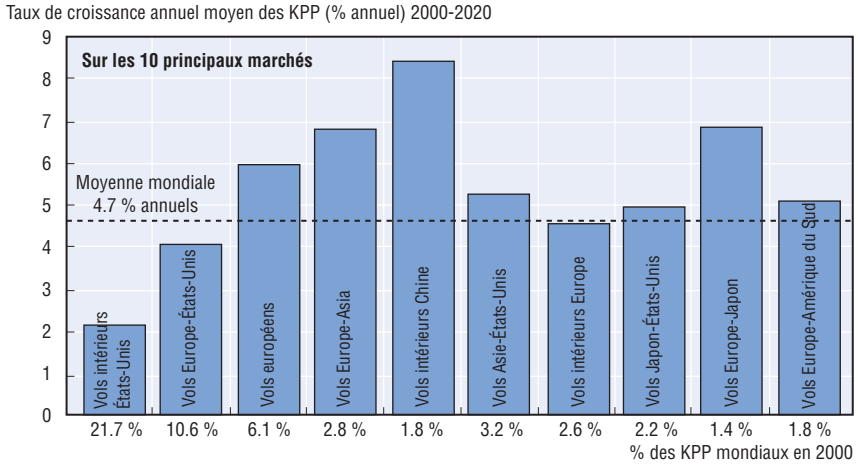
Les migrations internationales font partie intégrante de cette situation générale. Les entrées d'étrangers dans les pays de l'OCDE ont commencé à

Figure 3. **Projections du trafic aérien passagers : croissance du trafic aérien 2000-2020**



Source : OCDE.

Figure 4. **Projections du trafic aérien passagers : les 10 principaux marchés**

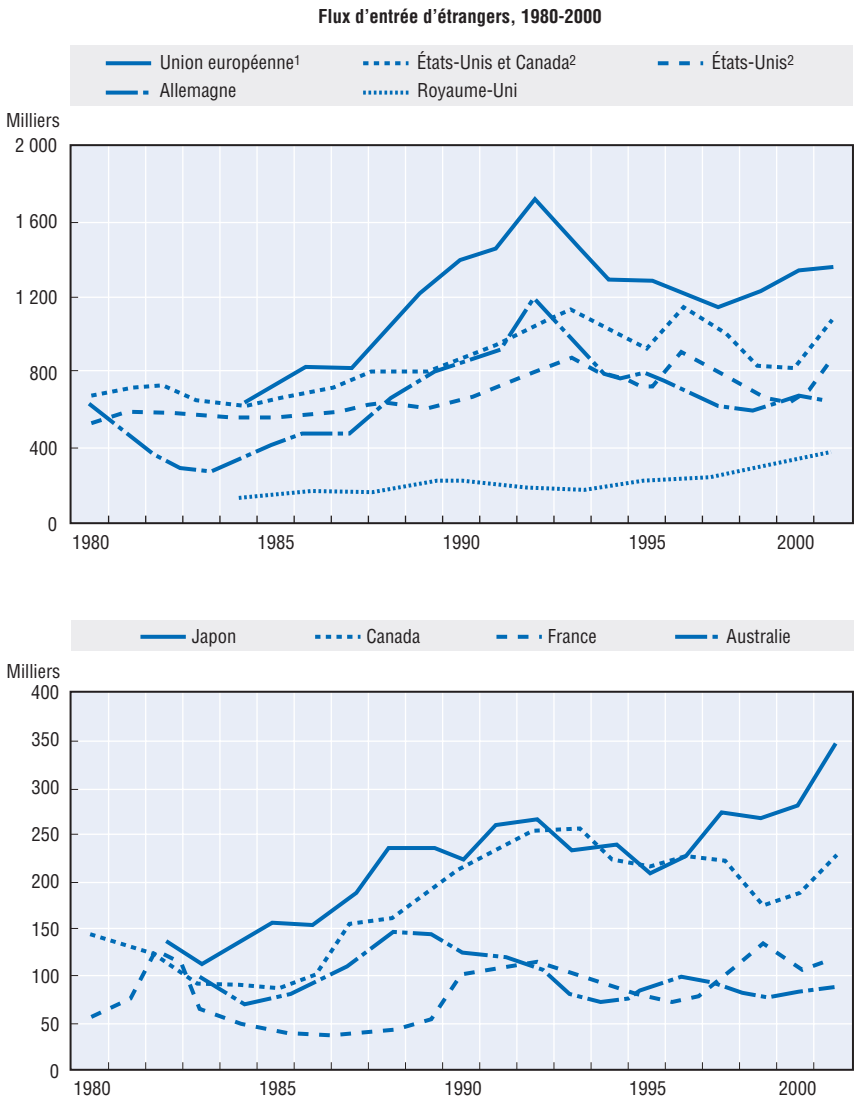


Source : Airbus.

augmenter au milieu des années 80, atteint un sommet au début des années 90, chuté ensuite, puis remonté de nouveau à la fin de cette même décennie (voir figure 5). Ce dernier renversement de tendance a confirmé le rôle croissant des migrations dans le contexte de la mondialisation économique. Au cours de la dernière décennie, l'évolution géopolitique, et notamment la plus grande liberté de mouvement des citoyens d'Europe centrale et orientale, a élargi le champ migratoire international, et un nombre croissant d'immigrants venus d'Asie, d'Afrique subsaharienne et d'Amérique centrale et latine sont venus gonfler les flux orientés vers plusieurs pays de l'OCDE. En 2000-2001, les flux entrants ont poursuivi leur progression, en particulier vers les États-Unis, le Canada, l'Australie, le Japon, le Royaume-Uni et l'Europe méridionale. Une bonne partie de ces mouvements sont motivés par des questions d'emploi et, notamment pour les flux de demandeurs d'asile, par un souci de regroupement familial. L'immigration illégale, aussi, a perduré.

L'existence d'un ensemble complexe de facteurs rend probable la permanence des pressions migratoires sur les pays de l'OCDE pour quelques décennies au moins : citons ainsi les écarts énormes des niveaux de vie et des taux de natalité entre les pays industrialisés et les pays en développement ; le vieillissement des populations et la diminution de la population active de maintes économies développées ; le coût relativement modéré des transports et des communications ; la présence de réseaux migratoires ; la dégradation de l'environnement, les guerres et les luttes civiques ; et, dans certains pays,

Figure 5. **Immigration dans certains pays de l'OCDE, 1980-2000**



Note : Les données relatives au Royaume-Uni sont tirées de l'*International Passenger Survey*. Pour l'Australie, le Canada et les États-Unis, elles concernent les nouveaux immigrants permanents ; pour la France et les pays de l'Europe méridionale, elles sont tirées des permis de séjour. Pour tous les autres pays, elles se fondent sur les registres de la population.

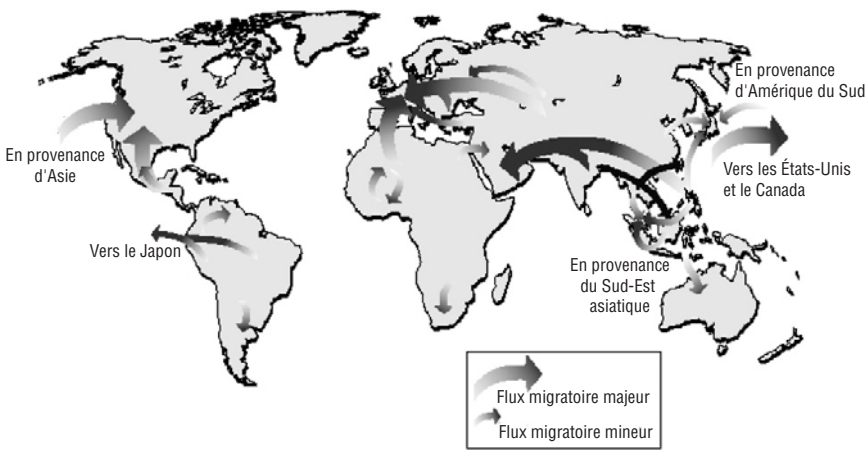
1. Allemagne, Belgique, Danemark, France, Luxembourg, Pays-Bas, Royaume-Uni et Suède.
2. Hors immigrants régularisés aux États-Unis dans le cadre du programme IRCA.

Source : OCDE, 2002.

l'effondrement de la gouvernance. Il n'est donc pas surprenant que différentes projections prévoient un afflux net dans les pays de l'OCDE d'environ deux millions d'immigrants par an, en moyenne, au cours de la première moitié du XXI^{e} siècle. Parmi les destinations les plus prisées se trouveront probablement les États-Unis (plus d'un million de personnes par an), l'Allemagne (173 000), le Canada (136 000) et l'Australie (83 000).

Étant donné ces perspectives de mobilité internationale globale, les pays se trouvent confrontés à la tâche colossale du maintien au cours des prochaines années de contrôles efficaces et efficients aux ports, aéroports et autres passages de frontière.

Figure 6. **Principaux schémas migratoires du début du XXI^{e} siècle**



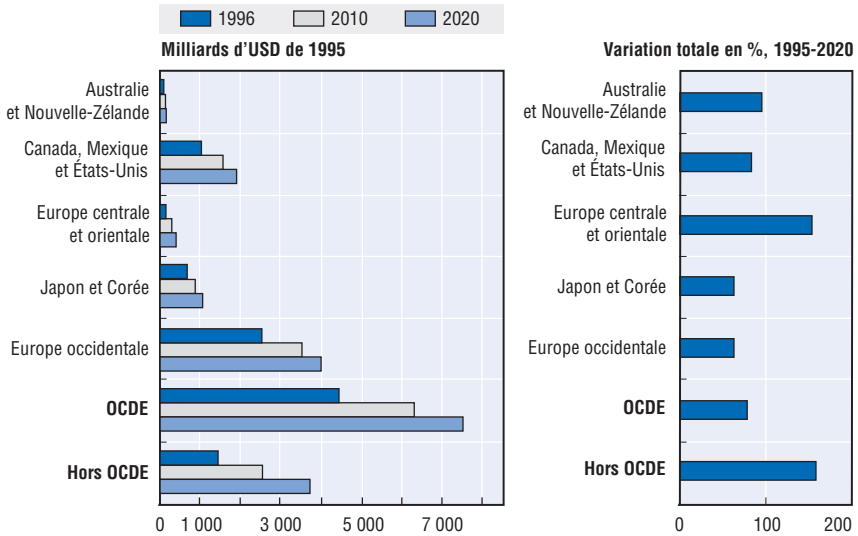
Source : Population Reference Bureau, *International Migration : Facing the Challenge*, mars 2002.

b) Mobilité des marchandises

Le commerce international constitue une indication intéressante de la mobilité croissante des marchandises. La hausse annuelle moyenne du commerce mondial a été de 4 % entre 1980 et 1993, puis de 8 % entre 1994 et 1996, progressant toujours plus vite que la production mondiale, avant de retomber un peu au tournant du siècle. Selon la plupart des prévisions, elle se poursuivra à ce rythme jusqu'en 2020, avec des exportations mondiales issues des pays hors OCDE progressant très probablement beaucoup plus vite que celles des pays de l'OCDE.

Certaines formes de transport de fret ont bénéficié plus que d'autres de l'expansion du commerce mondial. Le fret aérien, par exemple, a connu une

Figure 7. **Exportations mondiales, 1995-2020**



Source : Perspectives de l'emploi de l'OCDE, 2001.

croissance remarquable ces dernières décennies, et ses perspectives restent favorables. Les projections indiquent que le marché mondial du transport de marchandises par la voie aérienne pourrait aisément tripler entre 2001 et 2020. Une progression supérieure à la moyenne du fret aérien est attendue sur les trajets internes à l'Asie, entre l'Asie et l'Amérique du Nord, et entre l'Europe et l'Asie. Les autres moyens de transport du fret qui devraient fortement progresser d'ici 2020 sont le transport maritime et le transport par camions lourds.

La hausse remarquable du transport international observée ces dernières décennies est fortement liée au phénomène grandissant de l'internationalisation des systèmes de production. Les différentes étapes de l'activité économique – R-D, développement technologique, production, distribution, marketing, etc. – ont été de plus en plus intégrées à des chaînes de valeur mondiales qui se sont elles-mêmes fragmentées au gré de la différenciation des fonctions en activités toujours plus spécialisées. Plus récemment, les filières d'approvisionnement ont atteint de nouvelles zones du globe et intégré des activités productrices régionales jadis isolées. On constate par ailleurs une tendance croissante des entreprises, même lorsqu'il s'agit de grandes multinationales, à une spécialisation plus étroite et à l'externalisation d'un nombre croissant de fonctions auprès d'entités indépendantes sélectionnées sur la scène internationale pour tirer parti des écarts de prix et de logistique. Le résultat est

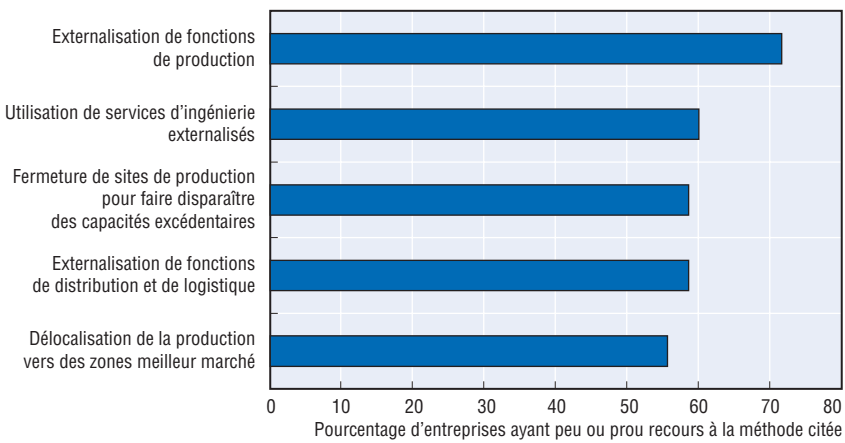
la création de filières mondiales d'approvisionnement qui sont de plus en plus dispersées, complexes et vulnérables aux perturbations, aux retards et aux actes criminels ou délinquants.

À titre d'illustration et en prenant l'exemple de deux économies ayant une frontière commune, on estime que les perturbations frontalières américano-canadiennes imputables aux activités terroristes pourraient concerner jusqu'à 45 % de l'ensemble des exportations du Canada, ainsi que 400 000 emplois et 2.5 milliards d'USD d'investissement.

La plupart des indices disponibles laissent à penser que les forces ayant créé ces chaînes de valeur mondiales fortement dispersées seront probablement nombreuses à perdurer. Les pressions qui s'exercent dans le sens d'une diminution des coûts des filières d'approvisionnement, de la conception des produits jusqu'à leur livraison, ne semblent pas faillir : les entreprises continueront d'être contraintes à délocaliser ou externaliser des segments de leur filière d'approvisionnement.

Par ailleurs, la recherche de nouveaux marchés étrangers mènera souvent à un étirement des chaînes d'approvisionnement lié à l'apparition de restrictions des échanges et à l'obligation de mettre en place une production locale ou un approvisionnement local pour pouvoir entrer sur un marché. Enfin, la pénétration de nouveaux marchés étrangers suppose que les filières proposent effectivement des produits adaptés au goût local, au moment voulu, avec les quantités et la qualité requises, et à un prix acceptable. L'accélération de l'innovation et le raccourcissement des cycles de vie

Figure 8. **Le resserrement des coûts des filières mondiales d'approvisionnement**



Source : Deloitte Touche LLP, 2003a.

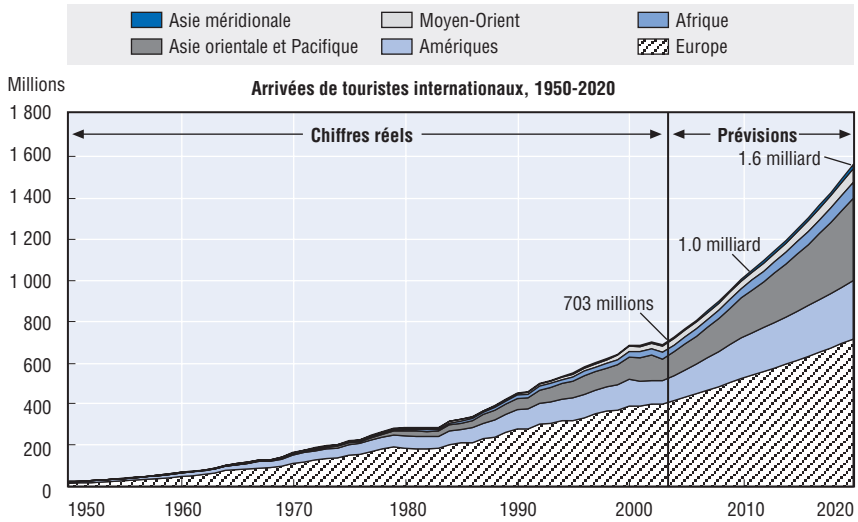
L'ÉCONOMIE DE LA SÉCURITÉ – ISBN 92-64-10773-8 – © OCDE 2004

des produits amplifient les exigences que subissent les filières d'approvisionnement. Partant, la sécurisation des réseaux mondiaux d'approvisionnement ne peut que devenir un enjeu majeur des entreprises au cours des années à venir.

4. L'efficacité opérationnelle

Au-delà même de la question de la sécurité, la plus forte concurrence et les attentes grandissantes des consommateurs, des citoyens et des entreprises aiguillonnent le besoin d'une efficacité accrue des opérations et procédures. Le renforcement des contrôles aux ports et dans les aéroports, par exemple, peut induire des retards perturbateurs et préjudiciables dans l'approvisionnement en produits essentiels ; et le passage massif de véhicules aux postes de douane peut provoquer des embouteillages monstres. Le passage de centaines de milliers de voyageurs aériens par des contrôles d'identité et de douane de plus en plus stricts coûte de l'argent et peut créer des retards importants. Le tourisme, à cet égard, est fort instructif pour l'avenir : comme le montre la figure 9, les arrivées mondiales de touristes internationaux devraient tripler entre 1995 et 2020 pour atteindre 1.6 milliard de personnes, avec une croissance bien plus forte des voyages au long cours que des voyages régionaux.

Figure 9. **Projections des arrivées de touristes internationaux jusqu'en 2020**



Source : Organisation mondiale du tourisme, *Tourism Highlights 2003*.

Comme nous l'avons vu dans la section ci-dessus, la mobilité connaît un essor important et les prochaines années devraient être le théâtre de hausses significatives des flux de personnes et de marchandises passant au travers d'installations publiques, de frontières, etc. Ainsi, la recherche de solutions rapides, efficientes et économiques rentables aux problèmes de cette sorte promet d'être un moteur important de l'émergence de technologies d'identification et de surveillance de pointe toujours plus innovantes.

5. Le besoin croissant de sécurité en matière d'information

L'une des évolutions les plus marquantes de ces dernières décennies a été la place stratégique qu'a prise l'information en tant que partie intégrante de la vie économique et sociale quotidienne. Cette importance grandissante de l'information s'est accompagnée d'un usage croissant du commerce électronique. Les entreprises se trouvent dès lors confrontées par millions aux menaces très coûteuses que représentent le vol d'informations (propriété intellectuelle, données clients, etc.), la fraude financière, ou tout simplement la perturbation des systèmes d'information par le biais de violations ciblées des sécurités mises en place ou de virus ou vers plus génériques. Des études périodiques (CSI/FBI, PWC/DTI, Deloitte, etc.) montrent qu'entre deux et trois cinquièmes des entreprises ont fait l'expérience ces deux dernières années de sérieuses violations de la sécurité de leurs informations, qui se sont souvent traduites par des pertes financières significatives.

Si la fréquence des attaques d'origine interne demeure non négligeable, celles issues d'Internet sont clairement à la hausse. Si l'on en croit des études mondiales, comme par exemple le *Symantec Internet Threat Report* (Rapport Symantec sur les menaces Internet), les entreprises de fourniture d'électricité et d'énergie et les prestataires de services financiers figurent parmi les entités les plus souvent ciblées. Les faits indiquent toutefois que le risque d'attaques via Internet et d'infection par des programmes malintentionnés reste élevé pour toutes les organisations connectées à Internet.

Différents facteurs vont probablement contribuer à la permanence de cette vulnérabilité au cours des prochaines années :

- Introduction de formes entièrement nouvelles et potentiellement plus destructrices de programmes malintentionnés et d'attaques par Internet.
- Prolifération de nouvelles applications Web dotées d'accès à distance relativement simples et faciles à exploiter.
- Usage de plus en plus répandu (souvent illicite) d'applications de messagerie instantanée et d'applications de poste à poste.
- Popularité croissante de périphériques itinérants dotés d'une connexion permanente et d'un accès distant à des données très sensibles.

Il est intéressant de remarquer que l'expansion des infrastructures des TIC semble contribuer à la vulnérabilité des systèmes d'information. Ces dernières années, la Corée, par exemple, a consacré avec succès des efforts de premier plan au développement d'une infrastructure haut débit au profit des consommateurs. Mais cette nouvelle accessibilité du haut débit renforce l'exposition aux activités malintentionnées. Ainsi, la Corée figure elle aussi parmi les pays connaissant la plus grande fréquence d'attaques (mesurée pour 10 000 internautes). Plusieurs pays d'Europe orientale à la population d'internautes en croissance rapide sont aussi en tête de la liste des pays « attaquants ».

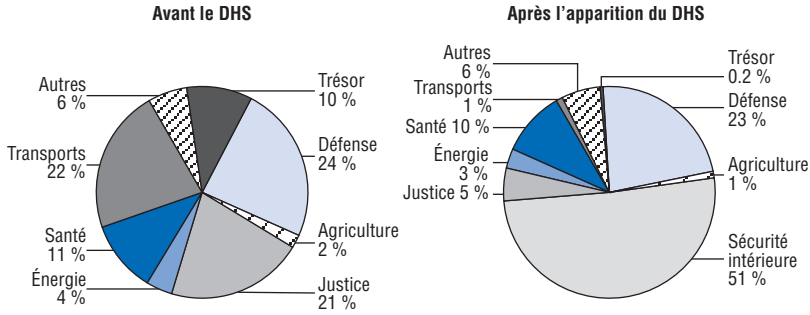
Ainsi, au moment où la vulnérabilité des systèmes d'information perdure et évolue, on peut s'attendre à une hausse de la demande de sécurité de l'information aussi bien en termes de sécurité physique et de contrôle des accès (biométrie, chiffrement des connexions) que de sécurité d'exploitation (pare-feu, logiciels antivirus, etc.).

6. Changements institutionnels et organisationnels

En raison de la prise en compte croissante des menaces pesant sur la sécurité, les réformes institutionnelles et organisationnelles qui ont été mises en œuvre ont – et continueront d'avoir – une incidence certaine sur le niveau et la structure de la demande de biens et services de sécurité. Sur toute la planète, des gouvernements ont réexaminé leur dispositif national d'indentification – depuis les procédures de délivrance jusqu'à la vérification de l'authenticité des documents par le truchement des services de police ou des douanes. Ainsi, de nombreuses installations et instances publiques ont commencé à resserrer les mailles de l'identification. Les pouvoirs publics ont étudié l'actualisation non seulement des passeports, mais aussi d'autres documents sécurisés tels que les visas, les cartes d'électeur, les permis de conduire et, bien entendu, les cartes d'identité.

Dans certains cas, l'examen de la situation a conduit à restructurer entièrement l'architecture institutionnelle. L'exemple peut-être le plus frappant de ce type d'évolution est la création aux États-Unis du ministère de la Sécurité intérieure (DHS) à la suite des attentats terroristes du 11 septembre 2001. Il a été créé par la fusion de 22 agences et programmes en un ministère de plein exercice doté notamment de quatre grandes directions : sécurité des frontières et des transports ; préparation et intervention d'urgence ; science et technologie ; analyse des informations et protection des infrastructures. La création du DHS a rassemblé au sein d'une seule entité la moitié des financements publics de la sécurité intérieure (soit 38 milliards d'USD environ). Le budget du DHS a augmenté des deux tiers entre les exercices 2002 et 2003, passant de plus de 11 à 19 milliards d'USD. La figure 10 ci-après

Figure 10. **Dépenses américaines publiques de sécurité intérieure**



Source : Report to Congress on Combating Terrorism, 2003.

illustre les répercussions de la création du DHS sur la répartition des financements de la sécurité intérieure entre les ministères concernés.

Une telle restructuration, aux conséquences budgétaires certaines, n'est pas limitée aux États-Unis. En Allemagne, par exemple, une nouvelle « stratégie » de protection de la population prévoit le regroupement des responsabilités fédérales en matière de gestion des catastrophes naturelles, des accidents industriels, des maladies infectieuses et du terrorisme international, ainsi que la création d'une nouvelle agence fédérale de protection civile et de gestion des catastrophes. Dans la même veine, la Norvège vient de créer une agence de gestion des urgences et de protection civile, dont le budget devrait croître de plus de 60 % entre 2003 et 2004.

Des modifications plus larges des législations nationales sont aussi fortement susceptibles d'avoir une incidence importante sur les dépenses de biens et services de sécurité. À titre d'illustration, l'Italie (voir le chapitre 5 du présent ouvrage) est en train d'introduire, avec un étalement sur cinq ans, une nouvelle carte d'identité nationale de haute sécurité ; et le ministre britannique de l'Intérieur a annoncé à l'automne 2003 un projet d'introduction de cartes d'identité obligatoires qui seront basées sur les caractéristiques biométriques du titulaire. En outre, un certain nombre de nouvelles initiatives de gouvernance font leur apparition ici et là sur la planète, dont on peut attendre un impact considérable sur la gestion de la sécurité dans les organismes publics et les entreprises. Dans le domaine financier, par exemple, des initiatives telles que l'Accord de Bâle et la Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA) renouvellent l'accent mis sur l'introduction de davantage de contrôles et sur la responsabilité des équipes dirigeantes du point de vue de l'intégrité et de la sincérité des informations financières qu'elles fournissent.

Enfin, le secteur privé lui-même connaît une évolution significative à la suite du resserrement des mesures de sécurité. Aux États-Unis, par exemple, on prévoit que les grandes entreprises privées auront dépensé entre 46 et 76 milliards d'USD en activités de sécurité intérieure au cours de l'exercice 2003. Certaines très grandes structures ont déjà créé une division interne de la sécurité intérieure afin de mieux cibler leurs efforts sécuritaires. Sur le front spécifique de l'information, les enquêtes menées à l'échelle mondiale soulignent quelques-uns des importants changements organisationnels qui sont en cours dans les multinationales. Depuis en particulier le milieu des années 90, les entreprises les plus en pointe ont commencé à rehausser de manière significative le niveau hiérarchique des responsables de la sécurité de l'information, de manière à leur donner plus d'autorité et d'accès. Aujourd'hui, l'organigramme de nombre de ces entreprises comporte un Directeur de la sécurité (*Chief Security Officer*) ou un Directeur de la sécurité de l'information (*Chief Information Security Officer*).

En conclusion, nous avons inventorié dans ce chapitre un certain nombre de facteurs économiques, sociaux et institutionnels qui ne manqueront pas de façonner la demande de sécurité dans les prochaines années. Bien entendu, d'autres facteurs – et notamment l'évolution technologique des offres du secteur de la sécurité, la rapidité de la chute des prix des technologies nouvelles et les plus en pointe, et bien sûr leur acceptation par le grand public – influeront sur l'évolution effective de ces perspectives. Ces thèmes seront abordés dans les chapitres suivants.

Bibliographie

AIRBUS (2002), *Global Market Forecast 2001-2020*, Blagnac.

ATKINSON, Giles, Susana MOURATO et Andrew HEALEY (2003), « The Cost of Violent Crime », *World Economics*, vol. 4, n° 4, octobre-décembre.

BANQUE MONDIALE (2003), *Global Economic Prospects 2004*, Washington, DC.

BOEING (2002), *World Air Cargo Forecast 2002/2003*, Seattle.

CNUCED (2002), *World Investment Report 2002: Transnational Corporations and Export Competitiveness: Overview*, Genève.

COMPUTER SECURITY INSTITUTE/FEDERAL BUREAU OF INVESTIGATION (2003), *Computer Crime and Security Survey*, San Francisco.

CONFEDERATION OF EUROPEAN SECURITY SERVICES (2003), *Annual Report 2003*, Wemmel, 20 octobre.

CONSEIL DE L'EUROPE (2002), *Rapport 2001 sur la situation de la criminalité organisée*, Strasbourg.

DELOITTE, TOUCHE et TOHMATSU (2003), *2003 Global Security Survey,* New York, mai.

DELOITTE, TOUCHE LLP (2003a), *The Challenge of Complexity in Global Manufacturing: Critical Trends in Supply Chain Management*, Londres.

DELOITTE, TOUCHE LLP (2003b), *Mastering Complexity in Global Manufacturing: Powering Profit and Growth through Value Chain Synchronization*, Londres.

EUROPOL (2002), *2000 European Union Organised Crime Situation*, La Haye.

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES (2002), *Budget for Fiscal Year 2003*, Washington, DC.

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES (2003a), *Budget for Fiscal Year 2004,* Washington, DC.

EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES (2003b), Report to Congress on Combating Terrorism, Washington, DC.

FEDERAL BUREAU OF INVESTIGATION (2002), *Crime in the United States – 2002*, Washington, DC.

INTERPOL (2003), Statistiques sur la criminalité dans quelques pays, 1995 et 2002.

J.P. FREEMAN REPORTS (2003), *US and Worldwide CCTV and Digital Video Surveillance Market Report*, J.P. Freeman & Co., Newtown, CT.

LAMBLIN, Véronique (2003), « Le développement des résidences sécurisées », *Futuribles*, n° 291, novembre.

LLOYD, Carolyn (2003), « Is Secure Trade Replacing Free Trade? » dans John M. Curtis et Dan Ciurak (dir.), *Trade Policy Research,* ministère des Travaux publics et Services gouvernementaux, Canada.

MINISTÈRE BRITANNIQUE DE L'INTÉRIEUR (2001), *British Crime Survey 2001*, Londres.

MINISTÈRE DES FINANCES DU CANADA (2001), *Le budget en bref 2001*, Ottawa.

MINISTÈRE DES FINANCES DU CANADA (2003), *Le budget en bref 2003*, Ottawa.

MINISTÈRE DES TRANSPORTS DES ÉTATS-UNIS (2000), *Criminal Acts against Aviation Report*, Washington, DC.

MINISTÈRE FÉDÉRAL ALLEMAND DES FINANCES (2002), *Finanzplan des Bundes 2002-2006*, Berlin.

MINISTÈRE FÉDÉRAL ALLEMAND DES FINANCES (2003), *Finanzplan des Bundes 2003-2007,* Berlin.

OCDE (2001), *Perspectives de l'environnement de l'OCDE*, OCDE, Paris.

OCDE (2002), *Tendances des migrations internationales 2001*, OCDE, Paris.

OCDE (2003), *Les risques émergents au XXI^e siècle*, OCDE, Paris.

ONU, DIVISION DE LA POPULATION (2002), *International Migration Report 2002*, New York.

ONU, DIVISION DE LA POPULATION (2003), *World Population Prospects : The 2002 Revision : Highlights*, New York, février.

ORGANISATION INTERNATIONALE DES MIGRATIONS (2003), « Faits et chiffres de la migration internationale », *Questions de politique migratoire*, n° 2, mars.

ORGANISATION MONDIALE DU TOURISME (2003), *Tourism Highlights 2003,* Madrid.

POPULATION REFERENCE BUREAU (2002), « International Migration: Facing the Challenge », *Population Bulletin*, 57:1, mars.

PRICEWATERHOUSECOOPERS (2002), *Information Security Breaches Survey 2002: Technical Report*, ministère du Commerce et de l'Industrie, Londres.

RANSTORP, M. (2003), Déposition devant la Commission nationale sur les attentats terroristes commis à l'encontre des États-Unis (*National Commission on Terrorist Attacks Upon the United States*), 31 mars.

RUTTENBUR, Brian (2002), « Biometrics and Security Update », *NextInnovator,* 25 novembre, *http://technologyreports.net*.

SECURITY INDUSTRY ASSOCIATION, statistiques sectorielles variées.

Smart Labels Analyst (2003), « RFID in Asia », Numéro 32, septembre.

SYMANTEC (2003), « Internet Security Threat Report », Symantec, Cupertino, CA, février.

SYNDICAT NATIONAL DES ENTREPRISES DE SÉCURITÉ, statistiques variées.

The Economist (2003), « Crime in Japan », 25 octobre.

UK NATIONAL CRIMINAL INTELLIGENCE SERVICE (Service de renseignement national britannique sur la criminalité) (2003), *United Kingdom Threat Assessment of Serious and Organised Crime 2003*, Londres.

UNION FÉDÉRALE DES ENTREPRISES DE SURVEILLANCE ET DE SÉCURITÉ ALLEMANDES, statistiques variées.

US CONFERENCE OF MAYORS (Conférence américaine des maires) (2003), *First Mayors' report to the nation: Tracking Federal Homeland Security Funds – Sent to the 50 State Governments*, septembre.

WILKINSON, Paul, « *Observations on the New Terrorism* », déposition devant la Commission britannique des affaires étrangères, juin.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 3

Biométries

par

Bernard Didier
Technical and Business Development
SAGEM SA
FRANCE

1. Brève introduction à la biométrie

« Sésame ouvre-toi… »

Toute la magie et la faiblesse de la reconnaissance sont contenues dans cette petite phrase de ce conte oriental. Reconnaître, identifier, authentifier sont des besoins qui remontent à la nuit des temps.

Les Chinois authentifiaient des actes de propriétés par empreintes digitales. Les potiers égyptiens savaient que leurs empreintes marquées dans la glaise permettaient de reconnaître leur production. L'épistémologie est friande d'inventions retrouvées : il faudra attendre la seconde partie du XIX^{e} siècle pour trouver enfin une réflexion biométrique construite avec la démarche de William Herschel qui eu l'idée, au Bengale en 1858, de sécuriser des engagements contractuels par l'impression d'empreintes palmaires. C'est ainsi que naquit la technique d'identification la plus connue et sans conteste la plus démontrée et la plus éprouvée : l'identification par empreinte digitale. Il fut suivi quelques temps après, en 1883, par Alphonse Bertillon qui introduisit les techniques anthropométriques pour identifier des criminels récidivistes. Cette même année, la technique d'identification par empreinte digitale était récupérée dans un roman « The life of the Mississipi » écrit par un certain Langhorne Clemens plus connu sous son nom de plume de Mark Twain.

Avec la conquête de l'Ouest, et l'essor du télégraphe, on découvrit que les télégraphistes avaient un « doigté » caractéristique qui permettait de les reconnaître. Cette technique fut communément utilisée pendant la dernière guerre mondiale pour authentifier les opérateurs de radiotélégraphie. C'est dans le milieu des années soixante, alors même que l'identification de criminels récidivistes à l'aide d'empreintes digitales était reconnue et utilisée depuis plusieurs décennies par l'ensemble des polices du monde, qu'enfin le FBI lançait un vaste programme de recherche sur le traitement automatique des empreintes digitales. C'est aussi à la même époque que l'université de Standford démontrait qu'il était possible de « discriminer » une population d'environ 5 000 personnes grâce à la mesure de la longueur des doigts d'une main. Cette technique biométrique fut utilisée expérimentalement pour contrôler l'accès aux salles d'examen. Cela donna naissance au premier système de contrôle d'accès biométrique connu sous le nom d'Identimat. Cette première avancée ouvrit ensuite de nombreux axes de recherches pour améliorer une technique quelque peu balbutiante.

Quelques définitions et conséquences

Les traitements biométriques ont pour objectifs fondamentaux d'« identifier » ou d'« authentifier » des personnes.

Identifier

Par identifier il faut comprendre : toute approche qui permet de décrire chaque personne d'une population connue de manière unique de telle sorte qu'il soit toujours possible de démontrer qu'une personne donnée est identique, ou non, à une des personnes de la population connue. Cette définition appelle plusieurs commentaires :

- La recherche d'une description, pour chaque personne, unique et immuable est le principe fondamental qui régit la construction d'une technique biométrique.
- L'unicité de la description sera d'autant plus difficile à construire que la population concernée – qui peut dépasser la population connue *a priori*[1] – sera importante. Il est facile de gérer l'identité d'une dizaine de personnes en utilisant quelques critères physiques élémentaires (couleur des cheveux, des yeux, sexe, taille…), ces critères sont notablement insuffisants pour gérer la population d'un État. On perçoit, intuitivement, qu'une description trop sommaire fera apparaître des homonymes – personnes reconnues à tort – et qu'une description trop détaillée, si elle ne respecte pas strictement le principe d'immuabilité, risquera d'entraîner des non-identifications – personnes non reconnues à tort.
- L'identification est un processus qui revient à comparer la description unique d'une personne à toutes les descriptions connues de la population et de décider laquelle est identique. Cette comparaison d'une personne à toutes les autres personnes est encore appelée comparaison UN à N (noté encore 1 : n).

Authentifier

Par authentifier il faut comprendre : toute approche qui permet à un tiers de confiance de décrire une personne de telle sorte qu'il soit possible ultérieurement de vérifier qu'une personne est conforme à sa description authentique. Plusieurs commentaires :

- La notion de tiers de confiance, bien que peu explicite est très prégnante dans l'acte d'authentification. La qualité de l'authentification reposera sur ce tiers de confiance[2].
- La description d'authentification peut être mémorisée soit dans des fichiers, et dans ce cas la personne à authentifier devra donner des informations permettant de retrouver cette information pour procéder à la

vérification, soit dans un support (carte à mémoire par exemple, passeport…) que possède la personne à authentifier. Dans ce dernier cas, l'authentification n'implique pas nécessairement, contrairement à l'identification, de construire un fichier de description de personnes.

- L'authentification ne met pas en jeu l'identité de l'individu, la description est conforme ou non. Néanmoins la qualité d'une authentification dépend de l'existence préalable d'une fonction d'identification : en effet, la délivrance de plusieurs moyens d'authentification à une même personne, et ce sous des identifications différentes, introduit une faille de sécurité.
- L'authentification consiste à vérifier qu'une description d'une personne est identique à la description authentique ou préalable associée à cette personne. Cette opération de comparaison d'une description à une autre s'appelle comparaison UN à UN (noté 1 :1).

Identifier, authentifier : deux approches complémentaires

D'une manière générale, la sécurité des systèmes repose sur l'usage judicieusement combiné de ces deux fonctions. L'identification servira, lors de la délivrance d'un droit, à vérifier que le demandeur ne fait pas l'objet d'interdit et qu'il n'existe pas déjà, dans le système, sous un autre nom. C'est à cette étape que sera aussi créée l'information biométrique de référence (template) qui servira à authentifier ultérieurement le demandeur lors de l'usage du droit. C'est grâce à cette approche globale qu'il est possible d'éviter la délivrance de vrais droits à partir de demandes reposant sur de fausses identités.

Toutes les techniques biométriques offrent des fonctions d'authentification ; il n'en est pas de même en matière d'identification. Seules les techniques qui reposent fondamentalement sur des informations biométriques uniques pour chaque personne peuvent envisager de remplir correctement cette fonction. Historiquement l'empreinte est la première technique permettant à la fois d'identifier et d'authentifier et ayant de plus une force légale. Dans l'état actuel de nos connaissances, à part l'iris et l'ADN, il n'existe pas d'autres techniques pouvant prétendre remplir efficacement une fonction d'authentification.

La voix de son maître… ou au doigt et à l'œil

Quels critères physiques permettent d'authentifier une personne ? Sur ce sujet l'imagination est débridée et le petit monde de la biométrie frémit régulièrement, sensible à des effets de mode où la nouveauté l'emporte malheureusement trop souvent sur la qualité. On classe généralement les critères physiques retenus en deux grandes catégories : les approches par apprentissage et les approches anatomiques.

Les techniques par apprentissage authentifient les personnes sur leur capacité à reproduire, de manière stable, certains mouvements musculaires. Sont rattachées à cette classe, par exemple : la reconnaissance dynamique des signatures, la reconnaissance vocale, l'authentification par la frappe sur un clavier. Ces techniques, comme leur définition le sous-tend, ont une fragilité dans le temps.

Les techniques anatomiques reposent sur le traitement de critères physiques réputés immuables et uniques pour chaque individu. Les représentants les plus significatifs de cette classe sont : l'empreinte digitale, l'ADN, l'iris, la forme de l'oreille ou encore les circuits veineux de la main. Est aussi rattachée à cette classe la reconnaissance du visage. Ces critères ont intrinsèquement peu de variation dans le temps, en tout cas pour les premiers cités. Les variations constatées sont très souvent dues à des artéfacts des systèmes d'acquisitions d'informations.

L'appréciation des performances des systèmes biométriques

Remarque liminaire

Il conviendrait d'aborder l'appréciation des performances sous l'angle d'une analyse systémique qui tienne compte des performances de la fonction globale de sécurité. À cet égard, il est possible de distinguer les performances de sécurité extrinsèques au choix de la technologie biométrique (élément de sécurité physique – difficultés physiques à casser le système – et logique – usage de technique cryptographique) de celles qui sont intrinsèques, telles que notamment les taux d'erreurs ou encore la capacité à reproduire artificiellement l'élément biométrique. Cette approche globale, encore appelée « Politique de profil de protection », sur laquelle l'administration française à une position peu lisible, mérite une attention particulière. Dans un premier temps, l'analyse sera réduite à la mesure des erreurs.

La défaillance à l'enregistrement ou FTE (Failure To Enroll)

Le FTE est le pourcentage de la population impossible à enregistrer. Toutes les biométries ont des difficultés sur certaines classes de population. Par exemple l'empreinte aura des problèmes avec des travailleurs manuels, l'iris avec les iris très clairs (pays nordiques) ou très sombres (certaines ethnies africaines), le visage aura aussi des difficultés à traiter certaines ethnies (*cf.* les erreurs sur les visages de Japonais lors de la démonstration officielle du système pilote de contrôle aux frontières australien). Le pourcentage est variable selon les stratégies retenues, on peut décider d'enregistrer coûte que coûte, mais alors on déplace le problème vers des erreurs en identification ou authentification[3]. Pour l'empreinte et l'iris, ce taux peut varier de 1 à 2 % pour les fournisseurs les plus performants.

Le taux de fausses comparaisons ou FMR (False Match Rate)

Le FMR est le pourcentage d'individus déclarés identiques à tort lors d'une opération d'identification ou d'authentification. La conséquence dépend de l'usage. Dans une opération de contrôle d'accès, on aura autorisé un accès à tort. Dans une opération de type « Watch List », cela se traduira par une fausse identification avec un individu recherché (rejet à tort). Dans une opération de détection d'enregistrement multiple, on rejettera encore à tort le demandeur.

Il est important de comprendre que les deux taux précédents sont corrélés : si on règle un système pour détecter tous les fraudeurs alors on arrêtera beaucoup plus de personnes à tort[4].

Le taux de fausse « non-identification » ou FNMR (False Non Match Rate)

Le FNMR est le pourcentage d'individus qui sont déclarés différents à tort. On transposera sans peine les conséquences de telles erreurs en fonction de l'usage.

Les précisions de différentes techniques biométriques

Pour une même technologie les performances peuvent varier de façon très significative entre différents fournisseurs.

En matière d'authentification, les différentes sources indépendantes des industriels convergent vers la situation moyenne représentée dans le tableau ci-contre :

Tableau 1.

	Visage	Empreinte	Iris
FTE	0-5 %	0-1 %	0-3 %
FMR (FAR)	1.0 %	0.1 %	> 0 %
FNMR (FRR)	10-40 %	0.5-1 %	2-3 %

Sources : US DOD, DARPA, NIJ, CESG (UK), Bologna Univeristy, US National Biometric Test Center, Isareli Based Project, et différents benchmarks.

Ces valeurs moyennes permettent d'éclairer des choix sur des petites opérations de contrôle d'accès par exemple, mais il serait extrêmement dangereux d'extrapoler ces valeurs et d'en tirer des conclusions lorsqu'il s'agit de mettre en place des systèmes touchant la sécurité des États et traitant quelques dizaines de millions de personnes. Dans ce cas, le pourcentage, même faible, de résultat nécessitant une validation manuelle peut devenir très vite rédhibitoire.

2. Éléments de segmentation : les différents usages de la biométrie

Une segmentation difficile

La biométrie ne se résume pas à une activité industrielle monolithique. Une bonne segmentation des marchés, des produits et des acteurs est le préalable à toute analyse de ce secteur d'activité. Certaines études de marché sur la biométrie ont péché, dans le passé, par un manque de rigueur en matière de définition des segments d'activités et ont abouti à des prévisions de chiffres d'affaires quelque peu surprenantes.

Certes, ce marché est dur à appréhender car on ne dispose que de très peu d'informations publiques et il y a pléthore d'acteurs. Mais élément plus fondamental, avec l'évolution des marchés, la chaîne de valeur de ce secteur s'est complexifiée. Au début des années 80, il n'existait que deux grandes classes d'acteurs : ceux qui fabriquaient des boîtiers de contrôle d'accès biométriques autour d'un système de contrôle d'accès relativement rustique et ceux qui fabriquaient des systèmes d'empreintes digitales pour le marché policier. La décennie 1990 a vu se dessiner une oscillation entre « horizontalisation » et « verticalisation » des acteurs industriels :

- Avec notamment des acteurs qui ont essayé de n'adresser que le sous-segment des capteurs biométriques – notamment en matière de traitement d'empreintes digitales.
- Une première classe d'acteurs s'est plus particulièrement intéressée aux capteurs policiers (Booking Station) qui accompagnaient l'évolution des systèmes policiers vers la suppression des techniques encrées et la tendance du bureau « sans papier ». Certains de ces acteurs ont fait évoluer leur offre vers des sous-systèmes d'acquisition voire vers des fonctions de service bureau de contrôle d'identité (Background Check). Vu les exigences de qualité demandées, ce secteur malgré une croissance réelle amplifiée par les événements du 11 septembre 2001, ne connaît que très peu d'acteurs.
- Une deuxième classe d'acteurs est issue de l'industrie des composants électroniques (Infineon, ST Microelectronics, Atmel notamment) et propose des capteurs à très faibles coûts adressant le marché de la sécurisation des ordinateurs portables, des PDA ou encore des téléphones mobiles. La lenteur de la montée en puissance de ces marchés a incité ces acteurs, soit à se retirer, soit à se verticaliser sur des solutions de contrôle d'accès logiques ou physiques en attendant des jours meilleurs.
- L'apparition de sociétés de Middleware, soit de technologie pure comme East Shore Technologie, soit de solutions de biométries multi-modales comme par exemple I/O Software ou Keyware.
- En cohérence avec la tendance Middleware, l'évolution des boîtiers biométriques vers des interfaçages compatibles avec les systèmes

industriels de contrôle d'accès ou de gestion du temps au détriment de solutions propriétaires. Dans le même ordre d'idée, il apparaît des solutions de plus en plus intégrées (Daon ou encore Activcard par exemple) avec les produits génériques du marché (gestion de documents, ERP, PKI…).

- L'apparition de gros intégrateurs offrant des systèmes complexes ou des services de gestion de titres institutionnels dans lesquels la biométrie devient une commodité au même titre qu'une carte à puce.

Cette complexité de la chaîne de valeur rend particulièrement difficile l'analyse économique de l'évolution du marché de la biométrie entre revenus directs et revenus indirects.

Il serait nécessaire que les différentes associations fédérant les industriels de la biométrie conduisent un effort permanent en matière de lisibilité financière de l'activité de l'industrie biométrique.

Dans le contexte actuel d'interrogation sur les nouvelles technologies, c'est un préalable de plus en plus nécessaire pour que ce secteur naissant d'activité se développe et acquiert une crédibilité auprès des acteurs financiers et des clients potentiels.

L'usage à des fins de lutte contre la criminalité : le marché policier

Ces systèmes sont plus connus sous l'acronyme AFIS (Automatic Fingerprint Identification Systems). Ces systèmes policiers permettent d'identifier des personnes à partir du relevé des empreintes des dix doigts, mais se distinguent surtout des autres systèmes institutionnels ou civils, par leur capacité à identifier des traces parcellaires d'empreintes digitales, souvent de mauvaise qualité, laissées sur les scènes de crimes.

Travaux de recherches conduits initialement à la demande du FBI, aux alentours des années 70, par Calspan Autonetics et Rockwell, notamment, ces systèmes ont véritablement attendu une dizaine d'années avant d'obtenir la confiance de la communauté policière aux États-Unis. À l'origine, les techniques de police scientifiques d'identifications automatiques de personnes n'étaient pas rattachées à la biométrie. La biométrie recouvrait plutôt un usage civil de contrôle d'accès. Il faut attendre la fin du siècle dernier, avec l'usage de plus en plus fréquent de systèmes AFIS à des fins de gestion civile de titres d'identités pour que la biométrie recouvre aussi l'usage de grands systèmes d'identifications.

Aujourd'hui, la quasi-totalité des polices modernes en est équipée.

Sur le plan technique, ces systèmes sont capables de gérer quelques milliers d'identifications par jour sur des bases de données de quelques millions de personnes, voire quelques dizaines de millions. Le dernier système dont s'est doté le FBI au milieu des années 90 avec environ

40 000 recherches par jour sur une population de 40 millions de personnes est le plus puissant du monde.

Sur le plan industriel, ces systèmes sont fournis par des sociétés qui commercialisent, installent et développent ces AFIS. Il existe trois acteurs historiques NEC (Japon), Printrak racheté récemment par Motorola (USA), Sagem (France) et un acteur plus récent Cogent (USA). Sagem, tant par son chiffre d'affaires[5] que par ses références, notamment celles du FBI et d'Interpol, est le leader mondial[6] de ce segment de marché.

Sur le plan économique, ces systèmes ont représenté probablement les investissements continus les plus importants, sur ces 20 dernières années, des services de police en matière de traitement de l'information (hors télécommunications). La mise en place de tels systèmes a permis d'augmenter le pourcentage de crimes résolus par un facteur multiplicatif de 5 à 10 ! avec vraisemblablement des effets induits – non analysés – sur la valorisation immobilière. C'est un segment de marché mature, essentiellement de renouvellement, d'environ 150 à 200 millions de dollars par an.

À ce segment il convient d'inclure les fabricants de capteurs biométriques policiers (Booking Stations). Ces équipements sont vendus, soit dans le cadre des systèmes précédemment cités, soit dans le cadre d'offres séparées. Le revenu de ces sociétés s'élevait à 100 millions de dollars en 2001, partagé entre le leader Identix (après la fusion avec Visionics DBII), CrossMatch et Heimann Biometric Systems.

Les systèmes biométriques institutionnels

C'est le segment de marché de la gestion de la délivrance et de l'usage de droits institutionnels tels que les cartes d'identité, les pensions, la sécurité sociale, les passeports et visas etc. Cette demande du marché est relativement récente et date des années 1992/1993. L'objectif est double : s'assurer que l'on ne délivrera pas plusieurs fois le même droit à une même personne, ou à une personne interdite, et contrôler l'authenticité du demandeur lors de l'usage d'un droit. Aujourd'hui ce sont essentiellement des systèmes de traitement automatique d'empreintes digitales qui sont utilisés.

Sur le plan technique, l'AFIS n'est qu'un des éléments d'une solution plus complexe, reposant sur la fabrication de titres sécurisés permettant un contrôle ultérieur du détenteur par analyse d'empreintes digitales et englobant parfois la gestion d'un état civil. Ces systèmes portent sur des populations plus importantes que celles des systèmes de lutte contre la criminalité, et se caractérisent par des demandes d'identification élevées, quelques dizaines de milliers, sur des bases de données de plusieurs dizaines de millions de personnes. L'importance des flux à gérer nécessite des

architectures différentes et plus complexes que des AFIS à usage policier. L'identification de traces disparaît au profit plus systématique de l'authentification.

Sur le plan industriel, les réponses aux appels d'offres des Etats se font au moyen de Consortiums conduits par des intégrateurs (TRW, LMC, Unisys, Siemens, IBM…), auprès desquels on trouve les traditionnels fabricants d'AFIS (Motorola, Nec, Sagem et Cogent) et des fabricants de titres (Polaroid, Gemplus, Oberthur, Giesecke et Devrient…). Sur ce marché, Sagem a remporté la majorité des appels d'offres, soit comme fabricant d'AFIS, soit dans un certain nombre de cas récents en offrant une prestation complète d'intégrateur, de fabricant d'AFIS et de production de titres sécurisés.

C'est un segment de marché en développement, d'environ 50 à 100 millions de dollars par an, avec des cycles de décisions longs (plus de trois ans). On peut estimer que sur les dix dernières années, l'ensemble des contrats signés a concerné près de 275 millions de personnes[7]. Les grands projets d'état civil ou de cartes d'identité se sont développés plutôt en Asie, au Moyen-Orient et en Afrique. L'Europe a utilisé cette approche essentiellement pour la gestion des droits d'asile (EURODAC) et les États-Unis sur quelques applications de délivrance de droits sociaux. Depuis les événements du 11 septembre, ce segment de marché fait l'objet de beaucoup d'agitations avec l'annonce des futurs passeports et visas biométriques complétée par un mouvement encore incertain sur les titres d'identités biométriques (aux USA avec les États de Georgie et d'Oklahoma, « Entitlement Card » en Grande-Bretagne, le titre fondateur en France…). Conséquence de cette tendance : le marché des « booking stations » institutionnelles, dérivé du marché policier, est en train de voir le jour, se développe rapidement avec une réduction notable attendue des coûts de ces équipements.

Depuis peu, avec les exigences de contrôle d'identité préalable à l'obtention d'une autorisation de travail sur des activités sensibles (aéroport, transport de fonds…), certains États américains ont favorisé l'apparition d'une offre de service.

Ce segment de marché est généralement structurant : un État qui se dote d'un titre sécurisé par une technique biométrique, favorisera l'usage de ce titre à d'autres fins que le seul contrôle de l'usage du droit (concept du titre fondateur). C'est par exemple le cas de la Malaisie avec le projet GMPC (General Multipurpose Card) qui se propose de gérer le permis de conduire, le passage aux frontières et un porte-monnaie électronique, le tout dans une seule carte sécurisée par empreinte digitale ou encore du projet de cartes d'identité multi-applicative des Émirats Arabes unis.

Les systèmes biométriques à usages commerciaux et industriels

Premiers prototypes dans le milieu des années 70, et premiers produits commerciaux offerts sur le marché au début des années 80, ces terminaux se sont adressés, dans un premier temps, à des marchés de contrôle d'accès et/ou de gestion du temps, avec pour clients des structures gouvernementales (prisons par exemple), et plus rarement des sociétés commerciales et industrielles. Dans ce dernier cas, les applications de « Back End » prennent le pas sur les applications de « Front End ». À noter, depuis maintenant deux à trois ans, l'apparition de solutions de services de sécurisations biométriques de transactions commerciales aux États-Unis avec notamment Biopay (Check Cashing), BAC et Indivos.

Sur le plan technique, les technologies historiques d'empreintes et de mesure de la longueur des doigts sont les plus utilisées. Récemment sont venues se rajouter la reconnaissance faciale et la reconnaissance de l'iris. Les solutions proposées peuvent aller du boîtier biométrique connectable à un PC accompagné d'un logiciel de traitement et, dans ce cas, c'est plutôt l'empreinte digitale qui est utilisée, jusqu'au boîtier de contrôle d'accès remplissant des fonctions d'authentification et plus rarement d'identification. Dans ce dernier cas, la comparaison s'effectue sur des empreintes digitales (quelques milliers d'empreintes).

Sur le plan industriel, les ventes sont souvent réalisées par des intégrateurs, des distributeurs ou des sociétés spécialisées sur des segments verticaux de marché (le transport, la santé…). Les équipements sont conçus par une myriade (plus de 200 début 2001) de petites sociétés, plus ou moins solides, et n'ayant que rarement des capacités de production et d'évaluation de performance de leur technologie. Les années 1998-2001 ont vu un début de consolidation[8] avec l'acquisition notamment d'Indenticator par Identix pour 43 millions de dollars, les difficultés de Veridicom (société ayant pourtant réuni quelques actionnaires significatifs comme Intel, ATT et Lucent Technologies) et d'Ethentica (avec des actionnaires tels que Citibank et Phillips Electronics) ne devant son salut que par l'injection de 40 millions de dollars et l'arrivée d'HP et Amdhal dans son capital. Cette consolidation devrait se poursuivre pour aboutir probablement à une dizaine d'acteurs, aucun « pure player » sur ce segment de marché ne gagnant de l'argent.

Les acteurs historiques sont Identix, Bioscrypt, STmicroelectronics pour le traitement des empreintes digitales, Iridian pour la reconnaissance de l'iris, Cognitec, Visionics, Viisage pour la reconnaissance du visage. Depuis maintenant deux ans, Sagem a commencé à entrer sur ce marché en proposant des technologies éprouvées dans le milieu de la lutte contre la criminalité et difficilement accessibles aux sociétés traditionnelles de ce segment de marché et a obtenu très rapidement quelques références

mondiales significatives (Postes d'inspections filtrages des Aéroports de Paris notamment). En 2003, Sagem a étoffé son offre en proposant des solutions de reconnaissance de l'iris et du visage originales dans le cadre d'accords stratégiques signés avec Iridian et Cognitec.

C'est un segment de marché encore naissant malgré son âge, mais en développement rapide. Au sous-segment traditionnel du contrôle d'accès et de la gestion du temps, vient s'ajouter depuis peu une demande en matière de contrôle d'accès logique (PC, transactions sur Internet et intranet..) et devrait être suivie par une demande en équipement personnel (PDA, téléphone).

Le marché des terminaux biométriques fait l'objet d'analyses de marché quelque peu divergentes. Selon les sources[9, 10, 11, 12], il est évalué entre 66 et 196 millions de dollars pour 2000, toutes technologies confondues. Si on retient, comme c'est les cas pour les systèmes de contrôle d'accès – mais pas pour le marché des PC et des PDA –, que les capteurs biométriques ne représentent que 10 % du prix de ventes des systèmes, alors les boîtiers biométriques génèrent probablement un revenu indirect supérieur à 1 milliard de dollars.

Par contre, il existe un consensus pour reconnaître que la technique d'analyse par empreinte digitale est la plus fréquemment retenue par le marché. Une majorité d'analystes estime qu'avec une part de marché évaluée entre 37 % et 55 % et une croissance d'au moins 40 % par an, l'empreinte digitale est la technologie la plus prometteuse en matière de produits biométriques.

Les systèmes biométriques à usage personnel

Ce segment est encore balbutiant, l'année 2003 a vu la confirmation des PC portables sécurisés par empreinte digitale (Samsung notamment), l'apparition significative des premiers téléphones mobiles à empreintes digitales au Japon (Futjisu) et des premiers PDA (HP-Compact).

Ce marché est un marché plus de confort que de sécurité. Il reste l'apanage de fabricants de capteurs (STmicroelectronics, Infineon, Atmel). C'est essentiellement un marché de vente de composants.

Le constat

D'un point de vue pratique, aujourd'hui, ce sont les systèmes de traitement automatique d'empreintes digitales qui sont les plus souvent utilisés au travers de nombreuses applications. La biométrie par empreinte digitale représente plus de 50 % des techniques biométriques utilisées dans le monde. Ce constat ne fait que souligner une évidence : la maturité de la technologie empreinte digitale s'appuie sur plus d'un siècle d'usage et sur

près d'un demi-siècle d'investissements industriels suscités par la demande des États au travers des systèmes policiers de lutte contre la criminalité.

3. Biométrie : les marchés de demain

Siècle passé ; siècle à venir…

Le siècle passé aura été celui de l'émergence des techniques biométriques. L'empreinte aura marqué le siècle par son usage mondial et aura généré les premières approches industrielles de traitement automatique de données biométriques. Mais c'est aussi vers cette fin de siècle qu'est né un mouvement biométrique profond avec les prémices de la reconnaissance des visages, de la parole, la reconnaissance de l'iris ou encore de l'oreille et surtout la reconnaissance ADN. On peut, sans trop se tromper, prédire que le siècle à venir apportera à maturité toutes ces nouvelles techniques pour des usages de confort ou de sécurité.

Dans la vie économique, la relation État-citoyen et la majorité des actions des organisations reposent fondamentalement sur l'existence visible ou implicite d'une chaîne de confiance. Historiquement, plus que tout autre, les acteurs ayant en charge la défense et la sécurité des nations ont développé un corps de techniques permettant de valider l'authenticité des informations et des ordres pouvant influer sur le bon fonctionnement de leurs missions. « Le code secret des Romains » apportait tout autant une garantie de secret que d'authenticité, plus près de nous le sceau de cire n'était que la représentation d'un effort, aujourd'hui désuet, de confirmation de l'authenticité d'un acte.

Le siècle dernier a été « cryptologique », de Turing aux infrastructures à clés publiques, il existe une continuité visible des efforts et des enjeux. Ce sont sur ces techniques que s'appuient aujourd'hui les États pour assurer la sécurité de leurs transmissions et de l'authenticité des messages. Il n'est plus raisonnable de se satisfaire seulement de cette approche : le siècle à venir sera « biométrique ».

Les clés de la fonction de confiance reposent sur la possession d'un objet (de plus en plus souvent une carte à puce), et la connaissance d'un secret. Les approches traditionnelles, reposant sur la possession d'un objet (clé) ou d'un secret (mot de passe) ne garantissent en rien l'identité formelle du possesseur de l'objet et/ou du secret. L'augmentation des vols d'identité, aux États-Unis notamment, l'évolution croissante des fraudes aux distributeurs de billets en sont des exemples. Pour une fois, ce sont les acteurs politiques qui ont été précurseurs de la prise conscience du chaînon manquant entre le monde vivant et le monde matériel/virtuel.

Comme toute nouvelle technologie, mais peut-être plus qu'auparavant, son usage suscitera des débats de société sur les risques à l'usage, notamment en matière de liberté individuelle. Les équilibres dépendront des choix de

société, mais aussi de la capacité des acteurs sociaux à comprendre que ces techniques, qui peuvent porter atteinte aux libertés individuelles, peuvent aussi défendre avec autant de qualité, des informations personnelles, des biens, l'identité et donc… la propriété ; alors la biométrie sera appréciée à l'aune du risque systémique d'effondrement du monde économique virtuel.

L'après 11 septembre

Certains acteurs du petit monde de la biométrie, suivi d'ailleurs par le marché boursier, ont pensé, au lendemain du 11 septembre, que la demande biométrique allait exploser. Effectivement, si les cours de ces sociétés ont été multipliés par trois, très rapidement avec une pointe en décembre, ces mêmes cours étaient redescendus à leur valeur initiale d'avant la crise en septembre 2002, les comptes d'exploitation ayant à assumer la montée des charges de marketing… avec peu de revenus supplémentaires.

En fait, les États ont d'abord accéléré les investissements sur des produits qu'ils avaient déjà en usage : les détecteurs d'explosifs, les centres de commandement ou de gestion de crise. L'usage d'approches technologiques nouvelles, telles que la biométrie, n'apparaîtra que dans un second temps et de façon intégrée à des édifices complexes : système de gestion de visas, système de gestion de passeports. Cette approche intégrée qui fait de la biométrie une commodité est la rançon de la reconnaissance et du début de maturité du domaine. Ces mises en œuvre institutionnelles, s'appuyant sur des réciprocités de traitements, accéléreront l'émergence de standards et l'usage généralisé de ces techniques. Ainsi, de plus en plus de citoyens détiendront des titres biométriques et constitueront le ferment d'un usage futur généralisé de la biométrie.

En conclusion, les événements tragiques du 11 septembre n'ont pas été générateurs d'un développement rapide de la biométrie, mais par contre, ils seront à coup sûr à l'origine d'un développement à long terme, inéluctable et de grande ampleur, des techniques biométriques.

La rupture du « business model »

Le passé a montré que la biométrie se développait significativement sur les applications gouvernementales et plus faiblement sur les applications commerciales et industrielles. Il faut y voir probablement les fondements de choix plus politiques qu'économiques. L'impact politique de la mise en place d'un système de titres d'identité ou de passeports biométriques ou encore de systèmes de lutte contre la criminalité est indéniable alors même que le retour économique, bien qu'existant, est dur à cerner. L'économie reprend le pas, ou plutôt est un moyen de résistance à l'usage de la biométrie, dès lors que le marché adressé soulève des problèmes de liberté individuelle : c'est le cas

notamment du marché des droits sociaux aux États-Unis qui s'interroge régulièrement sur le retour d'investissement. En effet, la fraude détectée étant très faible mais connue prend le pas sur l'effet dissuasif économiquement très important mais n'ayant jamais fait l'objet d'études sérieuses.

S'agissant des marchés commerciaux, et notamment celui des transactions financières, malgré une chute drastique des prix de la technologie (division par dix sur les cinq dernières années pour les solutions à empreintes digitales), aucun des acteurs n'est prêt à anticiper un retour sur la fraude évitée : l'utilisateur ne voit pas pourquoi il payerait un outil de sécurisation pour une carte de débit délivrée par des banques qui lui assurent la couverture des risques en cas de fraudes, les banques selon les cas, se retournent vers les marchands et/ou prennent des provisions pour risques sur les comptes des clients, les marchands provisionnent leur risque dans leur prix de vente. Ainsi s'est constitué un cercle « non vertueux » qui rend très difficile l'achat d'équipement de sécurité biométrique. Seul un risque systémique majeur[13, 14] ou encore un acteur mondial en recherche de différenciation forte peuvent provoquer une rupture de ce cercle et faire apparaître une valeur économique affichée.

La prégnante évolution des vols d'identité

Devant la montée en puissance des vols d'identité aux États-Unis, la commission fédérale du Commerce (FTC) a mis en place une organisation dédiée au recensement de ce type de crime. Le dernier rapport en date du 3 septembre 2003 a fait l'objet d'un communiqué de presse extrêmement alarmant :

Sur ces 5 dernières années :

- 27.3 millions de citoyens ou résidents américains ont fait l'objet d'un vol d'identité.
- 48 milliards de dollars ont été les coûts subis par les secteurs bancaires et industriels.
- 5 milliards de dollars correspondent aux coûts subis par les particuliers.

Sur la dernière année :

- 9.9 millions de citoyens ou résidents américains ont fait l'objet d'un vol d'identité.
- 3.23 millions de personnes ont eu à subir les conséquences de l'ouverture d'un nouveau compte bancaire.
- 1.5 million de personnes ont constaté que le vol d'identité avait servi à d'autres actions que des opérations sur leur compte : demande de faux documents aux autorités gouvernementales, de formulaires d'imposition.

- 5 millions de personnes se sont rendu compte de l'incident dans le cadre de la gestion de leur compte.
- 2.5 millions de personnes ont été informées par leur banque.
- 800 000 personnes ont constaté l'incident après épuisement de leur compte.

Cette situation très préoccupante devrait amener inéluctablement à repenser la sécurité des paiements ainsi que les mécanismes de délivrance de droits ou de documents gouvernementaux. Le passage au nouveau standard de cartes à puce (EMV) en Europe devrait amener un nouvel élément de réponse mais susciter un intérêt grandissant, de la part des fraudeurs, sur les mécanismes d'attaque des codes secrets. L'extension de cette approche à l'ensemble des cartes d'un utilisateur pose en outre un problème non négligeable de facilité d'usage. Dans ce contexte, la biométrie – sous réserve qu'elle ait résolu un certain nombre de challenges – devrait trouver une place significative.

L'évolution des marchés

Les marchés de la lutte contre la criminalité

Ces marchés ne devraient pas connaître de bouleversements fondamentaux, comme ceux connus durant le siècle dernier. Les systèmes d'empreintes digitales s'appuyant sur des solutions totalement logicielles devraient prendre place dans les plus petites organisations de police et permettre des identifications locales ou nationales au travers de microsystèmes, fixes ou mobiles, en réseau.

L'évolution vers le bureau sans papier et des services de type « background check », utilisant des booking stations, devrait se poursuivre sur les cinq ans à venir et devrait connaître une accélération grâce à la diminution des prix suscitée par les demandes importantes des marchés institutionnels.

Après l'empreinte, puis l'ADN, l'extension vers l'usage d'autres biométries – visages sûrement et iris probablement – devrait être dans la nature de ce segment de marché. En parallèle à ces choix technologiques, les fonctions devraient évoluer vers de la surveillance, à plus long terme vers de l'identification à distance. Ce développement tout biométrique devrait rendre plus délicat et plus complexe les choix des organismes de protection des libertés individuelles.

Ce marché établi et mature sur les systèmes d'empreintes digitales, avec la décroissance des coûts des technologies, devrait connaître une croissance douce.

Les marchés institutionnels

Ces marchés devraient d'abord se développer à l'international sur les cinq à dix années qui viennent, notamment sur la gestion des flux

transfrontières de personnes. La multiplicité des acteurs dans chaque pays et les positions différentes de chaque pays quant à l'usage de la biométrie en matière de liberté individuelle devraient favoriser un usage des trois biométries fondamentales à savoir : les empreintes, l'iris et le visage. L'indispensable interopérabilité et les choix qui seront faits sur les cinq ans qui viennent, devraient favoriser une consolidation des acteurs.

Sur le plan national, les choix de Société seront plus marqués autour de la mise en place ou non de titres d'identité biométriques. L'Europe, par son histoire, devrait plus facilement envisager de tels titres avec probablement quelques fonctions d'authentifications biométriques. Même l'Angleterre, pourtant éloignée d'un tel usage, devrait connaître quelques débats sur le sujet. Les États-Unis laisseront les États trancher quant à l'usage de la biométrie dans les permis de conduire et devraient se garder d'une approche fédérale.

La vraie question portera sur l'usage de fonction d'identification biométrique régalienne : l'État pourrait fournir un titre d'identité unique à chaque personne, permettant une authentification biométrique et dispensant chacun de ses services d'avoir à procéder à des identifications souvent peu performantes. Un identifiant propre à chaque service protégerait les personnes d'un recoupement injustifié des informations personnelles. C'est la notion de titre fondateur[15] qui rend enfin l'État responsable de la protection de l'identité de ses citoyens et de ses résidents.

Quels que soient les choix faits par les États, des problèmes aux limites se poseront et favoriseront une approche plus globale : par exemple, les frontaliers, auteurs de passages réguliers et fréquents, se verront doter de cartes de passage plus commodes d'usage qu'un passeport. Cette carte biométrique prendra probablement une légitimité d'usage aussi forte que la carte d'identité.

Enfin, les services d'identification (background check policier ou non) devraient se développer plus rapidement dans les pays qui ne retiennent pas l'option de titres fondateurs, donnant ainsi naissance à des marchés multiples, fragmentés et probablement plus importants.

Toutes ces approches feront l'objet d'évaluations et de projets pilotes et il est probable que dans un certain nombre de pays, les armées – pour lesquelles la sécurité est une nécessité de premier rang – devraient devenir les véritables incubateurs d'un usage de la biométrie au niveau des différents services d'un État. C'est déjà le cas avec le projet « Common Access Card » du département de la Défense des États-Unis.

Ce marché devrait connaître une très forte croissance sur les dix ans qui viennent.

Les marchés industriels et commerciaux

Les marchés de « Back End » continueront à se développer, surtout dans le contrôle d'accès physique qui profitera des exigences de sécurité des sites sensibles et des activités de transport.

L'arrivée des premiers ordinateurs portables biométriques devrait accélérer les solutions de contrôle d'accès logiques biométriques, notamment chez les utilisateurs nomades et devrait entraîner une généralisation, dans un second temps, de la fonction biométrique à l'ensemble des systèmes d'informations.

Le véritable enjeu de ce segment de marché porte sur la rupture du « business model » existant et l'usage de la biométrie dans les transactions économiques. Certaines sociétés pionnières sont en train de créer des références significatives. Le programme Biopay devrait être utilisé, au début de 2004, par plus d'un million d'Américains qui ont accepté, sur la base du volontariat, de faire enregistrer leurs empreintes digitales.

L'explosion du marché dépendra de l'appréhension du risque systémique de rupture de la chaîne de confiance des transactions financières[16]. Dans ce cas, des modèles nouveaux, basés sur un revenu à la transaction devraient générer des flux récurrents encore plus importants que le marché institutionnel. Dans le cas contraire, le marché connaîtra une croissance régulière légèrement supérieure à celle observée aujourd'hui.

Ce marché profitera dans tous les cas des baisses de coûts générées par le marché institutionnel ainsi que de la consolidation des acteurs.

Les marchés d'usage personnel

Ce marché est en train de voir le jour autour de produits semiprofessionnels nomades où le confort l'emporte sur la sécurité (téléphone, PDA, voiture). La baisse des prix qu'il implique devrait donner naissance à une fonction biométrique peu chère diffusable massivement : jouet, coffre-fort, serrures biométriques. Aujourd'hui inexistant, le marché devrait commencer à prendre corps à l'horizon de 3 à 5 ans.

4. Les challenges à venir

La technologie

Les recherches de technologies plus ou moins exotiques se poursuivront, mais ce ne seront pas des thèmes technologiques majeurs. Les technologies qui fourniront les marchés de demain existent. Les efforts porteront surtout sur la consolidation de l'existant avec notamment des thèmes tels que :

- Le durcissement des capteurs pour supporter les environnements opérationnels de routine (température, éclairage et humidité notamment).

- Le développement de techniques de captures non participatives (surveillance par identification à distance).
- L'amélioration des techniques de détection de leurres biométriques artificiels (faux doigts, faux iris, photos de visage) ou reposant sur l'emploi d'éléments anatomiques (doigts morts par exemple).
- La reconnaissance du visage en trois dimensions et le développement d'outils d'utilisation des archives de photos existantes.
- La définition d'approches architecturales « sûres » s'appuyant sur des approches de « critères communs » tels que mis en place en matière de cartes à puce.
- L'amélioration des performances et notamment la diminution drastique des « Failure To enroll » et des « False Reject Rate » : ce point est fondamental pour adresser correctement le marché des transactions financières.
- Le développement d'approches multi-biométriques afin d'améliorer simultanément les performances et la résistance aux attaques par leurre.
- La recherche de techniques d'analyse d'ADN en temps réel.

Le respect des libertés individuelles

Les doctrines traditionnelles des organismes en charge des libertés individuelles, telles que les principes de proportionnalité, de finalité et de traces[17] notamment seront remises en cause par l'usage de plus en plus fréquent des biométries et la multiplicité des technologies utilisées par les polices.

La recherche de solution passe par une communication et une éducation responsables de tous les acteurs : organismes en charge des libertés individuelles, les gouvernements, les industriels et les citoyens. Les solutions s'appuieront sur un choix judicieux d'approches légales et techniques.

Sur le plan technique

La notion d'identité ne repose pas sur la stricte donnée biométrique. L'identité est un ensemble de données attributs (état civil, adresse, photos, données personnelles, n° d'identification…) qui permet par exemple de retrouver un individu. La simple donnée biométrique, en absence d'attributs, permet de gérer l'unicité de la délivrance d'un droit, ce qui en soi peut présenter un intérêt sans pour autant porter atteinte aux libertés individuelles. Il existe des mécanismes techniques qui permettent de gérer un lien entre données biométriques et attributs de façon sûre et nécessitant l'accord préalable de la personne intéressée. Il existe aussi des moyens de cryptages qui peuvent être utilisés sous le contrôle de tiers de confiance.

Bien qu'il soit possible de s'appuyer sur des mécanismes difficilement inversibles, les principes de précautions développés par les organismes en charge des libertés individuelles envisagent toujours que ce qui est fait par un industriel peut être défait par ce même industriel dans le cadre de contraintes légales non initialement prévues.

Sur le plan légal

Des textes régissant l'usage des informations biométriques à des fins d'enquêtes policières peuvent et doivent venir compléter les approches techniques. Il est ainsi possible à chaque utilisateur d'apprécier avant usage de quelles manières peuvent être traitées les informations biométriques qu'il accepte de donner.

En matière d'éducation, la dualité identité-propriété doit être remise en perspective : dans une transaction, l'aspect « remise en cause de l'identité de la personne » prend trop souvent le pas sur la protection de ses biens propres.

Enfin question limite, d'un point de vue légal, quelle responsabilité prend un État qui refuse de contrôler par exemple l'identité de passagers alors qu'il possède les données et les moyens d'identifier des terroristes ?

Les standards

La principale question en matière de standard est la définition de formats de données biométriques interopérables préservant les évolutions techniques futures. Aujourd'hui, étant donné les limites des ressources des unités de traitement ou des cartes à microproceeseur (mémoire, débit et puissance de calcul), pour respecter des temps de traitement raisonnables, il est préférable d'anticiper les traitements d'authentification en enregistrant comme format de données un gabarit de référence. Cette approche ne pose pas de problèmes fondamentaux pour ce qui concerne le traitement automatique des empreintes digitales, les quatre acteurs mondiaux ayant une description commune à savoir les points caractéristiques. Il n'en est pas de même pour la reconnaissance des visages où différentes descriptions de gabarits s'affrontent.

L'évolution des technologies du traitement de l'information ne laisse aucun doute, il sera possible avant dix ans de garder l'image originale compressée de la donnée biométrique d'origine. Le standard reviendra plus simplement à se mettre d'accord sur les critères d'acquisitions et la technique de compression à utiliser.

En attendant, rien n'empêche de se mettre d'accord sur ce qui est déjà réalisable : l'utilisation du futur standard de gabarit par points caractéristiques des empreintes digitales[18] qui devrait être dans un état stabilisé dès milieu 2004.

Notes

1. Par exemple, en matière de gestion de titres institutionnels (titres d'identité, permis de conduire…) l'objectif est de distinguer et de gérer les personnes qui ne sont pas seulement les citoyens connus d'un État, mais aussi les résidents ou visiteurs étrangers. La population à gérer est distincte et plus importante que la population connue.
2. Prenons l'exemple d'une transaction au guichet d'un distributeur de billets : la description qui permet d'authentifier la personne est « la personne qui connaît le code secret yyyy ». Une personne qui tape ce code secret est authentifiée, mais la force de cette reconnaissance qui implique une remise d'argent, repose sur la qualité du tiers de confiance qui a défini et qui gère ce secret. Ainsi apparaît le concept d'authentification de titre différent de celui d'authentification de personne.
3. Par exemple le programme d'évaluation compétitive de la reconnaissance des visages (FRVT2002) conduit par le Département de la Défense US, a fait le choix d'évaluer ces technologies avec un FTE à zéro.
4. Sans rentrer dans des détails techniques, cette corrélation entre les deux taux d'erreurs est intuitivement comprise par tout voyageur aérien qui a pu constater l'augmentation des fausses alarmes des portiques de détection des métaux à la suite de l'évolution récente des exigences de sécurité.
5. Frost et Sullivan, Global AFIS Market 2002.
6. La dernière étude du cabinet américain Frost et Sullivan reconnaît une place de leader mondial à la société Sagem avec une part de marché de 49.4 % des systèmes AFIS vendus dans le monde en 2001.
7. Le marché mondial des Afis Civils. Rapport interne Sagem. mai 2001.
8. Making a Market in Biometrics. The Mc Lean Group. September 15, 1999. International Biometric Industry Association. *www.ibia.org*.
9. The Biometric Industry Report. Market and Technology, Forecast to 2003. Elsevier Advanced Technology. *www.biometrics-today.com*.
10. Round Three Comparative Biometric Testing for IT Security and E-Commerce. Final Report August 2001. International Biometric Group. *www.biometricgroup.com*.
11. World Biometric Market. juin 2001. Frost et Sullivan. *www.frost.com*.
12. Lehman Brothers 1999 Security Industry Overview : « Although the Biometric device industry may be less $100 million today, we estimate that this market will grow 30-35 % annually to reach $400 million in five years. »
13. US Secret Service, James E. Bauer, Deputy Assistant Director, Office of Investigations : « Ready or not, here it comes: Identity Take Over Fraud has come into its own, and promises not to away until significant changes evolve in the manner and methods by which personal identifiers are collected and used. Consumers would do well to arm themselves with knowledge on how to mend damages when victimized. »
14. BBC 16 / 11 / 2003 : « Identity fraud is a 21st century crime. It is silent, hidden, difficult to investigate and breathtakingly simple. »
15. Rapport d'étude qualitative, SOFRES juillet 2002 : La carte d'identité électronique : perception et attentes.

16. Biometrics and the « Financial Services Modernization Act of 1999 », IBIA. CardTech/SecurTech 2000, Miami Beach, 3 mai, 2000.
17. Commission nationale de l'informatique et des libertés : 23e rapport d'activité 2002.
18. Department of Defense and Federal DRAFT on « Biometric System Protection Profile for Medium Robustness Environments » (version 0.02, 3 mars 2002).

Bibliographie

Articles et rapports

DIDIER, Bernard et Francis « WEISS (2003), La biométrie, nouvel outil stratégique de souveraineté », *Revue défense nationale*, novembre.

DIDIER, Bernard « (2003), Moyens et technologies de détection et d'alertes sur les attaques de la chaîne de confiance identitaire », Conseil scientifique de la défense, rapport confidentiel, octobre.

Conférences

OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre » par M. Christian Cabal, député. Compte rendu d'áuditions (Bernard Didier *et al.*).

DIDIER, Bernard et Samuel HAILU CROSS (2003), « Biometric Management of Institutional Titles: Securing Passports and Visas », Salon Cartes, Paris, novembre.

DIDIER, Bernard (2001), « Brèves introductions sur le marché du traitement automatique de l'empreinte digitale », Conférence internationale CNIL.

DIDIER, Bernard (2001), « Identification et biométrie », Journées Sciences et Défense.

DIDIER, Bernard (2002), « À propos de biométrie… », Club CSA, Paris, décembre.

Études de marché

Worldwide Hardware and Biometrics Authentication Forecast and Analysis, 2001-2006, IDC.

The Biometric Industry Report – Forecasts and Analysis to 2006 – Second edition, Elsevier Advanced Technology, 2002.

Biometric Report 2003-2007, International Biometric Group.

MSI étude: « Le marché du contrôle d'accès électronique en France », MSI Marketing Research for Industry Ltd, août 2002.

Biometrics and the Automotive Industry, Frost and Sullivan, 2002.

Biometrics in Smart Cards, Frost and Sullivan, 2002.

Biometrics in Travel, Frost and Sullivan 2002.

World Biometrics Equipment Market, Frost and Sullivan, 2002.

BIOVISION Final Report, octobre 2003. Fifth Framework IST programme, European Commission.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 4

RFID : le concept et l'incidence

par

Steve Hodges et Duncan McFarlane
Auto-ID Lab, Université de Cambridge
Royaume-Uni

1. Introduction

L'identification par radiofréquences ou RFID connaît depuis les cinq dernières années une percée spectaculaire car elle apparaît comme une solution relativement peu coûteuse pour relier des objets non électroniques à un réseau d'information. Le secteur de la logistique, en particulier, semble tout désigné pour un déploiement à grande échelle de cette technologie. On trouvera dans le court rapport ci-joint une présentation générale de la technologie et de sa situation par rapport aux technologies concurrentes. Différentes applications sont passées en revue, avant quelques remarques de conclusion sur l'incidence probable de la RFID pour la collectivité et sur les obstacles possibles à son déploiement. Le présent rapport s'adresse à un public non technicien, notamment aux hauts responsables de différents secteurs comme l'assurance, la banque, les télécommunications, l'administration publique et l'université. Il ne traite pas de technologies autres que la RFID, comme celles qui pourraient être envisageables pour le suivi des personnes.

2. Technologie

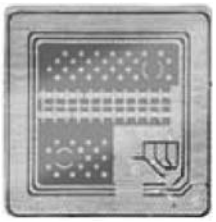
Nous allons dans cette section faire un bref historique des systèmes RFID et décrire leur fonctionnement (Finkenzeller, 1999). Nous allons également examiner les conséquences en termes de réseaux de la généralisation des données RFID et enfin comparer la RFID avec d'autres technologies similaires.

Introduction à l'identification par radiofréquences (RFID)

Sous sa forme la plus simple, un système d'identification par radiofréquences (RFID) est constitué de deux éléments, un marqueur (également appelé transpondeur) et un lecteur (également appelé interrogateur). Le marqueur est conçu pour être peu coûteux et de petite taille – au format d'une carte de crédit ou même plus petit – alors que le lecteur est plus coûteux et plus volumineux, en général de la taille d'un ordinateur portable (figure 1). Le marqueur RFID contient une petite quantité de mémoire pour la conservation de données, et chaque fois que le marqueur se trouve à proximité d'un lecteur RFID, le lecteur détecte sa présence et peut lire les données qu'il contient.

Dans la pratique, une application RFID mettra généralement en jeu un grand nombre de marqueurs RFID apposés sur des objets physiques. Quand l'un de ces objets se trouve à proximité d'un lecteur RFID, les données

Figure 1. **Exemples d'un marqueur RFID et de différents modèles de lecteurs**



Performa Tag

Performa Slimline RFID Reader

Performa Portable Reader

Performa Long Range Reader

Note : Fabriqués par Checkpoint Systems (a). La taille réelle du marqueur est d'environ 5 cm x 5 cm (en haut à gauche). Les dimensions du lecteur Slimline sont d'environ 35 cm x 25 cm.

mémorisées dans le marqueur associé peuvent être lues, de manière à identifier l'objet en question ou obtenir des informations à son sujet. Par ailleurs, les applications pratiques de la technologie RFID utilisent souvent plusieurs lecteurs RFID, afin que les objets marqués puissent être identifiés en différents endroits.

Il existe un grand nombre de types différents de systèmes RFID, dont le mode exact de fonctionnement et les performances varient. Avec les systèmes RFID actifs, le marqueur contient une petite pile qui lui permet de commander la communication avec le lecteur. Un marqueur RFID entièrement passif, cependant, n'a pas de source d'énergie propre et il retire l'énergie dont il a besoin pour fonctionner du signal de radiocommunication émis par le lecteur. C'est donc le lecteur qui commande la communication, mais le marqueur est de ce fait bien meilleur marché.

Aperçu du fonctionnement de la RFID

La RFID utilise des communications par radiofréquences Le lecteur RFID émet de l'énergie, sous la forme d'une onde radio à une fréquence donnée, qui sert à alimenter les marqueurs RFID et à communiquer avec eux. À mesure

que les ondes radio se propagent dans l'environnement, leur énergie diminue peu à peu de sorte qu'un marqueur situé au-delà d'une certaine distance d'un lecteur RFID ne pourra pas recevoir un signal suffisamment fort pour fonctionner de façon fiable. En d'autres termes, la distance maximale de fonctionnement entre un lecteur RFID et un marqueur (également appelé portée) est limitée. La portée exacte dépend d'un grand nombre de facteurs, notamment de la fréquence radio utilisée par la communication, de la puissance d'émission du lecteur RFID et de la présence éventuelle dans l'environnement de sources d'interférences radio ou d'objets susceptibles de réfléchir ou d'absorber les ondes radio. La portée d'un système RFID passif est en général comprise entre quelques centimètres et quelques mètres. Si le marqueur comporte une batterie, la portée est considérablement augmentée, jusqu'à plusieurs dizaines de mètres, voire davantage.

Comme la communication est basée sur la propagation d'ondes radio, il n'est pas nécessaire que le lecteur et le marqueur « se voient ». (À la différence des systèmes de codes à barres dans lesquels le lecteur doit pouvoir « voir » l'étiquette du code à barres.) Il est donc possible d'identifier les objets marqués, même si le marqueur ou l'ensemble de l'objet n'est pas directement visible par le lecteur – celui-ci peut, par exemple, être à l'intérieur d'un emballage ou masqué par d'autres objets. De même, la plupart des systèmes RFID modernes peuvent identifier très rapidement une succession de nombreux marqueurs (de quelques dizaines à plusieurs centaines par seconde). Il est donc possible de lire un grand nombre d'objets marqués pratiquement simultanément lorsqu'ils passent devant un lecteur RFID, chose qui n'est pas facilement réalisable avec d'autres technologies comme les codes à barres. Bien que l'orientation relative du marqueur et du lecteur soit susceptible d'influer jusqu'à un certain point sur la portée pratique du système, il est souvent possible de configurer le système RFID de manière à atténuer cet effet – en d'autres termes, les objets marqués peuvent passer devant un lecteur sans que leur orientation ou leur alignement soit véritablement une contrainte, ce qui est un autre gros avantage par rapport à plusieurs autres technologies d'identification.

Les systèmes RFID utilisent pour fonctionner un canal de radiocommunications, ce qui a un certain nombre de conséquences pour la sécurité de fonctionnement du système. L'aspect le plus fondamental est que le canal est, par sa nature même, partagé avec d'autres dans son environnement immédiat.

Cela signifie que :

- Toute transmission peut être détectée par un autre équipement quelconque situé à portée.

- Un autre équipement quelconque est susceptible d'émettre – et donc de créer des interférences.

On considère souvent que la première de ces deux possibilités correspond à un risque de sécurité significatif, car le système fonctionnant même sans visée directe, quiconque voulant espionner le système peut le faire relativement aisément tout en restant caché. Cependant, les signaux émis par le marqueur sont extrêmement faibles, et pour les écouter il faut donc être très proche (ou en tout cas à une distance pas plus grande que celle entre le marqueur et le lecteur autorisé). Il est possible de concevoir des systèmes RFID utilisant des communications entièrement sécurisées, dans lesquelles l'information échangée est chiffrée, mais cela pèsera sur le coût des marqueurs et les performances du système (en termes de portée, de vitesse de communication, etc.), et ils ne sont actuellement pas considérés comme commercialement viables.

L'autre éventualité envisagée ci-dessus est peut-être plus intéressante. D'une part, elle signifie qu'un lecteur non autorisé a la possibilité de communiquer avec les marqueurs. Elle signifie aussi que n'importe quel équipement produisant des signaux de radiocommunication à la même fréquence que le système RFID interférera avec le fonctionnement de celui-ci, ce qui réduira ses performances et pourrait le rendre inexploitable. Cela a peu de chance de se produire par hasard – et serait selon toute vraisemblance le résultat d'une utilisation malveillante (et illégale) d'un équipement générateur d'interférences.

Historique de la RFID jusqu'aux évolutions les plus récentes

Les concepts sur lesquels repose la RFID ont été mentionnés pour la première fois vers le milieu ou la fin des années 40, dans le prolongement des progrès techniques des radiocommunications réalisés au cours des années 30 et du développement du radar pendant la Seconde Guerre mondiale (Roberti, 2002). L'une des premières publications traitant de la RFID est le document d'Harry Stockman (1948) intitulé « Communication by Means of Reflected Power », dont la publication a fait date. Stockman indiquait à l'époque que « de toute évidence, des travaux considérables de recherche-développement doivent être faits avant que l'on puisse résoudre les problèmes fondamentaux qui subsistent dans la communication par énergie réfléchie et explorer les domaines d'applications utiles ».

Les années 50 ont été une période d'exploration des techniques RFID, durant laquelle plusieurs technologies d'identification par radiofréquences ont été développées, comme le système de transpondeur à longue portée IFF (identification, friend or foe ou identification ami/ennemi) pour les avions (Landt et Catlin, 2001). Il s'en est suivi une décennie de nouveaux

développements de la théorie et des applications de la RFID, notamment son utilisation par le ministère de l'Agriculture des États-Unis pour le suivi des mouvements du bétail. Dans les années 70, les toutes premières applications commerciales de cette technologie ont vu le jour et dans les années 80, l'exploitation commerciale de la technologie RFID a commencé à se développer, à l'initiative d'abord de petites entreprises.

Dans les années 90, la RFID a connu un déploiement beaucoup plus important. Toutefois, ces déploiements intéressaient surtout des domaines d'applications verticales, ce qui s'est traduit par la mise au point d'un certain nombre de systèmes propriétaires différents par plusieurs fournisseurs de solutions RFID. Chacun de ces systèmes présentait des caractéristiques légèrement différentes (principalement en termes de prix et de performances) qui les rendaient adaptés à tel ou tel type d'applications. Cependant, ils étaient incompatibles les uns avec les autres – les marqueurs d'un fournisseur ne pouvant fonctionner avec les lecteurs d'un autre. Cela a sensiblement freiné l'adoption en-dehors de certains créneaux spécifiques d'applications verticales – l'interopérabilité nécessaire pour une adoption plus générale ne pouvant être obtenue sans une spécification normalisée unique pour le fonctionnement intéropérable des systèmes RFID. Cette normalisation était également nécessaire pour faire baisser les coûts.

Le mouvement en faveur de la normalisation a débuté à la fin des années 90. Un certain nombre d'initiatives de normalisation ont été engagées, qui ont débouché sur deux projets :

- La série de normes ISO 18000 qui, en substance, spécifie la façon dont les échanges d'information devraient se faire dans un système RFID entre les lecteurs et les marqueurs.
- Les spécifications de l'Auto-ID Centre, couvrant tous les aspects du fonctionnement d'un système de suivi d'articles par RFID, qui ont été par la suite communiquées à l'AEN.UCC (l'organisme de tutelle du système commun de code à barres) pour normalisation internationale.

Il se pourrait tout à fait que les deux normes fusionnent à l'avenir, pour donner une spécification unique du fonctionnement interopérable d'un système RFID, ce qui encouragerait l'adoption à plus large échelle de la technologie et contribuerait à faire baisser les coûts. Ainsi, les marqueurs passifs et lecteurs RFID, qui par le passé coûtaient de l'ordre de 0.50-1 $ et 1 000-2 000 $ respectivement, tendent vers des coûts de 0.05-0.10 $ et 200-400 $.

Dans son projet de spécification d'un système d'identification automatisée basé sur la RFID, l'Auto-ID Centre (site web) a privilégié plus particulièrement la définition de spécifications globales et ouvertes afin de parvenir à des coûts très bas pour les marqueurs et lecteurs.

L'Auto-ID Centre

L'Auto-ID Centre est un organisme à caractère universitaire créé initialement en 1999 par le MIT, l'Uniform Code Council (ou UCC, en charge du code à barres en Amérique du Nord), Gillette et Procter & Gamble. L'idée avec ce Centre était de développer un système adapté au suivi des biens de grande consommation (CPG) quand ils circulent le long de la chaîne d'approvisionnement, de manière à surmonter les problèmes de démarque inconnue et de médiocre disponibilité en rayon pour certains produits. Le Centre a connu une croissance rapide et en octobre 2003 il comptait plus de 100 entreprises adhérentes, ayant toute un intérêt commun soit dans le développement d'une telle technologie dans le cadre de leurs activités, soit dans la fourniture de ces composants technologiques.

Dès les toutes premières années du centre, il est apparu clairement que la RFID allait être une pierre angulaire de la solution technologique, et avec l'aide d'un certain nombre d'entreprises utilisatrices et productrices de technologies, le centre a contribué de façon déterminante à faire baisser les coûts de la RFID à un niveau tel que son adoption a commencé à devenir rentable dans certains domaines d'application. Une partie de la solution pour maintenir les coûts à un faible niveau réside dans le souci constant de réduire la complexité des marqueurs RFID, et l'une des approches préconisée à cet effet par l'Auto-ID Centre est de mémoriser le moins de données possibles concernant le produit dans le marqueur. Il est préférable car plus rentable de stocker cette information sur le réseau informatique de l'organisation. Un système Auto-ID utilisant la RFID comprend donc en général les éléments suivants :

1. Un numéro d'identification unique attribué à chaque article (appelé code électronique du produit, ou EPC).
2. Un marqueur d'identité fixé sur l'article, qui comporte une puce capable de mémoriser – au minimum – le numéro d'identification unique. Le marqueur est capable de communiquer ce numéro par voie électronique.
3. Des lecteurs RFID et systèmes de traitement de données en réseau, capables de recueillir les signaux de plusieurs marqueurs très rapidement (des centaines par seconde) et de prétraiter ces données pour éliminer les doublons et les erreurs de lecture.
4. Une ou plusieurs bases de données en réseau, qui mémorisent les informations sur les produits.

Dans cette approche, le coût de l'installation et de la maintenance de ces systèmes peut être réparti entre plusieurs organisations, chacune étant en mesure de bénéficier de retombées spécifiques qui lui sont propres, grâce au marquage identifiant de façon unique les produits qui entrent dans la chaîne logistique de l'entreprise, y transitent et en sortent.

Comparaison avec d'autres technologies

La technologie la plus immédiatement comparable avec la RFID pour de nombreux domaines d'application est celle des codes à barres. Ces deux technologies fonctionnent par l'apposition sur un article d'un marqueur ou d'une étiquette contenant des informations sur cet article, qui permettent son identification par un système informatique.

L'identification des objets par marqueurs RFID présente deux avantages par rapport au système traditionnel par code à barres :

1. Les codes à barres ne peuvent plus être modifiés une fois créés, alors qu'il est possible d'enrichir ou de modifier selon les besoins les données contenues dans un marqueur RFID (Halliday). Cela signifie :
   - qu'il est possible de dissocier le moment où l'objet est marqué du moment où l'information est mise en mémoire dans le marqueur – ce peut être un avantage si l'on veut, par exemple, apposer le marqueur à un moment quelconque dans le processus de fabrication d'un article, avant que l'information devant être mémorisée dans le marqueur soit connue. Cela est impossible avec un code à barres ;
   - que l'information peut être mise à jour à mesure qu'un produit marqué circule dans un processus, ce qui permet de conserver les informations importantes dans le marqueur (et sur l'article) et donc de pouvoir y accéder à n'importe quel moment sur sa durée de vie (Hallyday).
2. La lecture des codes à barres est une opération volontaire effectuée par un opérateur, qui est difficile à automatiser. Les marqueurs RFID en revanche, peuvent être facilement lus de façon automatique, sans participation humaine. Cela signifie que :
   - les données peuvent être obtenues en continu et qu'elles sont donc plus à jour que des données obtenues uniquement à intervalles spécifiés (comme les relevés d'inventaire) et en des points spécifiques dans la chaîne d'approvisionnement (par exemple lors de l'expédition ou de la réception) ;
   - du fait de l'absence d'intervention humaine, la lecture est moins coûteuse et en général plus précise – les lectures incrémentales sont pratiquement sans coût, une fois le système mis en place. Cela peut également se traduire par une diminution des erreurs de lecture ;
   - le système est plus rapide – il est possible avec un ordinateur de lire plusieurs marqueurs simultanément, alors que manuellement il faut lire les étiquettes une par une.

3. Pour pouvoir être lus, les codes à barres doivent être visibles alors que les marqueurs RFID peuvent être lus (dans n'importe quelle orientation), dès lors qu'ils sont à portée du lecteur. Cela implique que :
   - le contenu de divers contenants (tels que remorques, caisses, palettes, caddies) peut être lu automatiquement, sans avoir à vider et trier ce contenu ;
   - les étiquettes de codes à barres sont moins performantes lorsqu'elles sont exposées aux éléments climatiques, lorsqu'elles sont sales ou lorsqu'elles sont endommagées au point de gêner la lecture directe. Les marqueurs RFID sont beaucoup mieux adaptés aux environnements sévères (Halliday). Le marqueur RFID peut même être caché à la vue si cela présente un avantage, alors qu'un code à barres se remarque très facilement.

Outre les systèmes RFID et de codes à barres, il existe également un certain nombre d'autres technologies pouvant être utilisées de façon similaire pour stocker les informations sur un objet ou pour identifier celui-ci. C'est notamment le cas des systèmes à bande magnétique et à contacts, dans lesquels l'information est mémorisée sur une bande magnétique ou dans un circuit imprimé (auquel on accède par des contacts électriques), ainsi que des systèmes de vision par ordinateur qui identifient des objets en fonction de leur apparence visuelle. Les avantages relatifs de toutes ces différentes technologies sont récapitulés dans le tableau ci-après.

3. Applications

On trouvera dans cette section un aperçu de la nature des applications dans lesquelles des systèmes RFID ont été déployés à ce jour, ainsi qu'une préfiguration des utilisations futures. Comme indiqué précédemment, l'analyse ne porte que sur l'utilisation de marqueurs sur des objets inanimés.

Applications passées, actuelles et projetées

La détection directe de l'identité d'un produit est importante dans des environnements dans lesquels il est trop complexe, incertain ou coûteux d'extraire des informations sur les mouvements des produits au moyen de méthodes indirectes – lesquelles reposent en général sur des modèles de suivi informatisé et sur des dispositifs simples à base de capteurs de proximité. Après la comparaison des systèmes de codes à barres et des systèmes RFID dans la section 2, il est clair que si l'on a besoin d'un système facilement automatisé, sans fil et sans obligation de lecture directe, permettant toutefois un grand nombre de lectures simultanées, la RFID présente des avantages significatifs.

Ces caractéristiques se retrouvent dans les applications actuelles de le RFID, comme la gestion des chaînes logistiques, les systèmes antivol, le péage

Tableau 1. **Comparaison de RFID avec d'autres systèmes d'identification et transfert de données**

Caractéristique	Technologie de marquage					
	RFID passif	Code à barres 1-D	Code à barres 2-D	Bande magnétique	Mémoire par contacts	Systèmes de vision
Capacité de mémoire	Importante	Faible	Moyenne	Faible	Importante	Faible
Nature des données	Réinscriptible	Lecture seulement	Lecture seulement	Réinscriptible	Réinscriptible	Lecture seulement
Visibilité/lisibilité par l'homme	Caché	Visible, peut-être lisible	Visible	Bande visible	Contacts visibles	Pas de marqueur spécifique
Identifications simultanées	Oui	Non	Non	Non	Non	Éventuel-lement
Robustesse	Forte	Moyenne	Faible	Moyenne	Moyenne	
Portée	Grande	Moyenne	Moyenne	Faible	Faible	Grande
Visée directe nécessaire ?	Non	Oui	Oui	Non	En pratique	Oui
Objets problématiques (par ex. métal)	Oui	Non	Non	Oui	Éventuel-lement	Oui (difficile à voir)
Coût du marqueur	0.1-1 €	< 0.01 €	< 0.01 €	< 0.1 €	0.1-1 €	0 € (n/d)
Coût du lecteur	Élevé	Faible	Moyen	Faible	Faible	Très élevé

électronique et la prestation multiservice (gestion de bibliothèque par exemple) ; la manutention des bagages dans les compagnies aériennes, ou le suivi d'objets. Le tableau ci-après compare la nature de ces différentes applications et montre que les applications dans les chaînes d'approvisionnement sont, du moins jusqu'à présent, assez différentes de la plupart des autres applications existantes.

Ces différences mettent en lumière l'incidence des travaux de l'Auto ID Centre, qui a fait évoluer le modèle de la RFID des applications à faibles volumes et coûts élevés vers des applications dans lesquelles des volumes

Tableau 2. **Résumé des caractéristiques de diverses applications de RFID**

	Péage	Bibliothèque	Objets	Compagnies aériennes	EAS	Chaîne logistique
Complexité de l'information sur le marqueur	Moyenne	Faible	Grande	Faible	Faible	Faible
Application simple ou multiple pour chaque marqueur	Simple	Simple	Simple	Simple	Simple	Multiple
Volume des marqueurs	Faible	Faible	Faible	Moyen	Moyen	Important
Durée de vie escomptée du marqueur	Longue	Longue	Longue	Moyenne	Moyenne	Longue

Tableau 3. **Applications RFID potentielle dans la chaîne logistique du commerce de détail**

Segment de la chaîne logistique	Description	Variations/incertitudes	Applications RFID
Expédition	Groupage, respect des contrats, optimisation du routage, appels d'offres et autres fonctions de gestion des transports associées à l'expédition des cargaisons.	Commandes de dernière minute, expéditions d'urgence, manque de capacité de transport, manque de visibilité de l'inventaire pour la réalisation des commandes, articles mal placés ou pris par erreur, etc.	Visibilité vers l'amont qui augmente les possibilités de planification, optimisation plus aisée du contenu des remorques, accélération des opérations de chargement.
Transport	Ensemble des processus et activités assurés par le transporteur, l'entreprise de logistique, ou quiconque, en relation avec l'opération de transport.	Retards, erreurs dans le routage des colis dans les terminaux, reroutage de dernière minute des expéditions, gestion dynamique du transport routier, erreur dans les opérations de dépose et de reprise, vol pendant le transport, avaries, etc.	Amélioration de la rapidité, de la capacité et de l'exactitude du suivi : suivi des commandes, suivi individualisé des charges partielles ou des palettes individuelles, suivi accéléré des différents articles.
Réception	Vérification, accusé de réception, appariement et mise en rayon à la réception des cargaisons chez l'acquéreur.	Articles manquants, erreurs dans les articles, erreurs dans les quantités, livraison à des destinations erronées (ou à la mauvaise porte), mise en rayon au mauvais endroit, erreur dans la saisie des données, etc.	Vérification instantanée, preuve automatisée de la livraison, localisation précise et à tolérance de panne des articles.
Opérations internes	Englobe tous les processus intervenant chez l'acquéreur. Il peut s'agir des opérations de transformation dans une usine, de stockage dans un entrepôt, de présentation dans un magasin ainsi que de l'ensemble des processus entourant ces activités.	Erreurs dans la détermination de l'état d'un produit en cours de transformation, problèmes de qualité, pénurie de matières premières, erreurs d'inventaire, localisation inconnue d'un produit dans les locaux, etc.	Fabrication : matières premières, suivi de sous-ensembles, suivi d'articles. Entreposage : gestion des stocks, gestion des pièces détachées. Vente au détail : surveillance des rayons, réassort automatique, encaissement automatique.

élevés sont essentiels, les coûts doivent être aussi bas que possible et un même marqueur doit pouvoir être exploité pour plusieurs applications. Le tableau qui suit indique la gamme des applications envisageables sur l'ensemble de la chaîne de l'approvisionnement de détail, pour laquelle la réduction des variations et des incertitudes est capitale.

Études de cas plus détaillées

Pour montrer la façon dont des solutions RFID ont été mises en place, nous allons présenter maintenant un certain nombre de courtes études de cas, qui visent à illustrer notre propos, et non à faire un point exhaustif sur la question.

Gestion de stocks

Des entreprises commencent à utiliser la technologie RFID dans des applications de stockage allant de la gestion d'un stock de produits marqués jusqu'à la localisation et l'enlèvement de produits.

Figleaves, qui est un vendeur en ligne britannique de sous-vêtements féminins, marque ses paniers avec des transpondeurs RFID et place des lecteurs dans les baies, afin que les employés puissent connaître avec exactitude la localisation de n'importe quel panier (Eurotag Newsletter, 2003). Grâce à ce système, la société fait des économies de temps et de personnel, car il est inutile de contre-vérifier les commandes avant leur envoi. Grâce à ce système, le personnel prépare 60 000 articles par mois avec un taux d'erreur inférieur à 0.1 %. L'entreprise souhaiterait cependant éliminer toutes les erreurs de préparation en utilisant également les marqueurs RFID pour faire en sorte que les casiers soient bien où ils sont supposés être. Aujourd'hui, si un casier est mal placé, il est très difficile de le retrouver, car il peut être pratiquement n'importe où dans les locaux. Figleaves voudrait installer des marqueurs sur les étagères et sur les casiers contenant les produits, et même sur chaque article à l'intérieur des casiers quand le coût des marqueurs aura encore baissé. Figleaves souhaiterait installer des marqueurs RFID à la fois sur les casiers et sur les étagères. Ainsi, les employés pourraient circuler dans l'entrepôt, interroger les étagères avec un scanner portatif et vérifier que chaque casier est bien au bon endroit. De la sorte, lorsqu'un employé s'arrête avec un chariot, il serait pratiquement assuré de trouver tout de suite le bon article. Figleaves a calculé que le marquage de chaque article serait rentable si le prix du marqueur tombait en dessous de 0.10 $.

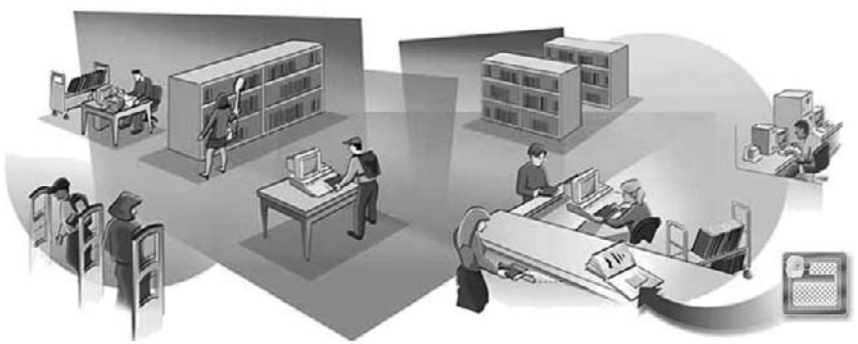
Le distributeur de produits frais Associated Food Stores de Salt Lake City utilise dans son centre de distribution un système de localisation en temps réel par RFID (Violino, 2004). Ce système permet aux dirigeants d'Associated de savoir quand les camions entrent et sortent de l'aire de distribution, et leur localisation exacte. Le système RFID permet également de mesurer certains niveaux de performance, par exemple de déceler une hausse de température, révélant que la porte d'un camion réfrigéré est restée ouverte.

Systèmes pour bibliothèque

La technologie RFID est bien adaptée à la gestion d'articles dans une bibliothèque. Des marqueurs RFID peuvent être aisément apposés sur les livres et autres supports. Ils peuvent être installés à la source (chez l'éditeur) ou plus tard, par exemple par le personnel de la bibliothèque au moment de l'acquisition de l'ouvrage.

Le système d'enregistrement automatique développé par Checkpoint (Checkpoint Systems Inc. b, c) permet aux abonnés de la bibliothèque d'enregistrer eux-mêmes leurs emprunts, ce qui économise du temps de personnel et garantit le respect de la vie privée. Tous les types de cartes de bibliothèque peuvent être utilisés, y compris celles qui utilisent des codes à barres traditionnels, des bandes magnétiques ou des cartes à puces. Les récépissés sont établis automatiquement. Un écran tactile convivial guide l'usager dans la procédure d'enregistrement. Des capteurs protègent automatiquement les entrées et sorties de la bibliothèque. Ils interrogent en permanence les objets qui passent devant le détecteur pour vérifier qu'ils ont bien été enregistrés. Les articles sont vérifiés par rapport au système d'emprunt de la bibliothèque. Si une personne tente de voler des livres, le système peut alerter le personnel. Il est également possible d'identifier un article volé si celui-ci était rendu plus tard, et de signaler les articles qui doivent être remplacés. Un lecteur portable à main peut être utilisés pour inventorier très rapidement les fonds documentaires d'une bibliothèque et aider à la localisation des ouvrages mal remis en rayon.

Figure 2. **Système bibliothécaire avec RFID**



Source : Landt et Catlin, 2001.

Péage routier

Les systèmes de paiement électronique, rendus possibles par la technologie RFID, deviennent de plus en plus populaires pour la perception des péages routiers. Un marqueur RFID (généralement un marqueur actif ou semi-passif) est fixé sur le véhicule et un détecteur est installé à chaque poste de péage. Chaque fois qu'un véhicule marqué passe devant un poste de péage, il est détecté et identifié et l'information est utilisée pour percevoir par des

moyens électroniques le péage correspondant au trajet. Les avantages du péage électronique sont clairs pour le conducteur – il n'a pas besoin de s'arrêter au péage, ni d'avoir la monnaie, ni de faire la queue. De même, les coûts de perception du péage sont sensiblement réduits car les besoins en personnel sont diminués, il n'y a pas à gérer la caisse etc.

Marquage dans l'industrie automobile

L'industrie automobile déploie des efforts considérables pour assurer le suivi et la traçabilité de la totalité des pièces d'une automobile, pour la garantie. Des applications sont en cours de développement pour le marquage des carrosseries (pouvant résister à des températures extrêmes), de pièces métalliques, des sièges et des pneumatiques). Nous allons examiner ces deux derniers produits à titre d'illustration.

Travaillant avec l'Automotive Industry Action Group, Intermec (2002) a mis au point un marqueur UHF lisible/réinscriptible qui peut être placé à l'intérieur d'un pneumatique d'automobile et qui comporte un numéro de série unique et un numéro de code du Department of Transport des États-Unis. Ces deux numéros permettent d'identifier le lieu exact, la date et les conditions de fabrication du pneumatique. Le marqueur est installé pendant la fabrication du pneumatique et les informations sont mises en mémoire sur le lieu de fabrication avant la distribution.

Le marquage des sièges d'automobiles et de camions fait également l'objet d'une grande attention :

Johnson Controls (Collins, 2003) a mis en place un système de marquage fonctionnant à 13.56 MHz développé par Escort Memory Services pour le marquage de la totalité des palettes utilisées pour le transport des sièges d'automobiles et de camions qu'ils produisent. Il s'agissait avant tout d'éliminer les erreurs de suivi, ou plus précisément les erreurs dans l'ordre de livraison et dans le contenu des envois destinés à des clients comme Daimler Chrysler, Ford Motor Co. et General Motors. La technologie RFID a été retenue en raison des environnements difficiles et de la nécessité d'avoir des lectures d'identité très précises. Les codes à barres ont été jugés inadaptés en raison des contraintes de vision directe et du fait qu'il aurait vraisemblablement fallu remplacer régulièrement les étiquettes au cours de la durée de vie de la palette. C'est la solution RFID qui a prévalu, en dépit du fait que l'installation de quatre marqueurs coûte 60 $ par palette. Il est particulièrement intéressant de noter que Johnson a pu utiliser le même système pour améliorer ses opérations dans sa propre usine de production. Ses chaînes de production sont particulièrement flexibles, car elles permettent la fabrication de petites séries de différentes catégories de produits. Cependant, en raison des

limitations des systèmes de gestion des matériaux, il faut établir des inventaires en fin de production, ce qui, par le passé, a conduit à des mélanges de commandes de sièges ayant des spécifications légèrement différentes. La société peut maintenant produire différents types de sièges sur une même chaîne de production sans crainte de confusion et elle peut donc non seulement livrer mais aussi produire à la demande, en flux tirés.

Un large éventail de solutions RFID ont été spécifiquement mises au point pour cette industrie qui est à bien des égards le chef de file en la matière, essentiellement car il se caractérise par des volumes et des prix des articles relativement élevés qui rendent ces solutions économiquement intéressantes aussi bien pour l'utilisateur que pour le développeur.

Applications possibles dans l'avenir

Outre qu'ils conduisent à des améliorations de nombreux processus existants, les systèmes Auto ID permettront dans l'avenir des services et des offres commerciales d'un caractère radicalement nouveau qui pourraient avoir de multiples ramifications. Alors que les applications examinées jusqu'à présent sont principalement justifiées par des considérations de coûts, les applications futures seraient plutôt considérées comme apportant une valeur ajoutée. On notera que l'analyse qui suit a un caractère plutôt spéculatif et qu'elle vise simplement à donner une idée de certaines applications fondamentalement nouvelles actuellement à l'étude.

Le commerce de détail de demain

Le « Saint Graal » du commerce de détail est de réduire les files d'attente aux caisses, sans augmentation de personnel. De nombreux détaillants explorent les possibilités de magasins « sans caisse enregistreuse », dans lesquels des scanners RFID installés soit au niveau des portes, soit sur les caddies facilitent le passage aux caisses pour le consommateur. De même, la RFID permettant la tenue des stocks en temps réel et des réassortiments plus fréquents, il est possible de sensiblement réduire l'espace occupé sur les rayons par chaque article, tout en améliorant les niveaux de services et en réduisant les stocks. Cela pourrait conduire à des supermarchés et autres magasins de détail occupant des surfaces plus réduites, pour un nombre de SKU (unités de stock) proposées demeurant constant.

Procter et Gamble dans l'Ohio, Phillip Morris dans l'État de New York, Sainsbury au Royaume-Uni et MGI (Metro) en Allemagne ont ouvert des magasins du futur pour faire la démonstration du type de facilités que l'on pourrait envisager dans un magasin utilisant l'Auto ID. Les applications vont des rayonnages intelligents (antivol) et des systèmes

sans fil automatisés de passation des commandes, à la gestion dynamique des dates de péremption, en passant par des caddies « intelligents » qui enregistrent les articles au fur et à mesure qu'ils sont déposés dans le caddy et qui actualisent en conséquence une liste de course électronique. Des systèmes de publicité personnalisée ont également été expérimentés.

Les systèmes RFID au foyer

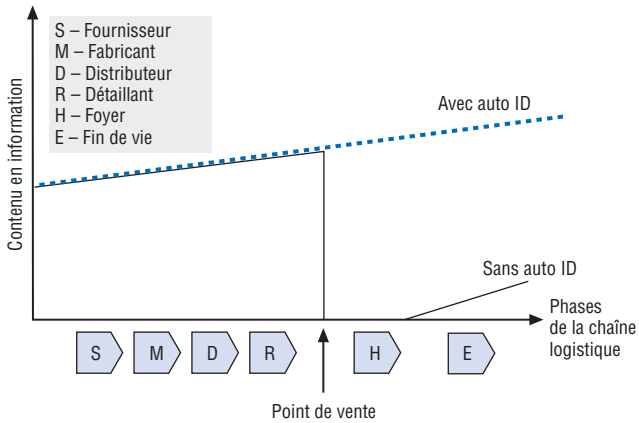
Une des premières applications au foyer pourrait être la tenue à jour permanente de l'inventaire du logement. Mais la RFID pourrait aussi déboucher sur une nouvelle génération d'appareils ménagers capables d'identifier leur contenu et d'agir en conséquence. On peut imaginer des systèmes de cuisson (four à micro-ondes qui lit les instructions mémorisées sur l'emballage) ; des réfrigérateurs ou des meubles de cuisine qui passent automatiquement commande de produits à une boutique quand le stock descend en-dessous d'un niveau fixé à l'avance ou des réfrigérateurs ou des armoires à pharmacie qui informent l'utilisateur des dates de péremption des produits qu'ils contiennent.

Suivre les produits sur tout leur cycle de vie

Aujourd'hui, la chaîne logistique du commerce de détail s'arrête en pratique au point de vente. Avec l'Auto ID, on peut imaginer des applications dans la phase d'utilisation (par exemple au foyer) et la phase de fin de vie (par exemple applications d'élimination/recyclage/réemploi), grâce à la préservation de l'information. Si l'information sur le produit par la mise en relation d'un marqueur RFID avec une infrastructure de bases de données en réseau peut être conservée au cours des phases d'utilisation et d'élimination, l'information est alors connue sur l'ensemble du cycle de vie. La figure 3, extraite de McFarlane et Sheffi (2003), illustre le profil caractéristique actuel de l'information sur les produits quand ils circulent le long d'une chaîne logistique Le gain que procurerait une mise en réseau RFID est représenté par la ligne en pointillés dans la figure 3.

L'un des avantages de l'extension de la visibilité jusqu'au foyer ou au lieu de travail est qu'elle améliore l'efficacité des opérations en fin de vie. Le fait d'être capable de déceler quelles sont les pièces que contient, par exemple, un appareil mis au rebut et de connaître la façon dont cet appareil a été utilisé au foyer peut aider à décider du type de traitement dont il doit faire l'objet, ce qui permettrait au centre de recyclage de se spécialiser. Dans les centres de recyclage, l'information RFID peut aider à automatiser les opérations de tri, qui sont le tendon d'Achille de la plupart des procédés de recyclage. Elle peut également aider à décider quelles sont les pièces à recycler, quelles sont celles

Figure 3. **Contenu en informations sur les produits le long de la chaîne logistique**



Source : Extraite de McFarlane et Sheffi, 2003.

qui peuvent être réutilisées et quelles sont celles qui doivent être mises au rebut et comment.

4. Facteurs d'évolution et effets

Facteurs commerciaux en faveur de la RFID

Un grand nombre de fabricants et de détaillants de produits de grande consommation (CPG) étudient les avantages possibles de la RFID pour le suivi et l'identification de leurs produits quand ils transitent dans la chaîne logistique. Bien que les retombées possibles les plus significatives du déploiement d'une telle technologie puissent varier d'une entreprise à l'autre, si un système RFID commun, normalisé et interopérable était déployé par tous les partenaires commerciaux dans la chaîne logistique, les coûts du déploiement de cette technologie pourraient être amortis sur l'ensemble de la chaîne.

Les progrès technologiques récents dans la RFID ont fait baisser les coûts des marqueurs, surtout si l'on considère les quantités très importantes de marqueurs dont aura besoin le secteur CPG, tout comme les évolutions récentes dans le domaine de la normalisation mondiale, pour lesquelles la RFID apparaît comme une solution beaucoup plus intéressante. De ce fait, les grands détaillants commencent à envisager très sérieusement de déployer cette technologie et le plus grand détaillant au monde, Wal-Mart a récemment annoncé qu'en juillet 2005 ses 100 premiers fournisseurs devraient utiliser la

technologie RFID pour marquer tous les emballages des produits qu'ils fournissent. A terme, cette exigence sera étendue à l'ensemble des fournisseurs. L'annonce de Wal-Mart revêt une importance considérable du fait de sa taille et de son pouvoir sur le marché – ce qui va manifestement doper l'adoption de la RFID dans la chaîne logistique du secteur CPG.

Aux États-Unis, le ministère de la Défense a publié une directive du même ordre, concernant le marquage RFID des articles qu'ils acquièrent, et l'un des premiers détaillants britanniques, Tesco, utilise déjà la RFID dans un de ses centres de distribution avec certains de ses fournisseurs. Tesco a l'intention d'étendre sensiblement le déploiement de la RFID au cours de l'année prochaine. Ces plans contraindront également les fabricants de produits à utiliser la RFID, ce qui sera une incitation forte à l'adoption de ces technologies.

Facteurs législatifs en faveur de la RFID

Outre les facteurs commerciaux, la législation peut être aussi un moteur puissant. Il existe un certain nombre de domaines dans lesquels de nouveaux textes législatifs pourraient bien induire l'adoption de la RFID dans certaines industries et pour certains domaines d'application.

La Directive européenne relative aux déchets de produits électriques et électroniques (WEEE) (Europa, 2004) a été adoptée comme législation communautaire en février 2003 et elle fixe des objectifs pour la collecte, le recyclage et la récupération de tous les types de produits électriques. Les directives doivent être transposées par les États membres européens d'ici août 2004, bien qu'il soit prévu une période supplémentaire de deux ans avant que leur application intégrale soit exigée. Un aspect particulièrement important en ce qui concerne la RFID est la responsabilité obligatoire du producteur à l'égard du financement de la gestion de déchets de produits électriques et électroniques. Cela signifie que les producteurs doivent pouvoir identifier les équipements électriques et électroniques qu'ils ont produits au départ (car ils ne voudront pas supporter les coûts de l'élimination d'équipements d'autres fabricants). De même, il serait intéressant pour eux de pouvoir identifier avec précision leurs propres produits, pour pouvoir recycler les sous-ensembles de la façon la plus efficace possible. De la même manière, les directives de l'UE sur les emballages et déchets d'emballages et sur la gestion des véhicules en fin de vie imposent de nouvelles contraintes dans les domaines de l'emballage et des véhicules à moteur.

La législation sur le suivi des médicaments et des produits alimentaires destinée à garantir la santé et la sécurité humaines est un autre facteur allant dans le sens de l'adoption de la technologie RFID. Dans certains cas, les législations existantes ou en projet imposent aux fabricants et détaillants un

suivi très lourd de ces produits. Dans de tels cas, bien qu'un certain nombre de technologies différentes soient susceptibles d'être utilisées pour répondre aux recommandations, la RFID s'impose comme une solution rentable. Il arrive cependant que la RFID soit explicitement recommandée ou imposée. Ainsi, la Healthcare Distribution Management Association (HDMA), qui est une organisation sans but lucratif de distributeurs, a récemment recommandé que les fabricants et les grossistes de produits pharmaceutiques et autres produits de santé commencent à fixer des marqueurs RFID sur les emballages à compter de 2005 et mettent en place l'infrastructure correspondante nécessaire pour l'utilisation de ces marqueurs (RFID Journal, 2003a). Par ailleurs, dans l'industrie alimentaire, la traçabilité des aliments rendue possible par la RFID est un thème majeur de discussion (Food Traceability Report, 2003).

Impact social de la RFID

Nous allons examiner ici brièvement les incidences possibles de la RFID pour la collectivité, que ce soit sur les individus, la société dans son ensemble et l'environnement.

Incidence sur le consommateur

- *Retombées pour le consommateur* – différents avantages pour le consommateur ont été identifiés en liaison avec la RFID, que ce soit dans les magasins de détail (réduction des files d'attente, produits plus frais, meilleure disponibilité de produits) au foyer (contrôle automatisé des produits, surveillance de l'authenticité et du dosage des médicaments, systèmes d'alarme) ou en déplacement (meilleure gestion des bagages dans les aéroports) ou du fait de la simplification des systèmes d'accès et d'emprunts pour des services publics comme les bibliothèques. Peu a été fait à ce jour pour essayer de chiffrer les retombées de la RFID pour les consommateurs, dans la mesure où l'essentiel des efforts des industriels ont porté récemment sur la chaîne logistique dans les entreprises, et les médias se sont surtout intéressés aux problèmes possibles de violation de la vie privée.
- *Inquiétudes des consommateurs concernant la vie privée* – la RFID a suscité une attention considérable de la part de la presse mondiale au cours des derniers mois en relation avec les problèmes de vie privée des consommateurs soulevés par un nombre relativement réduit de défenseurs de la vie privée (Jha, 2003 ; Dodson, 2003). Si les préoccupations des consommateurs sont légitimes, le plus souvent celles-ci reposent sur un manque de compréhension de ce que permet effectivement la technologie et de la façon dont elle peut être utilisée. L'Auto-ID Centre a dressé une liste de principes directeurs sur les meilleurs moyens de répondre aux

préoccupations du public (RFID Journal, 2003b) ; il s'agit notamment de signaler visuellement les produits ou conditionnements contenant un marqueur RFID, de donner aux consommateurs la possibilité de faire détruire le marqueur au point de vente et de garantir l'anonymat des données recueillies concernant tout article marqué.

Incidence sur la collectivité

- *Santé* – grâce aux progrès de la RFID comme aide pour les soins de santé à l'hôpital ou à domicile, il serait possible d'améliorer la qualité et réduire les coûts du traitement hospitalier et de beaucoup contribuer à la gestion de la population vieillissante d'Europe. Les applications vont du marquage des médicaments tout au long de leur cycle de vie (Commission européenne) aux armoires à pharmacie intelligentes capables de vérifier l'identité de l'utilisateur et celle du médicament, pour vérifier les « autorisations » de l'un et de l'autre.
- *Sûreté des produits alimentaires* – les législations relatives au suivi de la chaîne alimentaire examinées dans la section précédente sont destinées à sécuriser l'ensemble de la chaîne alimentaire et d'assurer un approvisionnement sûr et efficace des consommateurs en aliments, tout en donnant la capacité de suivre et rappeler rapidement et avec précision les produits, si nécessaire.

Incidence sur l'environnement

- *Recyclage et réemploi des matériaux* – les exigences législatives dans ce domaine ont été examinées plus haut. Par ailleurs, il faut noter que le déploiement efficace de la RFID dans la gestion des produits en fin de cycle pourrait, de fait, aider à rendre ces activités rentables, ce qui aurait un effet d'entraînement positif pour de nouveaux progrès dans ce domaine.
- *Gestion énergétique* – l'utilisation de circuits à base de RFID dans les produits électriques est à l'étude dans le cadre d'un projet de recherche communautaire comme moyen de surveillance et d'analyse de la performance des équipements en cours d'utilisation (ELIMA) Les données sont extraites périodiquement et utilisées pour analyser la consommation énergétique, parmi d'autres variables. Jusqu'à 50 % de l'ensemble de l'énergie consommée par de nombreux produits électriques sur l'ensemble de leur cycle de vie l'est dans la phase d'utilisation.

Obstacles possibles au succès de la RFID

Un certain nombre d'enjeux technologiques doivent être relevés :

- *Mémorisation et consultation des données* – le suivi individuel de chaque objet peut produire d'énormes quantités de données qui devront être mémorisées (sans doute dans des bases de données distribuées) et

consultées rapidement. Le Centre Auto-ID a développé des stratégies de migration, mais cela ne peut se faire qu'au prix d'une baisse de fidélité des données.

- *Exactitude* – à mesure que les activités et les systèmes d'information sur lesquels celles-ci s'appuient vont dépendre de plus en plus de données d'identité des produits automatisés et en temps réel, les spécifications imposées aux systèmes d'identification tendront vers la précision absolue des informations de localisation générées. Cela créera de nouvelles difficultés à résoudre dans la conception et la production de marqueurs et de lecteurs.
- *Interférences* – avec la prolifération des dispositifs sans fil (téléphones sans fil et portables, assistants numériques, électronique grand public, etc.) il existe un risque d'interférences électromagnétiques avec les systèmes RFID. Ce problème pourrait prendre une importance particulière dans la mesure où la RFID n'a pas de bande de fréquences propre dans la plupart des juridictions, mais fonctionne dans une bande partagée avec d'autres utilisateurs.
- *Intégration avec les systèmes informatiques* – les entreprises disposent en général d'un certain nombre de systèmes informatiques anciens. Si l'on peut penser que certains fournisseurs de systèmes informatiques proposeront des solutions toutes prêtes pour résoudre ces problèmes de mise en œuvre, il est probable que l'intégration des systèmes RFID dans les systèmes existants risque d'être difficile, de prendre du temps et de coûter cher. Comme les informations sur les produits qui peuvent être générées au moyen d'un système RFID sont des données en temps réel, l'infrastructure informatique sera beaucoup sollicitée.
- *Articles difficiles à marquer* – les performances d'un système RFID dépendent beaucoup du type d'objets marqués et de l'environnement dans lequel l'objet doit être identifié. Ainsi, les objets à fort contenu métallique ou liquide absorbent en général une grande partie de l'énergie des radiofréquences émises par le lecteur, ce qui réduit considérablement la portée du système RFID.
- *Législation sur les radiofréquences* – les systèmes RFID fonctionnent en général dans des bandes de fréquences qui ne nécessitent pas de licences. Cela signifie que tant qu'un lecteur RFID respecte certains principes de fonctionnement de base, il peut être exploité sans licence spéciale de transmission radio. Les gouvernements nationaux sont en général responsables de la définition des parties du spectre qui sont libres d'utilisation, et parmi celles-ci, de celles qui sont adaptées aux systèmes RFID. Malheureusement, pour des raisons historiques, les gouvernements ne répartissent pas tous les fréquences de la même façon – en Amérique du

Nord, en Europe, en Afrique et en Australie, par exemple, les allocations de fréquences et les principes d'exploitation diffèrent légèrement. Au fil du temps, ces différences seront progressivement éliminées, mais c'est un processus long et, à court terme, il peut se poser des problèmes d'interopérabilité.

- *Recyclage des marqueurs* – si un marqueur RFID est véritablement intégré dans un article (et non pas simplement apposé sur le conditionnement de cet article, par exemple), cela peut poser un problème pour le recyclage ultérieur du produit. Les matériaux utilisés pour fabriquer le marqueur RFID (puce au silicium, antenne métallique) peuvent ne pas être compatibles avec le procédé de recyclage du produit, ce qui réduira l'efficacité de l'opération.

D'autres problèmes sont également concevables :

- *Questions de santé et de sécurité* – jusqu'à présent, le nombre de lecteurs RFID déployés est assez faible. Toutefois, à mesure que la situation évoluera et que les travailleurs et le grand public seront de plus en plus en contact avec cette technologie, on peut penser que l'on s'interrogera sur les incidences pour la santé et la sécurité de l'exposition aux ondes radio produites par les lecteurs. Il n'y a actuellement aucune indication de risque potentiel pour la santé humaine, mais comme pour l'exposition aux rayonnements des téléphones portables, il est important de continuer d'approfondir nos connaissances dans ce domaine.
- *Activité délictueuse* – avec le développement de la technologie, les opérations et procédés physiques sont progressivement remplacés par des opérations et procédés électroniques. Cela a notamment pour inconvénient que ces opérations et procédés risquent d'être davantage exposés à certains comportements délictueux. C'est ce que l'on observe par exemple avec la multiplication des courriers électroniques non sollicités et des virus informatiques, qui sont transmis relativement aisément et à faible coût via les supports électroniques qui ont remplacé les modes de communication physique des générations antérieures. De la même manière, on peut imaginer des scénarios dans lesquels des systèmes électroniques s'appuyant sur des informations obtenues par RFID pour gérer les activités des entreprises puissent être utilisés de façon malveillante au détriment de l'entreprise. Cela pourrait prendre la forme de trafic malveillant sur le réseau informatique, ou de manipulations intentionnelles du spectre des radiofréquences pour empêcher la collecte d'informations RFID ou même générer des informations RFID destinées à induire en erreur (RFID Journal, 2003c). De telles activités délictueuses pourraient être motivées par un désir de relever un défi intellectuel (comme c'est le cas pour de nombreux virus informatiques), par la recherche d'un gain commercial ou par le terrorisme.

- *Coût des composants RFID* – les marqueurs et lecteurs RFID vont sans doute continuer de voir leurs prix baisser à mesure que l'on améliore la technologie et les procédés de production associés. Toutefois, à court terme, il est probable que les coûts limiteront l'adoption de la technologie au marquage des objets les plus coûteux, tels que palettes et caisses de produits et articles de forte valeur, comme les appareils électroniques grand public.
- *Coût de l'intégration* – outre les coûts directs de déploiement de la technologie RFID, l'intégration avec les systèmes informatiques sera très coûteuse. Comme on l'a vu plus haut, les systèmes informatiques traditionnels ne sont pas conçus pour faire face à la production en temps réel d'informations au niveau de chaque article, et l'ajout de cette fonctionnalité sera coûteux.

5. Conclusion

Nous avons vu dans ce rapport les aspects fondamentaux du fonctionnement de la technologie d'identification par radiofréquences et les domaines d'application dans lesquels ces systèmes ont été traditionnellement utilisés. La technologie gagnant en sophistication, tandis que les coûts des composants baissent, il est clair que vont se multiplier les domaines d'application dans lesquels la technologie est rentable. De plus, la normalisation d'un certain nombre d'aspects de l'utilisation de la RFID rendra interopérables des systèmes déployés dans des branches différentes par des entreprises différentes, ce qui rendre encore plus rentable le déploiement de cette technologie, du fait de la mutualisation de l'usage d'une même infrastructure.

Le déploiement de la RFID sera sans doute à court terme le plus fort dans la chaîne logistique du secteur CPG (produits de grande consommation), pour permettre aux producteurs, aux entreprises de logistique et aux détaillants de suivre beaucoup plus précisément le mouvement des marchandises. Par ce biais, ceux-ci espèrent réduire les pertes, les erreurs de livraison, la démarque inconnue, etc. La plus grande chaîne de supermarchés du monde, Wal-Mart, poursuit une politique volontariste de déploiement de systèmes RFID selon des calendriers très serrés, ce qui va donc inciter ses fournisseurs à adopter également cette technologie. D'autres détaillants de même que des organismes gouvernementaux s'orientent également dans cette direction, ce qui va aussi encourager l'adoption de la RFID dans la chaîne logistique du secteur CPG.

Des amendements législatifs récents ou programmés dans un certain nombre de domaines vont sans doute également promouvoir l'adoption de la technologie RFID – soit parce que l'utilisation de cette technologie spécifique est imposée ou recommandée, soit parce que la RFID est tout simplement le

moyen le plus rentable de se conformer à la nouvelle législation. S'il existe des facteurs susceptibles de freiner l'adoption de cette technologie, comme les inquiétudes des consommateurs ou les coûts d'intégration des systèmes, il apparaît actuellement que l'adoption de cette technologie va sensiblement se développer à relativement court terme dans un certain nombre de domaines d'application.

Bibliographie

AIM GLOBAL WEBSITE, « JTC 1/SC 31 Automatic Identification and Data Capture Techniques, » *www.aimglobal.org/standards/rfidstds/sc31.htm*.

AUTO-ID CENTRE WEBSITE, Archive, *www.epcglobalinc.org*.

CHECKPOINT SYSTEMS INC. (a), « Radio Frequency Identification (RFID) – Performa Commercial/Industrial Products », *www.checkpt.com/content/rfid/commperf.aspx*.

CHECKPOINT SYSTEMS INC. (b), « Radio Frequency Identification (RFID) Success Stories: Checkpoint Offers Proven RFID Solutions ».

CHECKPOINT SYSTEMS INC. (c), « Checkpoint Intelligent Library System – Changing the Role of the Librarian ».

COLLINS, Jonathan (2003), « Perfecting Just in Time Production », *RFID Journal*, novembre.

COMMISSION EUROPÉENNE – JOINT RESEARCH CENTRE, « DRIVE – Drug in Virtual Enterprise », IST 12040.

DODSON, Sean (2003), « The Internet of Things: A Tiny Microchip Is Set to Replace the Barcode on All Retail Items But Opposition Is Growing to Its Use », *The Guardian*, 9 octobre.

ELIMA – Environmental Life Cycle Information Management and Acquisition, EU Growth Programme 2001-3.

EUROPA (2002), « Activities of the European Union – Summary of Legislations, Waste Management ».

EUROTAG NEWSLETTER (2003), « RFID Helps to Perfect Order Picking », avril-juin.

FINKENZELLER, K. (1999), « RFID Handbook », 1st edition, Wiley and Sons Ltd.

« FOOD TRACEABILITY REPORT » (2003), *CRC Press*, LLC, vol. 3, n° 4, mars.

HALLIDAY, Steve, « But Can't Bar Codes Do Everything I Want? », High Tech Aid.

HODGES, Steve et Mark HARRISON (2003), « Demystifying RFID: Principles and Practicalities », Technical Report CUED/E-MANUF/TR-028, Cambridge University Engineering Department.

INTERMEC (2002), « Intermec Poised to Take the Fast Lane in RFID », *www.intermec.com/cgi-bin/ASP/*.

JHA, Alok (2003), « Tesco Ends Trial of CCTV Spy Chip on Razor Blades », *The Guardian*, 22 août.

LANDT, Jeremy et Barbara CATLIN (Transcore) (2001), « Shrouds of Time: The history of RFID », publié par AIM, the Association for Automatic Identification and Data Capture Technologies.

McFARLANE, D. and Y. SHEFFI (2003), « The Impact of Automatic Identification on Supply Chain Operations », *International Journal of Logistics*, vol. 14, n° 1, pp. 1-17.

RFID JOURNAL (2003a), « RFID Touted for Drug Distribution », 10 novembre.

RFID JOURNAL (2003b), « Creating an RFID Privacy Plan », 26 mai.

RFID JOURNAL (2003c), « RSA Security Designs RFID Blocker », 28 août.

ROBERTI, Mark (2002), « RFID: From Just-In-Time to Real Time », CIO Insight, 12 avril.

STOCKMAN, Harry (1948), « Communication by Means of Reflected Power », Proceedings of the IRE (Institute of Radio Engineers), octobre, pp. 1196-1204.

VIOLINO, Bob (2004), « The Intelligent Warehouse », *RFID Journal*.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 5

Localisation par satellite : GALILEO

par

René Oosterlinck
Agence spatiale européenne*

* Les vues exprimées dans ce document n'engagent que son auteur et ne reflètent pas nécessairement celles de l'Agence spatiale européenne.

Dans tous les aspects de notre vie quotidienne – au domicile, sur le lieu de travail, dans les activités industrielles et au niveau des nations – la sûreté et la sécurité sont devenues des enjeux prioritaires.

Des recommandations et des mesures ont été proposées dans de nombreux domaines pour mieux répondre à ces préoccupations à l'échelle mondiale. L'un de ces domaines est l'utilisation des satellites. Il existe une catégorie d'appareils tout à fait distincte des satellites de télécommunications et des satellites d'observation de la terre, qui joue déjà un rôle important dans ces questions et pourrait à l'avenir avoir une importance stratégique pour la sûreté et la sécurité : les satellites du Système mondial de navigation par satellite (GNSS).

Le Système mondial de navigation par satellite

Le développement des transports modernes s'est accompagné d'un besoin de systèmes de navigation rapides et fiables. Plusieurs ont été créés dans le courant du XX^{e} siècle. Un petit nombre d'entre eux permettaient d'obtenir des données de navigation quelles que soient les conditions météorologiques et sur une grande partie du globe. Il s'agit des systèmes de navigation terrestre radio par triangulation (dotés d'émetteurs orientés vers des directions connues) utilisés comme moyen de localisation. Le système LORAN en est un exemple. Le problème est que ces émetteurs ne pouvaient bien sûr être placés que sur la surface de la terre, ce qui en limitait la couverture. De plus, la localisation ne pouvait être que bidimensionnelle, puisque l'altitude ne pouvait pas être établie. Cela excluait l'utilisation de ces systèmes dans l'aviation. Pour un système de navigation mondial tridimensionnel, le satellite était nécessaire. Comme les besoins de localisation étaient avant tout militaires, c'est donc ce secteur qu'a porté sur les fonts baptismaux le nouveau système mondial de navigation par satellite.

Le système mondial de navigation par satellite – Comment ça marche ?

Le GNNS s'appuie sur la triangulation tridimensionnelle. Une constellation de satellites gravitant autour de la terre sur plusieurs plans orbitaux (six pour le GPS et trois pour GALILEO), émet des signaux. Ces signaux contiennent tous un message d'identification indiquant quel satellite émet le signal, un éphéméride indiquant la position de tous les satellites exploités, et

enfin le plus important : l'heure exacte à laquelle le signal a été émis. Lorsqu'il reçoit la position d'un satellite donné, le récepteur – grâce à l'éphéméride – connaît la position de tous les autres satellites à cette heure précise.

Les signaux émis par les satellites se déplacent à la vitesse de la lumière et arriveront à des moments différents selon la distance entre récepteur et satellite. Lorsqu'un signal est reçu par un premier satellite, la distance peut être calculée. Le récepteur est alors localisé sur la surface d'une sphère dont le rayon est donné par la distance entre le satellite et le récepteur ; le satellite est le centre de la sphère. Lorsqu'un second satellite est détecté, il définira également une sphère dont il est le centre. Le récepteur est alors localisé quelque part à l'intersection des deux sphères, mais le point d'intersection exact ne sera connu que grâce à un troisième satellite et à la sphère correspondante.

En théorie, les signaux provenant de trois satellites distincts devrait suffire à déterminer la position du récepteur. Cette théorie supposerait que l'horloge du récepteur ait la même précision que les horloges embarquées des satellites, ce qui n'est pas le cas en pratique. Le décalage de temps constitue une quatrième inconnue ; un quatrième satellite est donc nécessaire pour calculer la position précise du récepteur.

La précision du système dépend d'un certain nombre d'erreurs inhérentes à ce système. Les principales erreurs tiennent au retard des signaux dans leur déplacement à travers l'ionosphère et la troposphère, à la précision des horloges embarquées, au bruit de fond et au multitrajet. Des corrections peuvent être apportées pour réduire ces erreurs – modèles de l'ionosphère (l'effet de l'ionosphère sur les signaux varie notablement d'un endroit à l'autre de l'ionosphère), conception spéciale des signaux, etc. Des mesures extrêmement précises sont réalisées grâce à l'utilisation d'éléments locaux, permettant une précision de moins d'un centimètre.

Le Global Positioning System (GPS)

Les États-Unis ont été les premiers à mettre en œuvre un système mondial de localisation par satellite. Le premier satellite GPS a été lancé en 1978, et très peu de temps après les chercheurs ont constaté que le signal du GPS d'acquisition grossière (code C/A) pouvait être utilisé à d'autres fins que la seule acquisition. Comme ce signal n'était pas crypté, n'importe qui pouvait l'utiliser. De nombreuses applications ont été développées et ont rapidement progressé en importance et en diversité. Prenant conscience de l'éventail des applications civiles, le président Reagan a annoncé qu'une partie des capacités GPS pourrait être mise à la disposition des utilisations civiles.

Donc officiellement, le GPS donne deux signaux : un signal extrêmement précis, réservé aux applications militaires et crypté et un signal librement

utilisable par quiconque. Jusqu'à une date récente, ce dernier signal n'était pas parfaitement fiable car, pour des raisons stratégiques, suivant la pratique de la dégradation volontaire (selective availability), un certain nombre d'erreurs étaient introduites délibérément, de manière diminuer la fiabilité du signal pour d'éventuelles utilisations « non amicales ». Les erreurs étaient changées constamment, relayant des informations fausses de synchronisation et de localisation des différents satellites. Ces erreurs réduisaient considérablement la précision du signal à accès libre. Et le 1er mai 2000, le président Clinton a annoncé la fin de la dégradation volontaire.

Bien que le GPS soit un système d'origine militaire, il a peu à peu évolué vers les applications civiles. D'ailleurs la loi actuellement en vigueur concernant le GPS, comprend deux volets : maintenance et exploitation à des fins militaires, et maintenance et exploitation à des fins civiles. Cette dernière partie prévoit en particulier les services standard de localisation pour les utilisations civiles, commerciales et scientifiques pacifiques, dans le monde entier, avec un niveau de continuité élevé, et sans coût financier direct pour l'utilisateur.

GLONASS

L'Union soviétique avait aussi développé un système militaire de navigation par satellite : le système GLONASS (Système mondial de satellites de navigation). Cette constellation, maintenant gérée par la Russie, a perdu beaucoup de ses capacités d'origine. Actuellement un très petit nombre de satellites sont opérationnels et, même si quelques projets existent, il est peu probable qu'ils voient le jour avant longtemps.

Dans sa conception initiale, la constellation GLONASS se composait de 24 satellites placés sur trois plans orbitaux, et avait le potentiel d'offrir une couverture mondiale.

Le programme GALILEO

L'objectif de GALILEO est de créer un système mondial de navigation par satellite (GNSS) européen autonome qui soit extrêmement précis et interopérable avec les autres systèmes existants (GPS et GLONASS). L'objectif européen d'accéder à une totale autonomie dans la navigation par satellite sera atteint en deux temps, à commencer par le déploiement du Système européen de navigation par complément géostationnaire (EGNOS) en 2004. Ce système a pour objet d'offrir un service civil en complément du GPS et de GLONASS. EGNOS améliore la précision de ces deux constellations et prévoit un système d'alarme en cas de mauvais fonctionnement de GPS et GLONASS (intégrité).

GALILEO, la deuxième étape, sera le premier système de navigation par satellite conçu pour des besoins civils, conçu et exploité sous contrôle public. Sa conception et son architecture sont donc déterminées en fonction d'une multitude d'utilisateurs et de services. Les questions de sécurité ont reçu une attention particulière, la priorité étant de protéger l'infrastructure et d'empêcher une utilisation malveillante de ses signaux.

Les raisons qui ont poussé l'Europe à construire le système GALILEO sont de trois ordres :

- *Stratégiques* : pour protéger les économies européennes d'une dépendance vis-à-vis des systèmes d'autres états qui pourraient à tout moment refuser l'accès aux utilisateurs civils, et pour améliorer la sûreté et la fiabilité.
- *Commerciales* : pour accroître les parts de marchés de l'Europe dans le marché des équipements des technologies connexes et des services à valeur ajoutée. Le rôle du GNSS est appelé à se développer considérablement dans l'avenir ; n'importe qui, situé n'importe où sur la planète pourra l'utiliser quotidiennement, et de nombreux services à valeur ajoutée seront proposés. Le maintien d'un monopole aux mains d'un seul État présenterait des risques d'abus de cette position, et se traduirait par une perte de compétitivité des économies européennes.
- *Macroéconomiques* : pour permettre des gains d'efficience pour l'industrie, procurer des avantages aux sociétés grâce à des transports moins chers, une circulation plus fluide et moins polluante, et stimuler l'emploi.

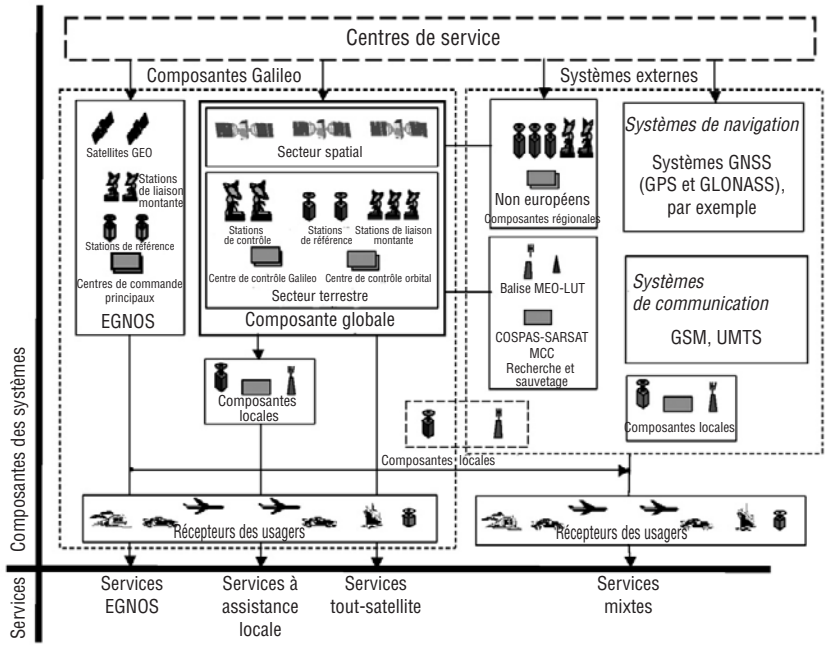
GALILEO – Architecture

GALILEO sera composé d'un réseau de communications mondial dédié qui produira les signaux électromagnétiques nécessaires pour des services tout-satellite. Il se composera d'un secteur spatial, d'un secteur terrestre et d'un certain nombre de centres de service. Le secteur spatial se compose d'une constellation de 27 satellites opérationnels plus trois satellites en réserve. Le secteur terrestre comprend un système de contrôle au sol pour les satellites en orbite et des stations terrestres de mission navigation pour le signal électromagnétique. Les centres de contrôle permettront de recueillir des informations et de garantir les performances et les données.

Des composantes régionales compléteront le système. Elles comprendront un secteur terrestre doté de stations terriennes réparties dans les différentes régions du monde pour assurer l'intégrité des données, reliées directement aux satellites ou reliées par l'intermédiaire du secteur terrestre de la composante mondiale à la liaison montante.

Des composantes locales sont aussi prévues pour optimiser les services tout-satellite par combinaison des signaux de GALILEO avec ceux d'autres

Figure 1. **Les composantes et services de Galileo**



systèmes GNSS ou non (GSM et UMTS). Ces composantes locales offriront des services améliorés aux utilisateurs et permettront le développement d'une large gamme d'applications.

Un système indépendant mais interopérable

GALILEO est conçu comme un système de navigation par satellite fonctionnant de manière indépendante mais pouvant être utilisé avec les autres systèmes, notamment le GPS.

Sa conception répond à trois grands objectifs d'interopérabilité :

- D'abord, assurer l'interopérabilité de GALILEO au niveau des récepteurs avec les autres systèmes GNSS (principalement le GPS), objectif que reflètent l'étude et le choix des fréquences, de la structure du signal, du cadre de référence temporel, et des données géodésiques.
- En outre, l'interopérabilité avec les autres systèmes non GNSS, comme les systèmes de navigation terrestre ou des réseaux de télécommunications mobiles, sera nécessaire pour permettre une réduction des défaillances du GNSS grâce à la fourniture de services de localisation combinés.

- Enfin, l'utilisation de GALILEO couplé avec les systèmes de télécommunications pour assurer des services combinés de navigation et de communication doit être optimisée. Il s'agit d'une fonctionnalité supplémentaire qui permet des communications améliorées (par exemple un débit de transfert plus élevé) et facilite la création de services GNSS à valeur ajoutée, comme les services basés sur le positionnement, qui occuperont une place importante sur le futur marché du GNSS.

Contrairement au GPS actuel, qui n'offre qu'un seul signal à usage civil, GALILEO produira plusieurs signaux, et assurera ainsi quatre services de navigation différents et un service pour les opérations de recherche et de sauvetage. Ces services ont été conçus pour couvrir les besoins d'une large palette d'usagers, à savoir les professionnels, les chercheurs, le grand public, la sûreté de la vie et le service public réglementé. Les services tout-satellite GALILEO suivants seront assurés dans le monde entier :

- *Le Service ouvert* (OS) fournit gratuitement en ensemble de signaux de positionnement et de synchronisation accessibles à tous, avec un niveau de performance équivalent à ceux des autres systèmes GNSS.
- Le *Service de sûreté de la vie (SoL)* offre des performances améliorées par rapport au service ouvert, avec des alertes immédiates pour l'utilisateur au cas où le système ne remplirait pas certaines exigences de précision (intégrité des données). Il est envisagé d'offrir une garantie de service.
- Le *Service commercial (CS)* se composera de deux signaux supplémentaires pour permettre un débit plus élevé et offrir aux utilisateurs une meilleure précision. Une garantie de service est prévue.
- Le *Service public réglementé (PRS)* offrira des données de positionnement et de synchronisation à des usagers spécifiques pour lesquels ils est nécessaire d'apporter un niveau élevé de continuité du service avec accès contrôlé.

Figure 2. **Service ouvert**

		Service ouvert (localisation)	
Type de récepteur	Porteuses	Mono- fréquence	Bifréquence[1]
	Calcul de l'intégrité	Non	
	Correction ionosphérique	Basée sur un modèle simple	Basée sur des mesures bifréquences
Couverture		Globale	
Précision (95 %)		H : 15 m V : 35 m	H : 4 m V : 8 m
Integrité	Limite d'alarme	Sans objet	
	Délai d'alarme		
	Risque d'intégrité		
Disponibilité		99.8 %	

1. La performance d'un service à trois porteuses est en cours d'évaluation.

Deux signaux PRS de navigation avec codes et informations de télémesure cryptées seront fournis.

- Le *Service recherche et sauvetage (SAR)* diffuse dans le monde entier les messages d'alerte reçus en provenance de balises de détresse. Il contribuera à améliorer le service assuré actuellement par le système de recherche COSPAS-SARSAT.

Figure 3. **Service public réglementé**

		Service public réglementé
Type de récepteur	Porteuses	Bifréquences
	Calcul de l'intégrité	Oui
	Correction ionosphérique	Basée sur des mesures bi-fréquences
Couverture		Globale
Précision (95 %)		H : 6.5 m V : 12 m
Integrité	Limite d'alarme	H :20-V:35
	Délai d'alarme	10 s
	Risque d'integrité	3.5 x 10-/150 sec
Risque de continuité		10-/15 s
Précision de la synchronisation w.r.t. UTC/TAI		100 nsec
Disponibilité		99.5 %

Applications de sûreté et de sécurité

Une centaine d'applications du GNSS ont été définies, dont beaucoup sont déjà, soit opérationnelles, soit en phase pré-opérationnelle. On peut s'attendre à ce que cette liste s'allonge dès que GALILEO sera en exploitation.

GALILEO est, à la base, un système de localisation et de synchronisation permettant à l'utilisateur d'établir sa position exacte à tout moment. Le système permettant une localisation dynamique, il pourra servir à guider l'utilisateur d'un point à un autre.

Toutefois, GALILEO lui-même n'est pas un système de localisation, hormis dans le service de recherche et de sauvetage. Il s'agit d'un système bidirectionnel dans lequel seul l'opérateur du récepteur sait où se trouve l'utilisateur. Pour de nombreuses applications de sûreté et de sécurité, cela ne sera pas suffisant. Il sera obligatoire de permettre également à des tiers de connaître la position ou le comportement dynamique de l'utilisateur. Pour ces applications, une combinaison de systèmes (notamment de communication) est donc essentielle.

Applications dans le domaine du transport

Comme nous l'avons déjà noté, GNSS est un système de localisation statique et dynamique ; on ne sera donc pas surpris qu'il trouve ses applications premières et principales dans le domaine des transports (presque tous les modes de transport : terrestre, aérien et maritime).

Applications routières

Les applications routières de GALILEO sont l'aide à la navigation routière, les opérations de gestion de flottes (taxis, camions, cars) et le guidage des véhicules. Parmi les aides à la conduite offertes, GALILEO assurera des fonctions d'amélioration de la sûreté et de la mobilité dans le cadre du trafic routier : alerte anti-collision, amélioration de la vision, aide aux manœuvres en faible vitesse, etc.

S'agissant de la sûreté et de la sécurité, une application importante est l'efficacité des interventions en cas d'accident. Le temps de réponse nécessaire pour que les services d'urgence arrivent sur place est très variable. Actuellement, la réaction dépend du contact téléphonique de l'utilisateur ou des équipements de détection intégrés dans l'infrastructure. S'il s'agit d'un appel par téléphone portable, la localisation d'un accident ou d'un incident ne peut pas être déterminée efficacement dans 40 % des cas.

La réactivité aux urgences est un impératif critique, d'une part pour sauver des vies et secourir les blessés, mais aussi pour enlever les objets qui font obstacle au trafic et maintenir sa fluidité. Un certain nombre de véhicules de tourisme sont maintenant équipés de détecteurs automatiques de collisions et de systèmes de localisation pouvant communiquer directement avec les centres de régulation des urgences. Ces systèmes ne nécessitent pas d'intervention du conducteur ; ils communiquent la position exacte du véhicule même s'il est dans l'incapacité d'agir. Faute d'une station centrale de contrôle, les véhicules d'urgence peuvent être équipés de systèmes de localisation indépendants permettant un déploiement des ressources précis.

GALILEO améliorera sensiblement les capacités de ces systèmes, allant jusqu'à préciser la file concernée par un incident donné.

Une autre application importante est la localisation et le contrôle du transport de matières dangereuses. Il sera possible de suivre de manière continue le transport de ces matières grâce à un récepteur GALILEO embarqué sur le camion, couplé à un émetteur qui envoie un signal à une autorité locale de sécurité. En cas de problème, cette autorité peut intervenir immédiatement en sachant précisément où se trouve le camion. Outre le positionnement du camion, il est possible de transmettre également à l'autorité de sécurité des informations sur les caractéristiques des matières dangereuses. Le système peut en outre être équipé d'un détecteur de vitesse, qui signale au chauffeur

du camion s'il dépasse la vitesse maximum autorisée et transmet simultanément l'information à l'autorité de sécurité.

L'Agence spatiale européenne a créé un service à base de positionnement intitulé AGENOS TRAN (Terrestrial Regional Augmentation Networks). Ce système se compose d'un centre de service situé à Rome d'où peut être suivi le positionnement des véhicules de transport de matières dangereuses. Ce centre de service communique par GPRS avec le véhicule, lequel est équipé d'un récepteur EGNOS et peut être assisté par le centre de service qui lui envoie des messages et des données EGNOS lorsque le signal électromagnétique EGNOS est momentanément perdu en raison de l'environnement (ville, région montagneuse, forêt, etc.).

Aviation civile

Dans le domaine de l'aviation civile, GALIELO sera utilisé dans les différentes phases de vol – guidage en vol, approche des aéroports, atterrissage (catégories I, II et III) – et pour le guidage au sol. GALILEO rendra des services appréciables dans les cas où l'infrastructure classique au sol (radars de mouvement à la surface) est absente ou insuffisante face à l'augmentation du trafic aérien.

Transport maritime

Dans le domaine maritime, GALILEO sera utilisé comme aide embarquée à la navigation pour toutes les formes de transport maritime, notamment la navigation océanique et côtière, l'approche des ports et les manœuvres portuaires, et le transport fluvial.

Transport ferroviaire

Le monde du transport ferroviaire bénéficiera également de GALILEO, avec des applications telles que le contrôle des trains, la supervision des trains, la gestion des flottes, la surveillance des réseaux ferrés et l'information des passagers. L'entreprise conjointe GALILEO a lancé, dans le cadre du 6^{e} programme cadre, une étude de démonstration (GADEROS). Cette étude consistera à explorer l'utilisation des caractéristiques GNSS d'intégrité et de sûreté de la vie en définissant un système par satellite de localisation des trains pour des applications de sécurisation des transports. Ces applications seront intégrées dans le Système de sécurité ferroviaire européen (ECTS).

Applications industrielles

L'un des domaines d'application de GALILEO est le génie civil : GALILEO sera le principal outil de relevé, et assurera une surveillance en continu de certaines structures (bâtiments, ponts, etc.).

Un deuxième domaine sera la surveillance de l'environnement. La combinaison de mesures environnementales spécifiques – GALILEO donnant le positionnement exact associé à chaque mesure – va considérablement améliorer la précision des images détaillées en 3D du plancher océanique dans les ports, les rades, les estuaires, les côtes et en mer afin de sécuriser les traversées et les opérations de dragage.

Une troisième utilisation sera la géodésie. Les géodésistes utiliseront des récepteurs GALILEO pour la surveillance de phénomènes géophysiques en mesurant le mouvement relatif de points de référence fixes ; les capteurs géodésiques pourraient être interfacés à d'autres équipements comme des caméras photogrammétriques, les radars à ouverture synthétique, des bathymètres, pour n'en citer que quelques uns.

Les services basés sur la localisation (LBS)

Les services basés sur la localisation sont tous les services dans lesquels les informations sur le positionnement de l'utilisateur sont combinées à un service à valeur ajoutée.

L'exemple classique est la personne qui demande comment se rendre à l'hôpital le plus proche. Le fournisseur de service compare la localisation de l'utilisateur avec celles des hôpitaux, qui figurent dans sa base de données. Il indique alors à l'utilisateur quel est l'hôpital le plus proche et comment s'y rendre. Ce service peut en plus donner des indications de guidage pendant tout le trajet, jusqu'à la destination finale. Les fournisseurs de services peuvent aussi orienter leurs clients vers des restaurants, des cinémas ou des parkings. Actuellement, ce type de lieux figure sur plusieurs cartes et guides, mais les indications s'avèrent bien souvent insuffisantes. Il est tout aussi important d'abord de savoir exactement où l'on se trouve que de d'être guidé en continu jusqu'à destination.

Beaucoup d'autres applications sont en cours de développement. L'assistance aux personnes handicapées en est une très importante.

Assistance personnelle à la navigation pour les mal-voyants

La lecture de plans pour mal-voyants dépend actuellement en grande partie d'une aide supplémentaire par rapport aux plans pour les voyants. Les plans tactiles sont utiles pour donner une idée générale d'un pays, d'une région ou d'une ville, mais ne permettent pas de bien rendre compte des rues et des lieux importants. À l'heure actuelle, les outils d'orientation par satellite ne permettent pas de bien guider les mal-voyants dans la rue car le signal est souvent perdu en raison des bâtiments élevés et d'autres obstacles. Cela peut se traduire par des erreurs de localisation de 30 ou 40 mètres. GALILEO permettra une meilleure couverture des zones urbaines et contribuera à offrir aux

mal-voyants un système de navigation amélioré. Grâce à des « éléments locaux », GALILEO améliorera et facilitera également la localisation à l'intérieur des bâtiments.

Un projet soutenu par l'ESA a déjà démontré la faisabilité d'un tel système en utilisant EGNOS, le précurseur de GALILEO. Un petit équipement portable donne à l'utilisateur des indications vocales, exactement comme un système de voiture – mais comme il pèse moins d'un kilogramme, il peut être porté sur l'épaule. Il peut servir à deux choses : guider l'utilisateur jusqu'à une destination et lui indiquer où il se trouve pendant qu'il se déplace. EGNOS offre la précision nécessaire au pilotage et à la navigation. Cet équipement comprend aussi un clavier en braille, un synthétiseur vocal et un accès Internet. Ce projet peut préparer le terrain pour GALILEO en démontrant les avantages de performances GNSS améliorées pour ces applications.

Assistance aux personnes souffrant de la maladie d'Alzheimer avec perte de mémoire

De nombreuses personnes souffrant de la maladie d'Alzheimer, aux premiers stades de la maladie, continuent de vaquer à certaines de leurs activités ordinaires : travailler, conduire, faire des courses. Un assistant numérique personnel (PDA) contenant des informations sur leurs habitudes et leurs destinations usuelles peut les aider à rester plus longtemps intégrés à la société et à résoudre des problèmes récurrents. Cet équipement aurait une interface simple dans laquelle l'utilisateur n'aurait qu'à cliquer sur une photo de la destination où ils souhaite se rendre, et une flèche directionnelle apparaîtrait à l'écran pour lui indiquer la direction à prendre. L'appareil pourrait aussi proposer des destinations en fonction de critères tels que l'heure, la localisation exacte et la direction de l'utilisateur, qui seraient fournis par GALILEO. Une personne souffrant de la maladie d'Alzheimer pourrait s'en servir pour retrouver sa voiture dans un parking. Une autre pour trouver l'arrêt où il prend d'ordinaire son autobus.

Protection de la personne et appels d'urgence

Des téléphones mobiles dotés d'un récepteur GALILEO intégré permettront de localiser précisément et immédiatement les personnes qui n'ont qu'une vague idée de leur localisation (ou qui l'ignorent complètement). Le délai d'intervention en cas d'appel de détresse serait alors nettement raccourci. Ce concept fait partie du développement du programme européen d'appels d'urgence E-112.

L'ESA développe actuellement, dans le cadre d'EGNOS TRAN, une application de protection de la personne. L'utilisateur communique avec un centre service situé à Rome grâce à un assistant numérique personnel équipé

d'un récepteur AGPS Cell Guide et d'une carte SIM GPRS. Ce service localise la personne sur demande ou en mode automatique. L'utilisateur envoie les données GPS brutes au centre de service, lequel suit le signal électromagnétique EGNOS et combine les données EGNOS avec celles de l'utilisateur afin de calculer une position EGNOS. La localisation est donc déterminée avec une précision de quelques mètres et l'assistance peut être mise en œuvre rapidement si nécessaire.

Surveillance et prédiction des catastrophes

Un objectif important de la protection civile est d'apporter une meilleure protection aux populations, à l'environnement et aux biens matériels. Cette fonction inclut la surveillance des catastrophes. GALILEO peut aider à surveiller les événements précurseurs de certains types de catastrophes, ce qui permet d'améliorer le temps de réaction. Par exemple, dans les zones sujettes aux inondations répétées, le niveau de l'eau et l'état des digues sont généralement surveillés. La précision de GALILEO, couplée aux données améliorées de localisation, optimiseront cette surveillance. La prédiction des séismes et la surveillance des volcans seront améliorées grâce à une transmission plus rapide des informations et des alertes.

Optimisation des opérations de secours aux sinistrés de catastrophes

Les brigades de pompiers seront aidées par GALILEO pour la gestion des flottes. En environnement urbain, des données de navigation et de trafic peuvent considérablement améliorer l'efficience de la flotte. La surveillance de la position des différents véhicules qui participent aux activités de sauvetage permettra une meilleure coordination des opérations, particulièrement lorsque (lors de catastrophes de grande ampleur) plusieurs services différents interviennent. Une bonne gestion des ressources et du personnel lors des opérations d'urgence améliorera leur efficacité et la sécurité des équipes de sauvetage. La position de chaque unité peut être suivie et des instructions adaptées peuvent être formulées et lui être communiquées à distance. La disponibilité particulièrement élevée de GALILEO dans des environnements difficiles – notamment à l'intérieur des bâtiments – en font un outil particulièrement adapté à ce type d'application.

La réduction de délai d'intervention est un facteur clé pour le succès de ces opérations. C'est plus difficile dans le cas de catastrophes de grande ampleur, où le suivi en temps réel et en continu des ressources est essentiel. GALILEO offre la précision et la fiabilité nécessaires.

L'utilisation d'hélicoptères en vol dans les opérations d'urgence nécessite généralement des procédures en vol très spécifiques qui nécessitent des

fonctions de navigation très précises et très exigeantes. Ici encore, la précision et la fiabilité élevées de GALILEO sont particulièrement appréciables et en font un élément essentiel du dispositif. L'atterrissage des hélicoptères sur un terrain difficile, en site éloigné ou sur le toit d'un hôpital peut être assisté par GALILEO, qui peut en même temps communiquer des informations à un centre de coordination pour optimiser les opérations.

Applications de maintien de l'ordre et d'établissement de la responsabilité

Pour empêcher des utilisations abusives du système, ou pour qu'il puisse être utilisé dans le contexte du maintien de l'ordre ou d'établissement des responsabilités, il est essentiel que les signaux reçus par les utilisateurs ne soient pas brouillés ou faussés et qu'ils soient parfaitement fiables. Pour cette raison, le signal commercial sera crypté et fourni avec un message d'intégrité et d'authentification. Pour profiter de cette fonction, l'utilisateur doit être certifié, ce qui suppose l'utilisation de la cryptographie à clé privée. Les signaux GALILEO contiendraient un message d'authentification nécessitant d'être décrypté par le récepteur. Seuls les messages authentifiés seraient utilisés. Les autres seraient automatiquement rejetés. Le message d'intégrité indiquerait le niveau de précision du système.

Un signal (service) spécifique à usage gouvernemental, intitulé PRS, est prévu. Le service PRS offrira un niveau de protection plus élevé que les autres services contre les éléments susceptibles de menacer le signal électromagnétique GALILEO.

Le besoin d'un Service public réglementé (PRS) ressort de l'analyse des menaces pesant sur le système GALILEO et de l'identification des applications d'infrastructures pour lesquelles la perturbation du signal électromagnétique par des terroristes économiques, des personnes malintentionnées, des agents subversifs ou des organisations ennemies porterait gravement atteinte à la sécurité nationale, au fonctionnement des services de maintien de l'ordre, à la sûreté ou à l'activité économique dans une zone géographique importante.

L'objectif du PRS est d'améliorer la probabilité d'une disponibilité continue du signal électromagnétique en cas de risque de brouillage, pour des utilisateurs et des récepteurs bien identifiés contrôlés par des autorités clés. Un certain nombre d'applications ont été retenues pour l'élaboration du cahier des charges du service RPS. Les principales applications sont au niveau européen des services de police (EUROPOL, autorités de réglementation des transports, douanes, OLAF) et des forces de maintien de la paix. En outre, le PRS peut servir à des applications spéciales jugées d'intérêt stratégique national dans certains États membres.

Les signaux du Service public réglementé seront diffusés sur des fréquences distinctes des autres services GALILEO tout-satellite, afin d'éviter le risque de perte le PRS au cas où l'accès aux autres services serait refusé localement. Il s'agira de signaux large bande résistants aux brouillages involontaires ou malintentionnés, et qui offriront par conséquent une meilleure continuité de service.

Conclusion

GALILEO permettra la création d'un grand nombre de services à valeur ajoutée, en particulier dans le domaine de la sûreté et de la sécurité. Il s'agira de services très puissants qui pourront sauver de nombreuses vies humaines et des biens matériels. Cela étant, on peut aussi considérer qu'ils sont trop puissants et susceptibles d'abus. Il importe par conséquent d'élaborer des mesures pour éviter les scénarios à la « big brother », mais tout cela est un autre sujet*.

* Voir en particulier Dee Ann Divis, « Saving private location » *GPS World*, 1er octobre 2003.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 6

Produits de sécurité : anatomie de la carte d'identité électronique italienne

par

Alfio Torrisi
Istituto Poligrafico e Zecca dello Stato S.p.A.
et
Luigi Mezzanotte
L.C. SISTEMIA
Italie

Synthèse

À l'heure actuelle, les gouvernements utilisent de plus en plus les réseaux de télécommunications et les systèmes de TI afin d'assurer efficacement de nouveaux services à leurs citoyens. Cela permet de baisser considérablement les coûts d'administration, tout en améliorant la qualité du service.

Après des mois de consultations et d'études, les parties prenantes ont fini par introduire officiellement un nouveau concept dans le Journal officiel italien n° 169 daté du 21 juillet 2000. La Carte d'identité électronique italienne (CIE) a été conçue pour assurer aux citoyens italiens de meilleurs niveaux de service et de sécurité dans leurs interactions avec tous les niveaux de l'administration : nationale, régionale et municipale. Ce document électronique a pour double objectif de répondre au plan d'administration en ligne et à la nécessité de faciliter les relations entre citoyens et administrations publiques. L'État a officiellement confié la production de la carte à l'Istituto Poligrafico e Zecca dello Stato S.p.A. (IPZS).

S'agissant de la plate-forme technologique de la CIE, l'État italien a opté pour une solution hybride, à puce et à lecture optique, utilisant à la fois un microcontrôleur et des technologies de mémoire optique.

La puce – bien connue en Europe pour certifier les transactions en ligne – contrôle l'accès aux services « d'administration en ligne ». Elle est conçue pour permettre l'identification et l'authentification électroniques et pour activer les liaisons aux Services nationaux (CNS). La zone de lecture optique, la technologie de carte la plus mature et la plus répandue dans les programmes publics d'identification, offre le plus haut niveau de résistance à la contrefaçon, d'intégrité des données et d'authentification, lisible à l'œil et à la machine. Enfin, elle garantit une traçabilité permanente de l'historique de la carte depuis son émission jusqu'à ses actualisations, et permet une série de services, grâce à une large capacité de mémoire.

La production, l'initialisation, la personnalisation et l'émission d'une carte sécurisée, multi-applications et multi-technologies exigent les niveaux de sécurité et de contrôle les plus élevés. Cela est d'autant plus important qu'il s'agit d'un système d'émission de cartes faisant intervenir plus de 8 000 collectivités locales.

Objectif

Les objectifs attendus de la CIE sont les suivants : 1) *sécurité,* pendant tout le cycle de vie de la carte – production, émission et phase d'utilisation – qui sert de document d'identité physique; 2) *fourniture de services,* pour assurer l'identification, l'authentification et l'accès à des ressources spécifiques sur réseau (administration en ligne), activer les services tant nationaux (santé, vote, sécurité sociale) que services locaux, en fonction des besoins et des impératifs des municipalités (transports, éducation); 3) *interopérabilité :* une carte unique utilisée dans tout le pays.

La solution adoptée

Structure du document

Le document se compose d'une carte plastique « hybride » au format ID1 comprenant, comme indiqué précédemment, une puce et une zone à mémoire optique. Les dimensions de la carte sont conformes au format standard décrit dans la norme ISO/IEC 7810:1995 pour les cartes d'identification sans embossage : longueur 53.92/54.03 mm, largeur 85.47/85.72 mm, épaisseur 0.68/0.84 mm.

Au recto de la carte, la zone supérieure contient des données personnelles et une photo du titulaire, et la zone inférieure – MRZ (zone lisible à la machine) de l'OACI – pour la lecture électronique des mêmes données, codifiées sur trois lignes et imprimées en caractères OCRB, lisibles avec des équipements appropriés.

Au verso, outre d'autres données personnelles, se trouvent une puce, une zone de lecture optique et un hologramme de sécurité (figure 1).

Impression

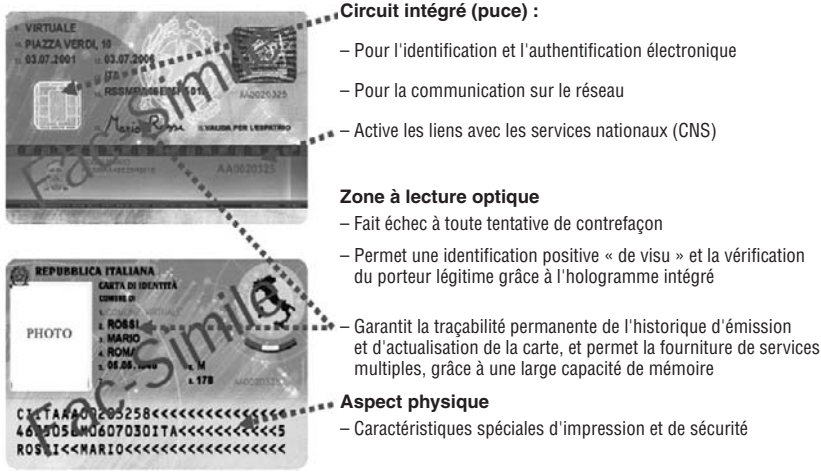
S'agissant des caractéristiques d'impression de sécurité présentes au recto de la carte, une bande bleue sépare la zone supérieure et la zone inférieure de la carte. Sur cette bande, se trouve une micro-impression (visible avec un agrandissement suffisant) portant les mots « REPUBBLICA ITALIANA ».

Au coin supérieur droit du document se trouve un élément à l'encre optiquement variable (OVI) représentant la carte de l'Italie. Cet élément imprimé, réalisé en sérigraphie, passe du bleu au violet selon l'angle où on l'observe en inclinant ou en déplaçant le document.

Un arrière-plan de sécurité, comportant deux éléments variables en bleu.

Au verso se trouve également un arrière-plan de sécurité associant une image en nuances de gris à un élément graphique bleu.

Figure 1. **Instruments (solution adoptée)**



Gravure au laser

Au recto de la carte, la première donnée personnalisée est le nom de la municipalité qui a émis le document. Cet élément est gravé au laser ; il diffère des autres éléments personnalisés par la profondeur de la gravure par rapport à la surface du papier. La même technique est utilisée pour l'inscription du numéro du document, qui apparaît au recto et au verso de la carte, dans la zone située au dessous de l'hologramme.

Au verso du document se trouve une micro-impression positive représentant le symbole de la République italienne : un élargissement de l'image fait apparaître en micro-impression les lettres « CIE ».

Le document comporte en outre un élément fluorescent invisible : éclairé par une lampe à UV, il apparaîtra de manière uniformément sombre, avec au centre une image rose représentant le globe terrestre et les lettres CIE au premier plan.

Hologramme de sécurité

Au dos du document, au coin supérieur droit, se trouve un hologramme métallisé à matrice de points combinant les techniques 2D et 3D. Si l'on approche l'hologramme d'une source de lumière (si possible halogène), on distingue au premier plan le symbole de la République italienne à l'intérieur d'un orbite ; l'étoile et la roue produisent un effet kinétique de contraction-expansion lorsque l'on change l'inclinaison de la carte. À l'arrière-plan, les mots « REPUBBLICA ITALIANA » sont répétés en continu en micro-impression.

Si l'on fait pivoter l'hologramme autour de l'axe horizontal, les couleurs de l'image varient.

Zone à lecture optique

La zone réservée à la mémoire (écriture et lecture par la technologie optique) se trouve au dos du document et se présente comme une ligne métallique horizontale. Le haut de la bande est une ligne de 3 mm sur laquelle le symbole de la République italienne est répété en continu entre deux éléments en guillochis. Sur la partie inférieure gauche de la bande se trouve en micro-impression le nom du producteur de la carte, Istituto Poligrafico e Zecca dello Stato. Sur la partie gauche de la zone à lecture optique se trouve un hologramme incrusté – réalisé au cours de la phase de personnalisation – reproduisant le numéro du document et la photo du porteur. Cet élément, tout comme l'hologramme, se voit mieux sous une source de lumière spécifique (voir figures 2 et 3).

La zone à lecture optique (LaserCard) est un support de technologie optique qui peut être inscrit et lu par faisceau laser avec les mêmes techniques que le disque compact ordinaire (CD-ROM). Le matériau utilisé est le polycarbonate, une matière plastique robuste utilisée pour les verrières d'intercepteurs à réaction mille fois plus résistante que le PVC, et qui n'est ni aussi toxique, ni aussi difficile à recycler que le PVC. La mémoire optique elle-même se compose d'un mince film de métal obtenu par un procédé

Figure 2. **Instruments (solution adoptée)**

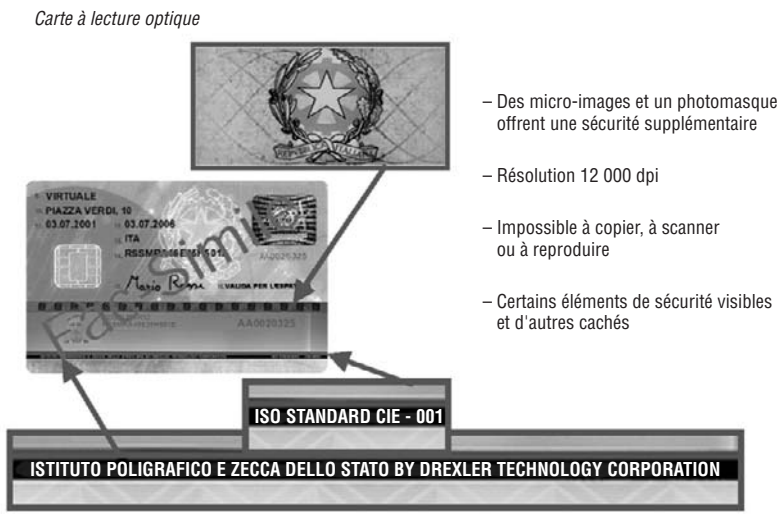


Figure 3. **Instruments (solution adoptée)**

Carte à mémoire optique

– Fonctionnalité unique dans la technologie des cartes
– Identification du porteur inscrite de manière indélébile dans la mémoire
– Support WORM ineffaçable et inaltérable
– Jusqu'à 16 partitions permettant des applications différentes
– Protection maximale des données privées
– Une partition réservée à l'identification
– Partitions libres pour les applications futures
– Protection des informations personnelles par code PIN
– Possibilité de stockage d'informations biométriques

photolithographique. L'enregistrement des données se fait par micro-perforation du substrat optique par un faisceau laser. Les normes de la zone à mémoire optique sont les suivantes: ISO 10 373-1/5, ISO 11693, ISO 11694. L'avantage de la zone à mémoire optique est d'offrir le maximum de sécurité contre la contrefaçon grâce à la technologie WORM (Write Once Read Many), qui permet l'actualisation d'informations ou l'ajout d'informations nouvelles, mais pas l'effacement ou la modification de données existantes.

Les normes de stockage sur cette zone sont 2.8 Mo pour le type à 35 mm (type adopté pour la Green Card américaine) et 1.0 Mo pour le type à 16 mm (type adopté par la EIC et par la Carte de résident permanent du Canada).

De cette manière, cette zone porte de meilleures informations biométriques que tout autre support portable, ce qui permet une vérification d'identité absolument fiable. Elle peut stocker les empreintes digitales (des dix doigts) pas seulement sous forme d'algorithme comme sur les microprocesseurs, mais sous forme d'image complète… même cryptée. Elle peut aussi être utilisée pour la reconnaissance de la voix, de la rétine ou de l'iris, de la main et du visage en 2D et 3D.

La zone à mémoire optique offre également une protection optimale de la vie privée.

Elle permet la vérification immédiate entre la carte et son porteur par comparaison biométrique, sans liaison avec une base de données. Les données personnelles stockées dans la mémoire de la carte sont également protégées.

La possibilité de vérification hors ligne est extrêmement intéressante en termes de sécurité, de rapidité et de réduction du coût de l'ensemble de l'infrastructure.

Évolutions récentes et perspectives

Le ministère italien de l'Intérieur, le ministère de l'Innovation et des Technologies et l'Association des maires d'Italie, ont présenté pour la première fois le Programme CIE.

La deuxième phase (après le succès d'une première phase pilote associant 83 municipalités qui ont délivré 170 000 cartes) consistera à délivrer 2.8 millions de cartes CIE dans 55 grandes, moyennes et petites municipalités, d'ici à la fin 2004. L'objectif du gouvernement italien est de munir le citoyen italien de sa carte d'identité électronique dans les cinq ans.

Des procédures ont été prévues pour le programme afin de garantir la sécurité, le respect de la vie privée, et l'optimisation technologique, tant pour les organismes d'émission que pour les citoyens.

La CIE servira, entre autres fonctions, d'instrument central du nouveau système national de sondage qui a déjà été expérimenté avec succès à Parme et Campobasso.

Enfin, les municipalités joueront un rôle crucial dans le système CIE, en assurant l'interface entre les citoyens et leurs institutions.

Services assurés

La CIE renfermera non seulement les informations personnelles démographiques et le code d'identification fiscale, mais aussi des informations de santé utiles en cas d'urgence, dans la mesure où la loi l'autorise. Elle pourra contenir d'autres informations, par exemple les données nécessaires pour générer la clé biométrique ou la signature numérique, ainsi que pour les sondages électroniques. Elle pourra aussi permettre les paiements électroniques des citoyens à l'administration publique.

Étant donné les multiples fonctionnalités et le niveau avancé de performance de la CIE, un ensemble de règles de sécurité et d'utilisation très strict a été conçu et adopté avant le début de la deuxième phase. Le gouvernement italien estime essentiel que tous les problèmes de sécurité, de vie privée et d'égalité entre citoyens et résidents étrangers soient pris en compte dans le cadre du programme CIE.

Processus de production

La procédure que doivent suivre les citoyens italiens pour obtenir leur CIE sera la même que celle en vigueur pour la délivrance du document d'identité

Figure 4. **Les acteurs impliqués : profil des sociétés**

L'Istituto Poligrafico e Zecca dello Stato S.p.A. (IPZS, l'équivalent de l'Imprimerie nationale et l'Hôtel de la Monnaie italiens) est l'organisme chargé de l'impression et de la distribution du Journal officiel et d'autres publications de l'État, sur supports classiques mais aussi sous des formats technologiquement avancés (en ligne et hors ligne). La Zecca participe également à l'élaboration et à la production de systèmes et de produits de sécurité anti-contrefaçon (cartes plastiques, hologrammes, papier officiel et papier monnaie, certificats d'épargne, timbres, plaques d'identification des véhicules, cartographie informatisée), tant pour l'administration publique italienne que pour des clients privés.

La Zecca est également éditeur d'art et de culture, et produit une large gamme de publications (notamment des fac-similés de manuscrits anciens), de littérature scientifique et juridique (revues trimestrielles de droit italien et européen), en format classique et multimédia.

Enfin, outre la frappe de l'euro pour le marché intérieur et la République de San Marin, la Zecca produit et fournit des médailles, décorations, sceaux, matrices et contreseings métalliques pour des organismes publics et privés. Elle fabrique également des pièces de monnaie et des billets pour le compte de pays étrangers.

papier, ce qui permettra de lui conserver un caractère simple et direct. Toutefois, la délivrance de la CIE suppose un jeu d'interactions complexes entre tous les niveaux de gouvernement – national, régional et municipal – et entre ces acteurs et des intervenants privés.

S'agissant du processus de production, il comprend quatre grandes phases impliquant des acteurs privés et publics.

Production de la carte

La phase de production fait intervenir des fabricants de microcontrôleurs (puces), un fabricant de bande laser (LCSistemia/Drexler – voir figures 4 et 5) et l'Istituto Poligrafico e Zecca dello Stato S.p.A. (IPZS). Dans cette phase, les fabricants de microcontrôleurs et de bandes laser fournissent leurs produits à la Zecca qui les intègre dans les CIE vierges et les stocke en attendant les demandes d'émission émanant desmunicipalités.

Phase d'initialisation

Cette phase fait intervenir les municipalités et la Zecca. Les autorités locales demandent les cartes nécessaires à la Zecca, laquelle doit alors :

- Initialiser le microcontrôleur et la structure de la carte laser.
- Installer les droits d'accès et privilèges du microcontrôleur.

- Générer le numéro de série de la carte d'identité.
- Imprimer les éléments constants et de sécurité.
- Intégrer l'hologramme dans la carte laser.
- Soumettre la demande d'émission au ministère de l'intérieur et attendre l'accord pour continuer.

Phase d'activation

Cette phase fait intervenir le ministère de l'Iintérieur, les municipalités et la Zecca.

Une fois reçu le feu vert du ministère de l'Intérieur, la Zecca inscrit la réponse du ministère dans sa base de données, fusionne le numéro de la CIE avec celui du gouvernement local et envoie le numéro ainsi obtenu au ministère de l'Intérieur. Enfin la Zecca envoie la « CIE vierge » aux autorités locales qui l'ont demandée.

Phase d'émission

Cette phase fait intervenir les mêmes acteurs que la précédente, auxquels s'ajoute le citoyen qui demande le document.

La municipalité :

- Réunit les données personnelles du citoyen (photo et autres informations d'identité).
- Génère la clé publique/privée de la carte et le code PIN de l'utilisateur.
- Envoie une demande de certificat CIE en format PKCS#10 (= IEIC ID + IEIC Kpub + données personnelles cryptées) au Ministère de l'intérieur et attend le « bon à tirer » final.

Figure 5. **Les acteurs impliqués : profil des sociétés**

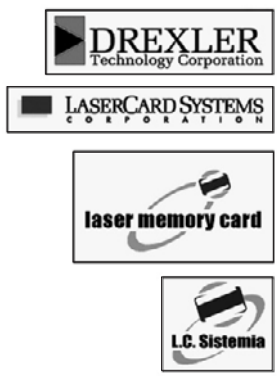
– **Drexler Technology Corporation** a crée les cartes à mémoire optique en 1981, et possède actuellement plus de 50 brevets américains dans le domaine de stockage optique de données.

– Le centre de fabrication de Drexler Technology, situé à Mountain View (Californie), a une capacité annuelle de production maximum de 25 millions de cartes.

– **LaserCard Systems Corporation** a été fondée par Drexler Technology en 1991 pour développer, commercialiser et vendre des systèmes à cartes optiques.

– La société italienne **Laser Memory Card S.r.l.** est depuis 1994 le partenariat le plus représentatif.

– **L.C. Sistemia S.p.a.** est le seul fabricant européen de lecteurs/graveurs de cartes mémoire optique et de cartes mémoire.



- Inscrit les données personnelles et le certificat CIE dans le microcontrôleur et la carte laser.
- Active les services nationaux sur les puces.
- Installe les annuaires nationaux.
- Active les services locaux sur les annuaires locaux de la puce.
- Imprime les données personnelles sur la CIE blanche.
- Imprime le code PIN de l'utilisateur.
- Délivre la CIE au citoyen.

Autres applications

Permis de conduire européen

À partir de 2005, l'UE va uniformiser les permis de conduire en créant un nouveau type de cartes plastiques auxquelles les pays pourront, s'ils le souhaitent, ajouter une puce pour y stocker davantage d'informations. Cette mesure vise non seulement à empêcher les fraudes, mais aussi à harmoniser les règles en matière d'examens médicaux et de contrôle de la vision pour les conducteurs âgés, ainsi qu'à imposer des exigences minimales de qualification et de formation initiales des examinateurs du permis de conduire, cela afin de faire converger les examens de conduite dans l'ensemble de l'Union européenne.

Permesso di Soggiorno (Permis de séjour)

Outre l'émission de la CIE, le gouvernement italien envisage de créer un Permesso di Soggiorno Elettronico pour les personnes non originaires de l'Union européenne qui résident en Italie. Cette carte sera technologiquement équivalente à la CIE, avec microcontrôleur et carte à mémoire optique. Elle assurera le même niveau élevé de sécurité. Ce document portera les informations d'identité du citoyen et le certificat d'authentification qui permettra l'identification en ligne. Le Permesso di Soggiorno Elettronico permettra aux personnes non originaires de l'Union européenne résidant en Italie d'accéder aux services assurés par les administrations par voie électronique, et facilitera la tâche des services de police.

Pour résumer, en optant pour une solution hybride pour ses nouvelles cartes d'identité, le gouvernement italien a fait le choix de la sécurité maximum et de la multifonctionnalité.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 7

Économie de la sécurité : arbitrages économiques*

par

Tilman Brück
Département d'économie internationale
Institut allemand de recherche économique (DIW, Berlin)
Allemagne

* L'auteur remercie pour leurs utiles commentaires Reza Lahidji, Patrick Lenain, Barrie Stevens et les participants du Forum de l'OCDE sur l'avenir consacré à « L'économie de la sécurité : quels arbitrages dans une société ouverte et mobile ? », qui s'est tenu le 8 décembre 2003 à Paris. L'assistance fournie par Till Stowasser pour les recherches a été précieuse. Les clauses déclinatoires habituelles s'appliquent.

1. Introduction

Le monde semble moins sûr depuis le 11 septembre 2001. Différents risques sont visibles, remarqués ou craints davantage depuis ces attentats meurtriers perpétrés à New York et Washington. Parmi ces risques figurent le nouveau terrorisme mondial, les grandes pannes totales d'électricité, les conflits du Moyen-Orient, une recrudescence des virus, vers et publipostages informatiques non sollicités, les attentats perpétrés par des tireurs fous, la fraude sur les achats électroniques, les attentats à l'anthrax, les grèves touchant la distribution de carburants et l'instabilité financière internationale.

La présente contribution aborde quelques concepts économiques communs à l'analyse de ces « nouvelles » sources d'insécurité et propose quelques recommandations d'action pour la nouvelle économie de la sécurité. L'analyse repose sur une définition large du risque englobant les risques sociaux et privés et les biens publics et privés adaptés à la réduction des risques. Ce chapitre aborde les principaux arbitrages à opérer et suggère des instruments d'action adaptés à la prise en compte de ces arbitrages. Sa conclusion est que les répercussions indirectes des actions des agents privés et des pouvoirs publics sont supérieures aux coûts directs de l'insécurité. Néanmoins, il n'existe pas de concept unique d'affectation optimale des risques et de la sécurité. Les responsables doivent définir un éventail d'instruments d'action permettant de diminuer, gérer et indemniser l'insécurité.

2. Les caractéristiques de l'économie de la sécurité

Définition de l'économie de la sécurité

La notion de « risque » peut revêtir plusieurs sens économiques. Tout d'abord, le risque décrit la possibilité qu'un événement survienne ou découle d'une situation. On peut citer comme exemple la probabilité qu'un chèque soit refusé pour manque de provision sur le compte ou qu'un émetteur frauduleux de chèques soit repéré. Dans le cadre du présent travail, ces risques entraînent habituellement des dommages importants.

En second lieu, le risque fait référence à la variation, à la variance ou à la volatilité d'indicateurs économiques tels que les taux de change ou la rentabilité future d'investissements. Ces fluctuations peuvent entraîner des coûts pour certains acteurs économiques.

Troisièmement, le risque peut être défini comme un indicateur proche d'un seuil, avec, là aussi, des coûts ou des dommages induits. Il s'apparente alors au concept de vulnérabilité. Prenons l'exemple du taux de croissance du produit intérieur brut (PIB). Si ce taux tombe au-dessous de zéro pour cent pendant une ou deux périodes, on peut dire de l'économie qu'elle est en récession même si, avant et après, elle a connu une forte croissance. Une économie progressant à un taux moyen nettement inférieur mais toujours positif tout au long de ces périodes n'aurait, elle, pas connu de récession. Les coûts d'une fluctuation donnée dépendent donc de la distance par rapport à un seuil.

Ces formes de risque sont, à divers degrés, d'ordre intrinsèquement privé. Par conséquent, l'analyse de l'économie de la sécurité et les politiques applicables en la matière diffèrent de l'analyse de la sécurité nationale et des politiques afférentes. La sécurité nationale est un exemple parfait de bien public – un bien dont la consommation ne donne pas lieu à rivalité, dont chaque citoyen peut jouir pleinement sans restreindre la consommation d'autrui, et qu'il est en outre impossible de ne pas fournir à la population. Dans l'analyse ci-après de l'économie de la sécurité, la distinction entre bien privé et bien public aura son importance.

Dans le présent chapitre, l'insécurité est définie comme une forme agrégée et non quantifiable des risques. Il existe différentes sources de risque, et donc d'insécurité, pour l'économie : forces naturelles, mondialisation, évolutions technologiques, sociales et politiques d'un côté ; forces économiques ou du marché de l'autre. Les premières pourraient être considérées comme exogènes par rapport aux mutations économiques, au moins à court terme ou telles que les considèrent les agents économiques individuels. Le réchauffement de la planète, l'amplification des migrations internationales, les innovations techniques telles qu'Internet ou les communications sans fil, et les événements politiques tels que les guerres et le terrorisme, qui génèrent de l'insécurité économique, peuvent en être des exemples. Les secondes sont endogènes par rapport au processus décisionnel économique et peuvent subir jusqu'à un certain point l'influence d'agents isolés. Citons par exemple les fluctuations des marchés boursiers, l'inflation ou les contrats d'assurance.

Cette distinction entre menaces exogènes et menaces endogènes soulève deux points importants. Premièrement, la classification d'un risque donné dans l'un ou l'autre groupe peut varier selon l'observateur, ce qui a des répercussions importantes. Deuxièmement, selon le type de menace ou de risque envisagé, ce sont des recommandations différentes qui s'ensuivront pour l'action sécuritaire publique, par exemple préventives (*ex ante*) ou au contraire compensatoires (*ex post*).

Dans le cadre du présent chapitre, l'économie de la sécurité sera définie comme l'ensemble des activités de prévention, de prise en charge et d'atténuation de l'insécurité de la sphère économique. Une définition aussi large inclurait les activités privées et publiques des secteurs tant licites qu'illicites de l'économie. Des versions plus restrictives de cette définition (mettant l'accent sur les dépenses de l'État pour la sécurité intérieure ou sur les dépenses privées en équipements anticriminalité) pourront être adoptées par d'autres auteurs dans d'autres contextes.

Périmètre de l'économie de la sécurité

Il n'est pas facile de mesurer un secteur de la sécurité d'acception si large à l'aide de concepts économiques standards. Pour commencer, toutes les mesures de la sécurité ne se traduisent pas par une hausse de coûts ou de dépenses, ce qui rend très difficile la mesure par les économistes des aspects non financiers du secteur de la sécurité. De plus, le risque de double comptabilité de certains postes de dépenses est grand : par exemple, un dispositif antivol intégré à une automobile peut être considéré comme une dépense de sécurité privée et une dépense automobile privée. Ainsi, la plupart des estimations des dépenses de sécurité sont soit extrêmement discutables et imprécises, soit trop étroites et spécialisées pour permettre une extrapolation des tendances de l'ensemble des dépenses de sécurité. La plupart des études portant sur les répercussions de l'économie de la sécurité reposent sur des hypothèses dont on retrouve fortement la trace dans les conclusions.

Les dépenses privées du secteur de la sécurité pourraient comprendre la consommation et les investissements sécuritaires des ménages et des entreprises (systèmes d'alarme, coffres-forts, systèmes de surveillance ou gardiennage). Sur un plan plus large, les primes d'assurance pourraient aussi être considérées comme des dépenses de sécurité dans la mesure où elles représentent une réaction essentielle du marché à l'existence de risques. Les dépenses sécuritaires publiques pourraient ajouter la consommation et les investissements de nature civile (programmes d'éducation, de prévention ou de protection) aux dépenses de sécurité de nature judiciaire, policière et militaire (telles que les dépenses de personnel ou d'équipement nouveau dans ces domaines). En outre, le législateur peut agréer de nouvelles règles en matière de sécurité (par exemple dans le domaine de la protection des données ou des droits civiques) qui peuvent avoir des conséquences économiques importantes sans être directement mesurables par des catégories ou des concepts financiers tels que les temps passés (Hobijn, 2002).

Certaines estimations valorisent le chiffre d'affaires annuel total du secteur de la sécurité à plus de 100 milliards d'USD (voir par exemple Stevens, 2004, dans le présent ouvrage). La plupart de ces dépenses sont le fait des États-Unis, dont le montant avoisinerait, selon une estimation, 40 milliards

d'USD (Lenain *et al.*, 2002). D'autres pays de l'OCDE ont un secteur de la sécurité non négligeable mais plus restreint : il serait par exemple d'environ 4 milliards d'EUR en Allemagne, et de 3 milliards d'EUR en France et au Royaume-Uni. Les taux de croissance annuels mondiaux enregistrés pour ce secteur semblent atteindre 7 à 8 % en moyenne, c'est-à-dire bien plus que les taux de la croissance économique (Stevens, 2004). Il n'est pas même certain que l'essor de l'économie de la sécurité reste aujourd'hui rapide – ambivalence qui s'explique par le fait, essentiel, que toute hausse des risques comporte deux effets opposés au niveau des dépenses de sécurité : d'une part un effet de substitution qui renforce la demande de diminution des risques, et d'autre part un effet de revenu consécutif au ralentissement économique général provoqué par le risque et se traduisant par la baisse du pouvoir d'achat de services de cette nature.

La disponibilité de données relatives aux dépenses du secteur public est meilleure. Mais celles qui concernent la sécurité souffrent des mêmes problèmes de délimitation que les dépenses sécuritaires privées. Les données disponibles varient donc considérablement. Dietz (2002), par exemple, calcule que le gouvernement allemand, en 2000, a consacré 52.1 milliards d'EUR (soit 2.5 % du PIB) aux questions de sécurité.

3. Les répercussions de l'économie de la sécurité

Nous détaillerons dans cette partie quelques-uns des effets économiques de l'insécurité elle-même et certains des effets des mesures prises face à l'insécurité. Il importe d'opérer cette distinction dans la mesure où la majorité des coûts engendrés par l'insécurité peut provenir non pas des risques eux-mêmes, mais des réactions de la population et des pouvoirs publics à la perception de tels risques. Nous aborderons en outre l'ampleur de ces deux catégories d'effets.

Les retombées de l'insécurité sur l'économie

L'insécurité impose des coûts à ceux qui ont une aversion pour le risque. La plupart des agents économiques préféreraient un monde affecté de moins d'insécurité ou de risques, et sont prêts à payer pour une réduction des risques. Pourtant, les coûts de l'insécurité sont triples : on a ainsi, premièrement, les coûts directs résultant de l'*événement* sous-jacent lui-même ; deuxièmement, les coûts indirects primaires induits par les réactions des *agents* à la menace ; et troisièmement, les coûts indirects secondaires induits par les réactions des *pouvoirs publics* à l'événement et aux réactions des agents.

Parmi les effets directs de l'insécurité figurent les dommages subis au niveau de la propriété, de la production, de l'usage, de la santé ou de la vie en raison d'événements tels que le vol, la fraude, les virus informatiques, les

coupures d'électricité ou le terrorisme. Les effets négatifs primaires comportent les réactions des parties directement touchées, comme par exemple des mesures de précaution informatique prises par une entreprise visée par des virus, ou les dépenses de retour à la normale après une situation de crise. Les effets indirects secondaires comportent les coûts des mesures mises en œuvre par les pouvoirs publics en réaction aux risques réels ou perçus : politiques économiques ou réactions politiques plus générales aux menaces et à l'insécurité.

La stabilité financière internationale qui a suivi le 11 septembre 2001 illustre clairement ce point. Les marchés mondiaux de capitaux sont très liés les uns aux autres. La nouvelle des attentats s'est propagée rapidement et a fait tâche d'huile. La forte volatilité et l'instabilité potentielle des marchés financiers créant des risques pour d'autres agents économiques, les autorités américaines ont fermé les marchés financiers durant quatre séances boursières. Malgré tout, les marchés de capitaux des États-Unis et d'autres grandes places se sont montrés bien plus adaptables que prévu. Dans le monde entier, les cours des actions ont lourdement chuté, mais pour un temps seulement. Par exemple, l'indice Dow Jones a retrouvé son niveau antérieur aux attentats en 40 séances seulement.

Une récente étude empirique de la réaction des marchés de capitaux aux cataclysmes a conclu que les marchés de capitaux américains avaient, ces cinquante dernières années, amélioré leur réactivité (Chen et Siems, 2004). Cette évolution peut s'expliquer par l'efficacité renforcée des secteurs bancaire et financier, qui fournit les liquidités nécessaires à la stabilité des marchés. La rapidité et la bonne coordination des autorités monétaires internationales ont contribué à stabiliser le système financier mondial. Ce n'est pas, apparemment, que les événements plus anciens aient été plus dramatiques que les plus récents, mais plutôt que l'économie n'avait pas été capable de surmonter correctement les crises. Cette observation montre bien que le mode de prise en charge, et non pas seulement la nature du cataclysme, détermine les conséquences de ce dernier.

Les retombées sur l'économie des réactions à l'insécurité

C'est la multitude d'effets indirects des risques, qui prennent la forme de changements dans les préférences, informations, perceptions, modes de comportement, incitations, modes d'organisation économique et politiques économiques et sécuritaires, qui domine les coûts de l'insécurité.

Pourtant, ces réactions ne sont pas toujours justifiées, même si elles sont volontaires, car le niveau d'insécurité est une question de perception. Il est extrêmement difficile d'évaluer les risques réels, non seulement parce qu'il existe peu de données dignes de foi, mais encore parce qu'on s'aperçoit bien

que la population, et par extension les décideurs, sont de mauvais juges du niveau objectif de risque. En particulier, lorsque des émotions fortes telles que la peur entrent en jeu, les individus ont tendance à se focaliser sur les pires scénarios plutôt que sur la probabilité de survenance. Du coup, les agents surestiment les risques mineurs ou font au contraire fi de risques indéniables (Sunstein, 2003).

Par ailleurs, la représentation publique de l'insécurité est tout à fait biaisée. Les accidents d'avion, par exemple, ont une couverture médiatique plus forte que les accidents automobiles mortels, alors qu'ils font moins de victimes. Pour ces deux raisons, on peut estimer que le secteur privé et les pouvoirs publics vont trop loin en matière de mesures et de législation sécuritaires, de sorte que les coûts peuvent aisément dépasser les avantages de la sécurité.

Les effets indirects primaires : la réaction de l'agent

Le niveau des dépenses sécuritaires du secteur privé est un élément clé de la nature des effets indirects primaires. Ces dépenses peuvent refléter le désir sous-jacent de protéger la production ou d'améliorer les produits d'une entreprise ; elles sont alors facultatives ou consenties en réaction à des forces du marché. Mais elles peuvent aussi être rendues obligatoires par une nouvelle législation sécuritaire. Cette distinction a un impact sur la compétitivité des entreprises.

Dans le premier cas, les entreprises décident de consacrer de l'argent à la sécurité à court terme de manière à réduire les coûts à long terme (par exemple en renforçant la sécurité pour éviter ou dissuader les incendies, les vols ou les attentats terroristes). De telles dépenses sont de nature assurantielle et témoignent de l'information, de la perception et des préférences de l'entreprise. On peut dire des entreprises qui engagent ces dépenses qu'elles s'auto-assurent contre certains risques. Il est probable que certaines d'entre elles auront des coûts plus élevés que d'autres, en fonction par exemple de leur éventuelle implantation dans des zones à haut risque.

Dans le deuxième cas, les entreprises réagissent à la demande du marché, par exemple parce que les salariés exigent de leur employeur qu'il prenne des mesures de sécurité (un exemple est la protection du personnel expatrié très exposé au risque) ou parce que les produits d'une entreprise nécessitent une sécurité accrue (c'est le cas des systèmes d'alarme des véhicules automobiles). Dans ces exemples, les coûts progressent, mais le chiffre d'affaires peut croître lui aussi ou ne pas baisser. Sur un marché donné, de telles mesures peuvent impliquer de nombreuses entreprises, même si certaines d'entre elles pourront choisir de fournir moins de sécurité, et donc des produits de moindre qualité, pour investir ainsi un segment différent du

marché. On peut de cette manière créer un niveau intermédiaire de différenciation par les coûts.

Dans le troisième cas, les entreprises ont l'obligation légale de mettre en œuvre certaines mesures de sécurité (par exemple les compagnies aériennes desservant les États-Unis). Dans ce cas, les dépenses sécuritaires supplémentaires s'apparentent à une réglementation environnementale, qui rehausse les coûts sans augmenter les profits des entreprises. Ces dépenses ont pour objectif de renforcer le bien-être social, mais sont à la seule charge des entreprises dans un premier temps. Elles ont pour conséquence un recul de la productivité du secteur concerné, ainsi que l'émergence parallèle de nouveaux secteurs répondant aux nouveaux besoins sécuritaires – comme on a pu le constater dans le secteur des services environnementaux. Dans une économie fermée, ceci implique que les coûts sont supportés uniformément par toutes les entreprises d'un secteur donné, ce qui n'est pas possible à l'échelle internationale et soulève d'importantes questions de politique commerciale.

Ce troisième cas contraste par ailleurs avec l'imposition d'une nouvelle taxe à un secteur. Les taxes réduisent aussi la productivité et peuvent toucher certaines entreprises de manière uniforme. Cependant, elles ont pour conséquence majeure d'augmenter les recettes fiscales, qui peuvent ensuite être affectées à d'autres prestations sociales ou à l'indemnisation d'autres agents. Aussi, dans le cas de l'imposition, le secteur imposé et le secteur à risque peuvent différer, tandis que dans le cas des dépenses publiques sécuritaires, les deux secteurs se confondent nécessairement. Dans ce dernier cas de figure, les secteurs menacés peuvent donc être touchés deux fois par l'insécurité nouvelle : une première fois par le risque lui-même et une deuxième fois par la contrainte légale associée. Selon les circonstances, ce constat peut conduire à dissocier les mesures de sécurité de leur financement, de manière à réduire le fardeau que représentent les nouvelles mesures.

Pour illustrer la gravité des effets indirects primaires pour l'économie, il convient d'examiner quelques répercussions possibles.

Une hausse de l'insécurité (due par exemple à des attentats terroristes) peut entraîner la modification des filières d'approvisionnement, et donc la réduction des avantages des processus de production en flux tendu. Les entreprises peuvent aussi décider de s'approvisionner auprès de fournisseurs locaux si ces derniers sont moins soumis à certaines formes d'insécurité. Ces fournisseurs locaux peuvent être plus fiables, mais aussi plus chers. À longue échéance, ces pressions sur les coûts peuvent entraîner différents changements, comme par exemple un gonflement des stocks, des investissements dans de nouvelles technologies ou la modification de l'équilibre de l'intégration horizontale ou verticale (Sheffi, 2001 ; Hodges et McFarlane, 2004, dans le présent ouvrage).

Parmi les autres effets indirects d'une hausse de l'insécurité figure l'augmentation des coûts transactionnels liés à l'exercice d'une activité commerciale, et notamment des coûts de transport et d'assurance du transport. Cette augmentation a pour corollaire un recul des flux commerciaux et des secteurs du transport et du tourisme sur le plan tant intérieur qu'international. Le déclin des échanges peut réduire l'essor de l'activité économique et renforcer le cloisonnement géographique. Or, plus une économie est cloisonnée, et plus elle constitue une cible intéressante pour, par exemple, des terroristes, ce qui renforce l'insécurité.

En fait, les violences de grande ampleur touchent les villes de trois manières. Premièrement, l'effet « sphère de sécurité » incite les individus à la concentration dans l'espoir de mieux se défendre face aux attaquants, ce qui rend les villes plus attrayantes en période de recrudescence de la violence. En second lieu, l'effet-cible fait des villes des objectifs plus tentants pour les auteurs de violences, ce qui incite à la dispersion. Troisièmement, l'effet-transport laisse supposer que, dans la mesure où le terrorisme cible souvent des moyens de transport, la violence est susceptible d'accroître le coût réel du transport, ce qui renforce habituellement la demande de densité. Toutefois, l'étude empirique des guerres et des villes au XX^{e} siècle donne à penser que les effets des guerres ou du terrorisme sur la sphère urbaine ne sont pas significatifs. Cela dit, il existe des exceptions de taille, notamment dans des situations extrêmes telles que les villes en temps de guerre (Glaeser et Shapiro, 2001).

De manière générale, si l'insécurité se nourrit de l'ouverture du monde, les entreprises et les ménages ont tendance au repli. À titre d'exemple, le commerce électronique recule lorsque sévit la fraude en ligne, et l'externalisation internationale diminue en présence de soulèvements civils périodiques, de blocages routiers ou de grèves à l'étranger. L'évolution des prix relatifs qui résulte de l'insécurité entraîne une réaffectation non optimale des ressources. L'économie souffrant d'insécurité affiche donc une croissance du PIB plus faible que celle à laquelle elle parviendrait dans des circonstances plus favorables (Lenain *et al.*, 2002).

Par ailleurs, la hausse des niveaux de risque sape la confiance des investisseurs et diminue leur propension à engager de nouveaux projets. Avec le temps, la hausse des primes de risque fait augmenter les exigences de rentabilité des investissements, ce qui pèse sur le cours des actions et fausse les décisions d'investissement au détriment des investissements de long terme à haut risque et haute rentabilité et au profit d'investissements de court terme à faible risque et faible rentabilité. Les effets cumulés de ces ajustements de portefeuilles sont des changements dans la composition de ces derniers, une diminution de l'investissement global et un retard de la poursuite de la croissance économique. Néanmoins, les marchés suscitent

aussi, par ricochet, des effets positifs prenant la forme d'évolutions structurelles au profit des produits et services qui s'occupent sérieusement de la sécurité (Brück, 2002).

Les effets indirects secondaires : réactions des pouvoirs publics

La loi américaine portant sur la prohibition de l'alcool qui a été en vigueur de 1920 à 1933 peut servir d'exemple de diminution perverse de la protection sociale par une intervention étatique bien intentionnée. Il est empiriquement difficile de savoir si la réglementation publique en matière de sécurité est elle-même productrice, généralement, d'insécurité. Le phénomène peut théoriquement se produire à deux niveaux. Tout d'abord, la densité réglementaire croissante, même si elle a pour objectif de renforcer la protection de la société, peut être un élément d'insécurité dans la mesure où elle augmente l'incertitude pour les entreprises qui opèrent dans un environnement aux obligations légales nouvelles. En second lieu, certains types de réglementation peuvent susciter des réactions illégales génératrices d'insécurité. Par exemple, la « guerre » que mènent les États-Unis « à la terreur » et la « doctrine Bush » peuvent, à court terme au moins, augmenter les risques connexes, à savoir la probabilité d'attentats terroristes contre des cibles américaines à l'étranger. Ce point soulève aussi la question de savoir si l'action gouvernementale peut modifier les préférences du secteur privé, économie parallèle comprise. Nous examinerons ce thème plus loin de manière plus détaillée.

La réglementation sécuritaire publique est tout à fait prégnante dans de nombreux secteurs économiques. Par exemple, un durcissement des contrôles et d'autres règlements sécuritaires créent des retards aux frontières, augmentent les délais d'expédition et réduisent la perméabilité des frontières, ce qui se traduit par un recul des flux commerciaux. Comme nous l'avons indiqué plus haut, une telle réglementation renforce ainsi les effets de l'insécurité sur les échanges. De surcroît, les dispositions standards prises par les pouvoirs publics dans le domaine de la défense nationale, de la lutte contre la criminalité et de la défense des droits civils imposent des coûts supplémentaires aux entreprises (Hobijn, 2002 ; Philips, 2001 ; Banque mondiale, 2003). L'ajout de réglementations portant sur la sécurité entraîne un transfert de ressources économiques du privé au public qui bride les forces du marché propices à l'efficience, mais aussi la croissance.

Le secteur aéronautique, par exemple, a été gravement touché par la réglementation sécuritaire qui a vu le jour à la suite du 11 septembre (Lenain *et al.*, 2002). Le niveau de la concurrence dans le secteur étant déjà trop élevé et les attentats terroristes ayant eu un impact négatif sur la demande, il n'a pas été possible de répercuter la hausse des coûts sur les clients. Par ailleurs, les actions aéronautiques, voyant leurs cours chuter, sont passées de

défensives à offensives. La capacité a été réduite et l'emploi a vraiment reculé. Ainsi, le processus d'ajustement structurel en cours dans le secteur aéronautique s'est trouvé accéléré par l'insécurité nouvelle.

L'expansion du budget public serait elle-même un facteur retardateur de la croissance à long terme. Ceci vaut particulièrement pour les budgets de la défense et de la sécurité intérieure de création récente.

Ampleur des retombées

L'ampleur des effets de l'insécurité et des réactions des secteurs public et privé à cette dernière est difficile à estimer, comme nous l'avons souligné plus haut à propos de l'ampleur de l'économie de la sécurité. La tâche est encore compliquée par la nature de l'insécurité, sauf dans les cas de terrorisme ou de guerre. De nombreuses études font l'hypothèse d'une hausse des coûts provoquée par l'insécurité, puis estiment les modifications qu'elle induit dans les échanges ou la croissance. Par conséquent, les estimations de ces effets varient et ne peuvent que rester vagues sur l'ampleur des effets probables.

On a par exemple estimé qu'une journée de prolongation des contrôles douaniers engendrait un coût équivalent à 0.5 % de la valeur de la marchandise (Hummels, 2001), et que le 11 septembre avait été responsable d'un surcoût des échanges de 1 à 3 % (Leonard, 2001). Sur ces bases, on a estimé qu'une hausse de 10 % des stocks américains et de 20 % des primes d'assurance commerciale aux États-Unis coûteraient respectivement 0.1 % et 0.3 % du PIB chaque année (Raby, 2003). Une autre étude calcule que l'élasticité des flux d'échange (en volume) concernant les coûts de transport (en valeur) oscille entre –2 et –3.5 (Limao et Venables, 2001).

Au niveau du commerce international, le préjudice social mondial total imputable au 11 septembre, chiffré à environ 75 milliards d'USD annuels, est relativement limité (Walkenhorst et Dihel, 2003). Pourtant, certaines régions et certains secteurs sont particulièrement touchés. Les marchandises qui ont un faible ratio valeur/poids (produits agricoles, textiles, minéraux non métalliques, équipements) sont vulnérables à une hausse des coûts des transactions. Les régions les plus touchées en termes absolus par le 11 septembre sont l'Europe occidentale, l'Amérique du Nord et l'Asie septentrionale. Pourtant, par rapport à la taille de leur économie, ce sont l'Asie du Sud, l'Afrique du Nord et le Moyen-Orient qui souffrent le plus, notamment à cause de leur plus forte dépendance vis-à-vis des importations – ce qui revient à dire que les pays en développement sont particulièrement touchés par les effets primaires et secondaires du 11 septembre.

Dans une autre approche méthodologique, on estime directement les répercussions de l'existence de l'insécurité sur la croissance et le commerce international. L'une des études utilisant cette approche constate que les flux

d'échanges internationaux sont considérablement réduits par l'existence du terrorisme chez un pays partenaire (Nitsch et Schumacher, 2004). À court terme, cette incidence a diminué le commerce international de 4 % lorsque le nombre d'incidents terroristes d'un pays avait doublé.

Ces études soulèvent la question de la dissipation des effets négatifs de l'insécurité sur le long terme. On peut accroître l'efficience au moyen d'une meilleure réglementation et d'une meilleure application (Sheffi, 2001 ; Hobijn, 2002 ; Lenain *et al.*, 2002 ; Walkenhorst et Dihel, 2003 ; Raby, 2003 ; Banque mondiale, 2003). On peut davantage cibler la réglementation et réduire ainsi les mesures de sécurité inutiles. Les marchés peuvent réagir aux mesures de sécurité existantes et trouver de nouveaux modes de communication, de production et de livraison des marchandises. Des mesures de sécurité peuvent parvenir à dissuader ou identifier des criminels, réduire l'exposition au risque et devenir ainsi superflues à long terme. *Possibles*, ces résultats ne sont pas certains. L'action publique devrait donc s'attacher tout particulièrement à surveiller la situation sécuritaire, les politiques sécuritaires et leurs effets sur l'économie pour ajuster les mesures en tant que de besoin.

Selon Poirson (1998), les effets de l'économie de la sécurité sur l'investissement privé et la croissance de 53 pays en développement entre 1984 et 1995 seraient une progression de la croissance économique atteignant 0.5 à 1.25 % par an. Une autre analyse citée par Raby (2003) estime à environ 0.2 % du PIB le recul de l'investissement aux États-Unis imputable à la menace terroriste continue, et indique que cette chute est répercutée à d'autres économies par l'intermédiaire de la baisse des importations américaines.

Dans son évaluation des conséquences économiques des dépenses de sécurité, Hobijn affirme que ni les dépenses privées ni les dépenses publiques de sécurité n'auront d'impact majeur sur l'économie (2002). Selon lui, aux États-Unis, les premières réduiront la productivité du travail de 1.12 % et la productivité multifactorielle de 0.65 %, des reculs qui ne se traduiront que par de faibles baisses du PIB américain. Il prédit en outre que la R-D relative à la sécurité n'écornera pas sérieusement la R-D propice à la productivité. Concernant les dépenses sécuritaires publiques, il calcule que les dépenses de sécurité intérieure ne diminueront la production que de 0.6 % sur cinq ans. Par rapport aux dépenses militaires bien plus importantes des années 80, il les considère comme négligeables et sans effet sur le déficit budgétaire des États-Unis.

Il convient cependant de lire les conclusions optimistes de Hobijn avec quelque prudence. Son analyse repose sur quelques hypothèses de taille, comme le fait que les dépenses sécuritaires privées ne feront que doubler à l'avenir. Hobijn sous-estime peut-être aussi les dépenses publiques futures de l'Administration Bush, surtout lorsqu'on additionne les dépenses de sécurité intérieure et nationale occasionnées par la guerre et l'occupation irakiennes.

Nordhaus en particulier va à l'encontre des assertions de Hobijn (2002), en conseillant de ne pas trop s'inspirer des estimations gouvernementales des budgets futurs de la sécurité. Selon lui, le coût des guerres, par exemple, est toujours largement sous-estimé, ce qui est parfaitement rationnel du point de vue du pays en guerre.

Une autre analyse partiellement favorable à la position de Hobijn existe sous la forme d'une simulation des effets combinés sur la croissance d'une hausse des dépenses sécuritaires privées (jusqu'à 0.5 % du PIB) et des dépenses militaires (jusqu'à 1 % du PIB) financées par l'emprunt (Lenain *et al.*, 2002). Cette étude laisse à penser qu'au bout de cinq ans, la réduction corrélative du PIB n'atteindrait que 0.7 % – une incidence faible mais permanente, due aux conséquences d'un ébranlement de la consolidation budgétaire. Le dividende de la paix postérieure à la Guerre froide n'est pas menacé par une telle hausse des dépenses sécuritaires.

4. À la recherche d'une sécurité optimale

La présente partie aborde le concept de « politique sécuritaire optimale ». Elle met en avant le rôle des préférences dans l'obtention d'un résultat « optimal », détaille les coûts et les avantages des politiques sécuritaires, et explique quelques-uns des aspects de la politique sécuritaire internationale, notamment en présence de biens publics. Nous aborderons également certains arbitrages potentiellement induits par la volonté de sécurité, en particulier du point de vue de l'efficience, de l'équité et de la liberté.

De l'existence d'un niveau de sécurité optimal

Le rôle des préférences

L'introduction du concept d'optimalité en ce qui concerne les dépenses et la réglementation sécuritaires implique une prise de position par rapport aux préférences et donc à la nature probable des apports des dépenses sécuritaires. Il existe deux interprétations de l'impact des nouvelles informations concernant les risques sur les préférences : considérer que la fonction d'utilité d'un individu change en raison des informations nouvelles ; ou estimer que ces dernières révèlent des pans cachés de la carte des préférences d'un individu. Indépendamment de la plus forte probabilité de l'une ou l'autre de ces deux interprétations, les préférences jouent sur la façon dont l'insécurité se transmet aux individus.

Les préférences sont en outre fonction des perceptions, ce qui complique l'analyse de l'optimalité. Les perceptions, étant subjectives, ne reflètent pas forcément des conditions objectives. Les préférences n'ont donc pas nécessairement à refléter une réaction rationnelle à un environnement modifié.

D'un côté, les préférences peuvent induire un fort désir de mesures de sécurité si les risques sont surestimés par les agents. Dans ce cas, le niveau de sécurité réclamé est supérieur à l'optimum social même si l'utilité individuelle a été maximisée.

De l'autre, les préférences initiales ont pu traduire une évaluation erronée des risques réels. Par exemple, les événements du 11 septembre ont pu révéler au grand public l'état d'insécurité réel. Ce constat est corroboré par le fait que si la probabilité d'attentats terroristes n'est pas plus forte depuis le 11 septembre, les agents économiques évaluent ce risque de manière plus réaliste (Sandler, 2003). Cette interprétation implique également que les changements structurels de l'économie (la hausse de la part des dépenses sécuritaires), loin d'être inefficaces, rapprochent l'économie de son optimum.

Le rôle des coûts et avantages

Les investissements sécuritaires sont porteurs d'avantages à long terme, mais aussi de coûts immédiats. Le niveau optimal des dépenses de sécurité est atteint lorsque les coûts marginaux sont égaux aux avantages marginaux. Il est donc important de détailler la forme des fonctions de coûts et d'avantages au niveau tant individuel que collectif.

Les coûts de la sécurité sont déterminés à la fois objectivement par une fonction de production intégrant des composantes technologiques et subjectivement par la perception de l'insécurité. En outre, la société peut avoir, pour établir la sécurité, de solides préférences quant à la différence entre les erreurs de type I et de type II. En fait, dans la société de la sécurité, l'importance de l'équilibrage des erreurs de type I (où l'innocent va en prison) et de type II (où le coupable reste libre) peut être inversée. Lorsqu'elles protègent leurs citoyens des attentats, de nombreuses sociétés préfèrent punir des innocents plutôt que de laisser des coupables s'échapper et commettre des atrocités. Le coût d'opportunité de l'inaction pèse donc particulièrement lourd dans l'économie de la sécurité, ce qui peut conduire à un niveau de réglementation et de dépenses sécuritaires par ailleurs excessif.

Il est moins facile d'identifier les avantages de la sécurité pour l'individu et la collectivité. On citera la prévention des incidences directes (décès, blessures, handicaps physiques) et indirectes, ainsi que les avantages intrinsèques de la sécurité pour les agents peu enclins au risque.

Efficience privée et sociale

À l'instar d'un phare, la sécurité nationale est l'exemple même du bien public. Le niveau de sécurité que procure le secteur privé ne sera donc pas optimal du point de vue de la société. Ainsi se justifient, dans une économie fermée, l'apport public ou la réglementation publique de la sécurité.

Dans le contexte international, la concurrence concernant tant l'offre sécuritaire internationale que la nature de sa prestation pourrait évoluer. Certains pays pourraient se spécialiser dans l'utilisation de l'avantage concurrentiel qu'ils détiennent vis-à-vis de tel ou tel apport sécuritaire (comme par exemple les États-Unis et l'Afghanistan des talibans pour le terrorisme, ou la Suisse et certaines petites îles-États pour les régimes bancaires protégés).

De surcroît, les pays peuvent choisir différents modèles de prestation sécuritaire par le biais d'une organisation internationale. L'OTAN, par exemple, a été constituée au fil de son histoire aussi bien de démocraties que de dictatures, aussi bien d'armées de conscription que d'armées professionnelles. Quant aux entreprises, elles ont à opérer un choix géographique au titre de leurs décisions de production, à la fois du point de vue du niveau de sécurité souhaité et de sa nature. Tout pays *i* atteindrait ainsi son propre niveau optimal de sécurité s_i^*.

Un autre problème se pose cependant si l'on considère la sécurité comme un bien public de type « maillon le plus faible » (Hirshleifer, 1983), dont l'archétype est la digue qui empêche la mer d'inonder une île. Chaque habitant peut ériger une portion de la digue de l'île pour se protéger des inondations, mais la protection effective est celle qu'offre la portion la plus basse de la digue. Le même concept vaut pour le cas général des questions de sécurité internationale : même si un pays *i* a dépensé de grosses sommes pour sa sécurité (c'est-à-dire qu'il a atteint un s_i^* élevé), il peut subir le s_j^* inférieur d'un autre pays *j* ; par les échanges internationaux, un pays *j* peut exporter l'insécurité sans le vouloir, par exemple en transportant des marchandises dangereuses dans son fret.

Simultanément, les pays qui restent en deçà des normes sécuritaires internationales évolutives sont dans l'incapacité de tirer parti des atouts de la mondialisation si leur territoire n'est plus considéré comme sûr ou fréquentable (c'est-à-dire garantissant la sécurité, procurant des technologies intelligentes et protégeant les filières d'approvisionnement). Ces économies seront confrontées à des primes de risque plus élevées et le coût de la protection des actifs croîtra, ce qui réduira les investissements directs étrangers.

C'est notamment le caractère de bien public de type « maillon le plus faible » qui met en exergue la nécessité d'une coopération et d'interventions internationales. Chaque fois que le niveau général de protection est fixé par la partie qui y contribue le moins, la concurrence n'apporte pas à la société un niveau optimal de sécurité. Des alliances internationales telles que l'OTAN, des organisations telles que l'ONU, d'autres accords, normes et dispositifs de contrôle et d'assistance mutuels tels que le FMI, sont donc destinés à

amoindrir l'insécurité internationale en fixant des normes minimales dans les domaines militaire, politique et économique. Ces institutions gomment les caractéristiques tant standards que « maillon le plus faible » de la sécurité considérée comme un bien public.

Ces réflexions font apparaître la complexité du concept d'optimalité. Il n'est pas possible de déterminer *le* niveau optimal de sécurité car il faudrait différencier les valeurs objectives et les préférences subjectives, les coûts et les avantages de la sécurité, les gains privés et les gains sociaux, les conséquences directes et les répercussions indirectes. Étant donné ces difficultés, il n'est pas certain qu'existe un niveau optimal de sécurité absolu, ni même local.

Les arbitrages possibles

Comme nous l'avons vu au début de cette section, la recherche d'une sécurité optimale doit obligatoirement équilibrer les avantages et les coûts. C'est l'existence de coûts autres que ceux déjà mentionnés qui impose des arbitrages entre un renforcement de la sécurité et d'autres objectifs. Lorsqu'on considère les implications de l'économie de la sécurité, cinq grands arbitrages se dégagent.

Dépenses de sécurité ou autres dépenses

Le premier arbitrage concerne les différents types de dépenses engagées par le secteur privé et le secteur public, comme c'est souvent le cas dans une économie de guerre. L'idée est simple : ce qui est dépensé pour la sécurité ne l'est pas pour la consommation ou des investissements propices à la croissance. Nous avons déjà abordé la question de cet arbitrage entre dépenses civiles et militaires plus haut.

Les dépenses publiques consacrées aux services militaires sont principalement des dépenses de consommation, car une part réduite des budgets militaires est dévolue à la R-D. La préservation de la paix est un avantage économique des dépenses militaires. En pratique, cet effet reste cependant difficile à estimer. De plus, le PIB croîtra à court terme sous l'effet de la demande, mais les répercussions négatives pourront prévaloir à plus longue échéance : un gros budget de la défense freine l'investissement public, et abaisse ainsi la productivité factorielle totale. Elles peuvent aussi augmenter le déficit budgétaire, la dette nationale et, partant, les taux d'intérêt. La réduction des budgets de la défense (ou la concrétisation d'un dividende de la paix) peut donc stimuler la croissance par une accumulation accrue de capital, une hausse de la population active civile et une affectation plus productive des capitaux face à une menace sécuritaire donnée. Étant donné la difficulté que l'on a à maîtriser une menace sécuritaire exogène et à

en mesurer les effets exacts, les estimations empiriques des effets du dividende de la paix sur la croissance restent ambiguës (Lenain *et al.*, 2002).

Un raisonnement similaire s'applique au cas des dépenses *privées* de sécurité. Comme la production n'est pas touchée de manière positive par ces dépenses (notamment lorsque ces dernières concernent l'embauche de main-d'œuvre de gardiennage supplémentaire), la productivité chute. En outre, les investissements productifs risquent d'être partiellement empêchés et, partant, la croissance d'être retardée.

Sécurité ou efficience

Le deuxième arbitrage concerne l'efficience. La société atteint l'efficience lorsqu'elle obtient la plus forte utilité des ressources et technologies disponibles. Comme nous l'avons avancé plus haut, la recherche de la sécurité comporte à la fois des avantages et des coûts. Parmi ces derniers peuvent figurer des frictions empêchant le fonctionnement efficient de l'économie.

On peut visualiser l'efficience comme un plancher de coûts transactionnels, par exemple lors du passage frontalier ou, plus généralement, dans les échanges. On aperçoit là un arbitrage évident entre la sécurité et l'efficience, dans la mesure où les contrôles aux frontières augmentent la sécurité mais réduisent la rapidité et la facilité de déplacement des biens et des individus. Sur le long terme, néanmoins, cet arbitrage peut disparaître, comme nous l'avons avancé plus haut. Les améliorations induites par un souci de sécurité peuvent même faciliter les échanges à long terme. Un surcroît d'investissement dans des installations sûres et des technologies modernes peut amoindrir les coûts transactionnels. Les pressions induites par les coûts sécuritaires pourraient susciter des réformes des institutions et des infrastructures relatives aux échanges, avec des effets bénéfiques sur le commerce et la croissance. Le fait de favoriser les échanges par la déréglementation des secteurs du commerce, l'harmonisation des services douaniers et la coordination internationale augmenterait les échanges des 75 pays étudiés de 377 milliards d'USD (Banque mondiale, 2003).

Un autre exemple d'efficience concerne le caractère public ou privé de la fourniture ou de la réglementation des services et règles sécuritaires. Par exemple, après le 11 septembre, les États-Unis ont accru les effectifs publics affectés à la sécurité aéroportuaire. Il n'apparaît pas d'emblée qui, des autorités fédérales/étatiques ou, avec la réglementation adéquate, des entreprises privées, aurait été le plus à même de fournir ces services.

Sécurité ou mondialisation et évolution technologique

Un troisième arbitrage peut s'imposer entre la sécurité d'un côté et la mondialisation et le changement technologique de l'autre. On ne sait pas à

l'avance si la mondialisation renforce ou atténue les problèmes associés à l'économie de la sécurité. Une course semble se dessiner entre deux effets de la mondialisation.

D'un côté, les mêmes forces qui peuvent doter certains pays et secteurs de cette prospérité sont très vulnérables aux menaces sécuritaires. Ce sont à la fois le caractère ouvert et l'interdépendance qui permettent à différents risques de déstabiliser l'économie internationale (voir aussi Stevens, 2004, dans le présent ouvrage). D'un autre côté, la coordination, l'intégration et l'harmonisation qui vont habituellement de pair avec la mondialisation peuvent aussi réduire le champ de l'insécurité dans certains domaines et considérablement faciliter le suivi des sources d'insécurité.

Par ailleurs, la mondialisation est un processus qui s'accompagne de flux permanents d'avantages, tandis que de nombreuses formes d'insécurité engendrent des coûts exceptionnels dans leur périodicité comme dans leur montant (à la différence de la lutte contre l'insécurité qui, elle, peut aussi créer des coûts permanents). Bâtir des coalitions anti-insécurité par l'apport de biens publics peut donc s'avérer une tâche bien plus aisée dans une économie planétaire mondialisée et intégrée que dans une économie planétaire dominée par des États-nations privilégiant les productions nationales réductrices des importations.

Chen et Siems concluent ainsi que la planète mondialisée s'est stabilisée face aux menaces (2004). La réaction des pouvoirs publics au 11 septembre en particulier a montré l'efficacité dont la coopération pouvait faire preuve. L'intégration internationale a établi à la fois la nécessité et l'obligation, pour les autorités de toute la planète, d'échanger les informations utiles et de rapprocher les politiques de manière à absorber un choc d'une telle ampleur.

La mondialisation et le changement technologique entraînent, dans les économies ouvertes, des changements structurels qui pourraient être accélérés en particulier pour l'économie de la sécurité (Sheffi, 2001 ; Banque mondiale, 2003) par l'évolution technologique consécutive aux investissements réalisés dans les infrastructures sécuritaires permettant l'automatisation, la surveillance et les échanges d'informations dans les ports, dans les aéroports et aux postes frontières. La mondialisation peut donc être le moyen même d'atténuer à long terme l'arbitrage à opérer entre sécurité et efficience.

L'intégration des protocoles techniques de sécurité aux organisations, conventions et normes techniques internationales (UE, OMC et Organisation internationale de normalisation respectivement) représente un défi important pour les pouvoirs publics. Il convient de rechercher la transparence et l'harmonisation pour réduire les coûts transactionnels. Il faudrait en outre éviter que les préoccupations sécuritaires n'aboutissent à l'établissement d'obstacles autres que douaniers aux échanges. Le rôle des gagnants et des

perdants économiques au jeu du changement structurel induit par les nouvelles réglementations sécuritaires constitue un autre thème d'action pour les pouvoirs publics ; nous en reparlerons plus loin.

Sécurité ou équité

Le quatrième arbitrage est à la fois politiquement et socialement sensible car il concerne les coûts de distribution de la sécurité renforcée. D'un point de vue analytique, on ne sait pas a priori quels groupes bénéficieront ou au contraire pâtiront le plus d'un renforcement de la sécurité. De nombreux services de sécurité sont assurés par des personnels peu qualifiés (gardiens, par exemple), mais de nombreux produits à forte intensité technologique seront mis au point par des personnels très qualifiés. Si le commerce international subit une diminution du fait d'une hausse des coûts transactionnels, l'emploi peut en souffrir dans les secteurs ou pays les plus touchés par ces mesures. L'emploi public peut croître si les dépenses sécuritaires publiques se concentrent sur le personnel judiciaire, policier, douanier et militaire. Néanmoins, certains services peuvent être sous-traités au privé, ce qui, comme nous l'avons avancé plus haut, peut constituer une option importante pour la puissance publique soucieuse d'efficacité dans sa politique sécuritaire.

Les pouvoirs publics pourraient envisager d'indemniser leurs ressortissants qui pâtissent des mesures de sécurité. Sur le plan international, une telle démarche pourrait être particulièrement importante si les perdants de l'économie de la sécurité (par exemple des groupes ou des pays entiers touchés par une baisse des échanges dans les pays en développement) pouvaient eux-mêmes être sources d'insécurité future. L'indemnisation des perdants (et peut-être la taxation des gagnants) est donc étroitement liée aux causes et à la nature de l'insécurité. Une solution pourrait consister à réduire de manière accélérée et unilatérale les obstacles aux échanges dans les pays en développement particulièrement sinistrés par la guerre contre le terrorisme.

L'accès aux services et produits de sécurité pose un autre problème d'équité. Des groupes à revenus modestes peuvent, sous l'effet des forces du marché ou en raison de processus administratifs, se trouver exclus de l'offre de produits ou services sûrs. On peut aussi penser à la catégorisation sociale qu'induit l'impossibilité, pour les catégories indigentes, d'accéder à la propriété ailleurs que dans des environnements ou des régions moins sûrs. Il incombe aux pouvoirs publics de se préoccuper de la manière de garantir accès et participation égalitaires à l'économie de la sécurité.

Sécurité ou liberté et respect de la vie privée

Le cinquième arbitrage touche aussi à la sphère politique : il concerne l'équilibre des droits civils, du respect de la vie privée et de la liberté individuelle face au besoin potentiel d'entraver ces droits en raison de la recherche d'une sécurité accrue. Internet, l'informatique et les technologies mobiles et sans fil sont hautement vulnérables face aux atteintes sécuritaires. Simultanément, ces technologies peuvent être utilisées pour surveiller les mouvements, l'utilisation et les profils d'individus ou de biens – qu'il s'agisse des consommateurs ou des fauteurs potentiels de troubles.

Ce thème soulève différents points intéressants et pertinents qui ne relèvent toutefois pas tous ou exclusivement de l'analyse économique. Tout d'abord, il faut à l'évidence faire, au moins à l'extrême, un arbitrage entre liberté économique et croissance économique. L'estimation empirique de cet arbitrage peut générer des résultats ambigus, mais l'analyse suggère nettement qu'un haut niveau de réglementation et de restriction entrave la hausse de la productivité et l'optimisation de l'utilité (Paldam et Würtz, 2003).

En second lieu, l'évolution de l'économie en réseau et celle de l'économie de la sécurité sont étroitement liées. Les occasions de traitement et de mise en relation de données à la valeur marginale faible prolifèrent. Elles accroissent à la fois la vulnérabilité des systèmes de données interconnectés et interdépendants et les possibilités de pistage des auteurs de délits. La protection de ces systèmes, la mise à profit de leurs possibilités et le maintien des libertés civiles nécessitent un fin travail d'équilibrage. La demande accrue de surveillance de nature sécuritaire et les progrès technologiques réalisés dans ce domaine facilitent un usage potentiellement exagéré de l'extraction de données, de la catégorisation sociale et des atteintes à la vie privée (Lyon, 2004, dans le présent ouvrage).

En fait, de nombreux secteurs économiques exigent pour leur production des chaînes d'information de plus en plus complexes. Le traçage des aliments, des produits chimiques industriels (notamment dans l'Union européenne) et des déchets dangereux nécessite de plus en plus des chaînes d'information allant de la source jusqu'à l'utilisateur. On peut donc s'attendre à ce que l'usage d'étiquettes intelligentes se généralise, de même que l'utilisation de systèmes de positionnement et de navigation associés à des technologies mobiles (Hodges et McFarlane, 2004, dans le présent ouvrage). Ces évolutions technologiques et légales démontrent l'existence de défis croissants pour l'économie de la sécurité et ses responsables. Il faudrait résoudre les questions de droits civils et de sécurité technologique en parallèle avec la mise en œuvre de chaînes d'information de ce type. La résolution contrainte des problèmes de sécurité pourra en fait accélérer le développement de systèmes d'information allant de la source à l'utilisateur.

5. Les implications pour l'action publique

Après notre étude de la nature et du périmètre de l'économie de la sécurité, des effets et des politiques de réduction de l'insécurité, et des arbitrages rendus nécessaires par la recherche d'une sécurité accrue, la présente partie détaille différents types de politiques sécuritaires, les motivations d'une intervention de la puissance publique, ainsi que la réglementation et l'organisation des politiques sécuritaires économiques.

Le principal argument justifiant l'intervention de l'État est le côté « bien public » de la sécurité. Les agents ne prennent pas en compte l'externalité positive que comporte leur investissement sécuritaire pour autrui. Du coup, le niveau effectif de sécurité n'est socialement pas optimal. C'est un exemple du dilemme du prisonnier.

De tels résultats non souhaités peuvent être évités grâce à la réglementation (interdisant les stratégies dominantes mais inefficaces, ou jouant sur les incitations en faisant varier la rentabilité par des subventions ou des impôts) ou grâce à une coordination couplée avec des règles d'application crédibles. Clairement, la fourniture par l'État de biens publics tels que la sécurité est une nécessité. Néanmoins, il reste la question épineuse de l'ampleur de l'implication étatique et de la détermination des champs d'action prioritaires.

Typologie des politiques sécuritaires existantes

Les politiques sécuritaires peuvent être classées selon plusieurs dimensions. Tout d'abord, une menace peut être exogène (catastrophes naturelles, certaines guerres) ou endogène (volatilité ou insolvabilité des marchés boursiers). Cependant, la distinction entre risques exogènes et risques endogènes n'est pas tranchée. En pratique, les risques ont tendance à être plus exogènes à court terme et à un niveau individuel, et davantage endogènes à long terme et à un niveau collectif. Des individus peuvent choisir de vivre sur un volcan car les prix immobiliers sont inversement proportionnels à l'altitude de la propriété sur la pente volcanique. Des actes terroristes ou guerriers peuvent cibler, à tort ou à raison, certains protagonistes pour les punir d'actes qu'ils ont commis dans le passé. Et les problèmes d'insolvabilité ont tendance à apparaître à la suite d'erreurs passées de gestion.

En second lieu, les politiques qui visent à réduire notre exposition aux risques peuvent agir *ex ante* (par exemple en préconisant l'installation de logiciels antivirus) ou *ex post*, avec des intentions essentiellement punitives (par exemple en sanctionnant les pirates informatiques) ou compensatoires. Les actions menées *a priori* peuvent être classées de manière plus fine en actions de prévention, de dissuasion et de protection. Certaines de ces

politiques peuvent ne pas être des politiques sécuritaires au sens étroit du terme. Il reste utile de rappeler que la réduction de l'insécurité économique implique bien d'autres domaines de l'action publique que ceux de l'économie ou de l'ordre public.

Dans le contexte international, prévention et protection ont des externalités différentes (Sandler, 2003 ; Trajtenberg, 2003). Si la prévention assurée par un État donné atténue la probabilité globale, par exemple, d'un attentat terroriste (externalité positive), la stratégie de protection d'une cible individuelle réduit seulement la probabilité pour cette cible d'être touchée tout en l'augmentant pour les autres cibles (externalité négative). Dans le premier cas, on aboutit à un sous-investissement global dans les activités préventives, et dans le second à un excès de dépenses défensives globales. Les deux externalités justifient l'intervention des pouvoirs publics par un apport sécuritaire, réglementaire et coopératif international.

En troisième lieu, la conjugaison de ces deux dimensions semble indiquer que des politiques *ex post* conviennent en général mieux aux risques exogènes, cependant que des politiques *ex ante* semblent plus efficaces pour les risques endogènes. La probabilité d'un événement exogène ne peut être modifiée par des politiques de l'un ou l'autre type. En revanche, les coûts d'un tel événement peuvent être réduits par une politique d'indemnisation a posteriori. Dans le cas de risques endogènes, une politique adaptée a pour objectif de diminuer le risque de survenance de l'événement néfaste, et se prévoit donc par définition *a priori*. Il existe aussi des contre-exemples : l'annonce d'une politique qui sera menée *a posteriori* peut aussi avoir des implications a priori en raison des anticipations d'interventions qu'elle suscite. Les dispositifs d'indemnisation, par exemple, sont considérés comme un facteur essentiel de l'attitude face au risque.

Quatrièmement, les politiques publiques sont les plus à même d'apporter les aspects de la sécurité qui ont un caractère de bien public, comme la sécurité nationale. Le secteur privé, d'un autre côté, a un rôle important à jouer pour décider de son exposition aux risques privés. La réglementation et les normes générales détiennent en la matière un rôle plus important pour l'action publique que la fourniture détaillée de biens et services de sécurité, qui peut aussi incomber aux forces du marché.

Cinquièmement, les politiques sécuritaires peuvent protéger de manière plus ou moins offensive contre un risque. Dans le cas d'un risque endogène, l'une comme l'autre démarche est susceptible d'induire une modification du risque. Par exemple, le fait de renforcer la garde des ambassades américaines à l'étranger après le double attentat qui a frappé les représentations des États-Unis au Kenya et en Tanzanie au cours des années 90 a diminué les attaques d'ambassades, mais mené à une recrudescence des fusillades et des

enlèvements visant du personnel diplomatique à l'extérieur des ambassades (Sandler et Enders, 2004).

Sixièmement, outre celles intéressant directement la sécurité, des politiques peuvent viser la réduction des coûts de l'insécurité, afin de diminuer à la fois l'impact de l'insécurité et l'attrait d'actes déstabilisateurs délibérés aux yeux mêmes de leurs auteurs potentiels. Frey et Lüchinger, par exemple, indiquent que l'adoption de politiques de dissuasion visant à accroître le coût marginal des attentats pour les terroristes pourrait ne pas être la réponse la plus adaptée à ces menaces (2002). Il peut en effet s'avérer plus efficace de combattre le terrorisme en amoindrissant les avantages que les auteurs potentiels d'actes terroristes espèrent retirer de ces derniers. Une telle politique peut reposer sur le renforcement de la décentralisation dans la mesure où un coup porté aux autorités ne peut plus avoir que des effets limités sur la stabilité de leur action et sur l'économie dans son ensemble.

Enfin, l'analyse des politiques sécuritaires doit faire la différence entre les différents instruments d'action. L'information et les institutions constituent un premier groupe de politiques visant la dissuasion et la sanction. Comme la probabilité d'actes malveillants est plutôt surestimée par les individus, il faut utiliser l'information pour améliorer la transparence des risques. La réglementation, la supervision et la coordination sont des instruments, au même titre que la mise en place de mesures incitatives et dissuasives, par exemple au moyen de la politique budgétaire. À titre d'exemple, une économie de marché peut fournir une sécurité insuffisante, mais aussi sous-investir dans la R-D. Cette dernière comportant des retombées pour la société, son taux social de rentabilité est normalement plus élevé que son taux privé, et les investissements privés de R-D sont donc habituellement en deçà du niveau socialement souhaitable. Ainsi, même si la sécurité était un bien privé, la R-D de ce domaine aurait besoin de subventions de l'État.

Le débat public qui entoure le combat antiterroriste depuis le 11 septembre, par exemple, s'est fortement axé sur les dépenses sécuritaires et l'ajustement des droits civils, négligeant certains autres instruments tels que la coordination internationale, les signaux politiques et même, à certains moments, un désintérêt délibéré. De manière plus importante encore, le débat public a souvent omis d'examiner en quoi le marché pourrait aider à résoudre certains problèmes rencontrés par la société, au lieu de s'intéresser essentiellement aux interventions, à la réglementation et aux dépenses de l'État.

La réglementation de l'économie de la sécurité

Même si la réglementation par l'État de l'économie de la sécurité est nécessaire, elle doit être adaptée avec soin. Afin de rehausser l'efficacité de ces interventions, il faut privilégier les incitations, les attentes et les capacités

du marché. Il faut éviter de toucher au passage à d'autres mécanismes, de manière à atténuer de néfastes effets secondaires. La coopération entre le public et le privé peut s'avérer utile dans plus de cas qu'on n'avait pu l'envisager, par exemple en mettant des services de sécurité ou de nouveaux dispositifs réglementaires en place (Sheffi, 2001). Simultanément, des politiques de libéralisation prévoyant des indemnisations ou des compléments ont leur importance pour stimuler la croissance et générer des excédents au profit des groupes vulnérables au sein de l'économie mondiale de la sécurité. Ces considérations valent particulièrement dans le domaine des coûts de transport et du commerce mondial, où un accès accru aux échanges peut être fourni aux pays qui risquent d'être défavorisés dans l'économie de la sécurité (Leibfritz, 2002 ; Banque mondiale, 2003).

Outre ces mécanismes de coordination, le marché fournit aussi certains dispositifs de renforcement des dépenses sécuritaires spontanées. Par exemple, les agents économiques qui investissent dans la sécurité peuvent bénéficier de primes d'assurance inférieures. À l'appui de ces mesures peuvent venir des réglementations incitant davantage les parties concernées à un comportement responsable.

Le secteur de l'assurance postérieur au 11 septembre est en fait un exemple de l'importance que revêt la réglementation face aux subventions, et du rôle potentiel des forces du marché vis-à-vis de l'allègement des coûts économiques de l'insécurité. Les compagnies d'assurance ont pour vocation de prendre l'insécurité en charge. Pourtant, les plus grands réassureurs mondiaux eux-mêmes ont été confrontés à des problèmes de fond après les attentats en question (Wolgast, 2002). Là encore, ce ne sont pas les effets directs des attentats terroristes qui sont au cœur du problème, quoique qu'avec un montant de dommages compris entre 30 et 58 milliards d'USD le 11 septembre représente le plus gros sinistre de tous les temps (Lenain *et al.*, 2002) : son impact n'a pas été suffisant pour provoquer la moindre faillite majeure de compagnie d'assurance.

Ce sont les effets indirects qui incitent à examiner le secteur assurantiel sous l'angle économique : depuis le 11 septembre, la probabilité d'attentats terroristes de grande ampleur est perçue comme plus élevée. Les compagnies d'assurance ont rehaussé le montant maximal des dommages considérés comme probables, ce qui a entraîné une hausse des primes allant jusqu'à 30 % (Lenain *et al.*, 2002). Plus grave encore, les garanties ont été sérieusement réduites, et des contrats comprenant une assurance contre les attentats terroristes ont été tout bonnement annulés. Par voie de conséquence, les grands attentats terroristes ont cessé d'être entièrement assurables, ce qui pose un problème dans la mesure où la propension à porter les risques est un facteur de production rare : dans un monde plus incertain, les investissements sont moindres, d'où une croissance à long terme moins forte. En particulier, les

investissements portant sur des projets innovants et risqués mais très propices à la croissance sont évités.

On entrevoit déjà le contenu des effets secondaires indirects. Des appels à l'action des pouvoirs publics se font entendre. Comme le secteur privé s'avère incapable d'assurer les risques de nature terroriste, l'État doit adosser le système à des subventions et des garanties. Si une intervention peut être intrinsèquement positive, le dispositif réglementaire doit être soigneusement élaboré. En particulier, les problèmes de compatibilité des incitations font courir le risque que les pouvoirs publics n'aillent jusqu'à exacerber les effets négatifs de l'insécurité. En fait, ce ne sont pas des apports financiers directs qui ont aidé le secteur de l'assurance après septembre 2001, mais la refonte de la réglementation du secteur réassurantiel face à l'hyper-terrorisme. Comme le Royaume-Uni, l'Allemagne a mis en place un réassureur de dernier ressort bénéficiant de la garantie de l'État, mais de statut privé, pour les dommages dus au terrorisme. Fait important, ce dispositif a davantage incité le secteur privé à se prémunir contre les risques terroristes, et aide le marché à estimer la valeur de l'assurance antiterroriste.

Les pouvoirs publics ne sont cependant pas seuls à réagir aux modifications de l'environnement. Des initiatives émanant du secteur privé et des partenariats public-privé spécialement conçus pour couvrir les risques de dommages de grande ampleur voient le jour. Exemple de mécanisme de partage mutualisé des risques susceptible d'apporter une solution satisfaisante, l'entité allemande Extremus AG implique les assureurs, les réassureurs, les pools et les pouvoirs publics en tant qu'assureur de dernier ressort. Fondée par 16 grands assureurs, Extremus AG propose des polices exclusivement conçues pour les risques de dommages de grande ampleur (supérieures à 25 millions d'EUR). La capacité de l'entité est de 13 milliards d'EUR et se déploie sur trois niveaux de garanties. Les pouvoirs publics allemands assurent seuls la couverture du troisième seuil, qui n'est déclenché que lorsque les deux premiers sont entièrement utilisés (Lenain *et al.*, 2002 ; Wolgast, 2002).

Les obligations dites « obligations-catastrophes », associées à une forte rentabilité et à un risque élevé, constituent un autre mode de prise en charge par l'économie des risques d'origine terroriste. Si cette titrisation des risques sur les marchés de capitaux semble théoriquement représenter une solution efficace au problème, elle a pour l'instant mal fonctionné dans la pratique (Leibfritz, 2002 ; Lenain *et al.*, 2002).

Les modes possibles de coordination de la politique sécuritaire

Le dilemme du prisonnier peut être résolu par la réglementation, comme nous l'avons soutenu plus haut, ou par la coordination. Cette dernière solution

s'applique particulièrement aux cas où la sécurité est dépendante de son maillon le plus faible, comme nous l'avons vu plus haut à la section 4.

Ces problèmes sont similaires aux externalités réticulaires dans lesquelles une communauté adopte, parmi plusieurs normes concurrentes, une norme déjà retenue par un nombre suffisant de ses membres. Dans l'économie de la sécurité, la propension de tout agent à investir dans la sécurité est une fonction croissante du nombre d'autres agents l'ayant déjà fait.

La coordination peut être améliorée par le partage d'informations, la multiplicité des prises de contact, l'amélioration de la renommée, la mise en place de mécanismes de sanction (même informels) et le partage de normes techniques. Des organisations internationales telles que l'IATA (*International Air Transport Association*, ou Association internationale du transport aérien) pour le secteur aérien peuvent édicter des règles et des réglementations pour leurs États membres. Les sanctions appliquées localement par les États membres face à des comportements localement déviants constituent une question centrale de l'action publique.

De manière générale, les pouvoirs publics devraient s'abstenir de recourir à des politiques extrêmes. La concurrence seule ne peut résoudre les problèmes, pas plus que l'intervention de l'État. Les meilleurs résultats résulteront de la mise en œuvre d'une palette d'actions conjuguant des moyens politiques, économiques, juridiques et sociaux. Il faut rechercher cet équilibre en particulier pour atteindre un niveau sécuritaire global raisonnable. Des institutions telles que l'OCDE devraient jouer un rôle essentiel dans cet effort de coordination.

6. Conclusions

La récente poussée de terrorisme mondial a attiré l'attention des responsables de toute la planète sur l'émergence, les répercussions et la réglementation de l'économie de la sécurité. Le vocable d'« économie de la sécurité » n'a pas de sens économique strict, et recouvre de nombreuses activités différentes des secteurs public et privé. Par ailleurs, il n'existe pas un niveau optimal unique de sécurité. Nous avons pu néanmoins démontrer que l'insécurité avait des effets directs non négligeables, et des effets indirects primaires et secondaires encore plus forts. Parmi ces derniers figurent respectivement les réactions comportementales des agents et les interventions consécutives de la puissance publique.

Celle-ci doit soigneusement penser son action pour prendre en compte les préférences et les perceptions des agents, les coûts et avantages des interventions et la dimension internationale de l'insécurité. Le secteur privé a un rôle important à jouer pour assurer une offre sécuritaire privée efficiente. Les aspects sécuritaires nationaux intérieurs sont peut-être mieux pris en

charge par les gouvernements, tandis que la sécurité internationale doit passer par une coopération mondiale. L'intervention publique sur les marchés et une offre privée sécuritaire accrue peuvent accroître la sécurité – peut-être, toutefois, au détriment de l'efficience, de l'équité ou de la liberté.

Bibliographie

ARCE, D.G. et T. SANDLER (2001), « Transnational Public Goods: Strategies and Institutions », *European Journal of Political Economy,* 17(3), pp. 493-516.

BANQUE MONDIALE (2003), « Reducing Trading Costs in a New Era of Security », *Global Economic Prospects 2004: Realizing the Development Promise of the Doha Agenda*, pp. 179-203.

BRÜCK, T. (2004), « The Economic Consequences of Terror: Guest Editor's Introduction », *European Journal of Political Economy*, à paraître.

BRÜCK, T. et S. SCHUBERT (2003), « Krieg und Wiederaufbau im Irak », *DIW Wochenbericht,* 70(18), pp. 291-297.

CHEN, A.H. et T.F. SIEMS (2004), « The Effects of Terrorism on Global Capital Markets », *European Journal of Political Economy,* à paraître.

DIETZ, O. (2002), « Öffentliche Ausgaben für äußere und innere Sicherheit », *Wirtschaft und Statistik,* 4, pp. 310-315.

FREY, B.S. et S. LUECHINGER (2004), « Decentralization as a Disincentive for Terror », *European Journal of Political Economy*, à paraître.

GLAESER, E.L. et J. M. SHAPIRO (2001), « Cities and Warfare: The Impact of Terrorism on Urban Form », *NBER Working Paper Series* 8696.

HIRSHLEIFER, J. (1983), « From Weakest-link to Best-shot: The Voluntary Provision of Public Goods », *Public Choice* 41, pp. 371-386.

HOBIJN, B. (2002), « What Will Homeland Security Cost? », *Economic Policy Review,* 8(2), pp. 21-33.

HODGES, S. et D. MCFARLANE (2004), « Radio Frequency Identification: Technology, Applications and Impact », présent ouvrage et Forum de l'OCDE sur l'avenir sur « L'économie de la sécurité : quels arbitrages dans une société ouverte et mobile ? », Paris, 8 décembre 2003.

HUMMELS, D. (2001), « Time As a Trade Barrier », document non publié, Department of Economics, Purdue University, West Lafayette/Indiana.

KUNREUTHER, H. et G. HEAL (2003), « Interdependent Security », *The Journal of Risk and Uncertainty,* 26(2/3), pp. 231-249.

LEIBFRITZ, W. (2003), « Auswirkungen des Terrorismus auf die Volkswirtschaften und Implikationen für die Wirtschaftspolitik », *Ifo Schnelldienst,* 56(1), pp. 14-20.

LENAIN, P., M. BONTURI et V. KOEN (2002), « The Economic Consequences of Terrorism », Documents de travail du Département des affaires économiques de l'OCDE, 334.

LEONARD, J.S. (2001), « Impact of the September 11, 2001 Terrorist Attacks on North American Trade Flows », Manufacturers Alliance E-Alert, Arlington, Virginie.

LIMAO, N. et A.J. VENABLES (2001), « Infrastructure, Geographical Disadvantage, Transport Costs and Trade », *World Bank Economic Review,* 15, pp. 451-479.

LYON, D. (2004), « Surveillance Technologies: Trends and Social Implications », présent ouvrage et Forum de l'OCDE sur l'avenir sur « L'économie de la sécurité : quels arbitrages dans une société ouverte et mobile ? », Paris, 8 décembre 2003.

NITSCH, V. et D. SCHUMACHER (2004), « Terrorism and Trade », *European Journal of Political Economy,* à paraître.

NORDHAUS, W.D. (2002), « The Economic Consequences of War with Iraq », *The New York Review of Books,* 49(19).

O'HANLON, M.E. *et al.* (2002), *Protecting the American Homeland: A Preliminary Analysis*, Brookings Institution Press, Washington, DC.

PALDAM, M. et A. WÜRTZ (2003), « The Big Bend – Economic Freedom and Growth », allocution présentée à la réunion annuelle de la *European Public Choice Society* à Aarhus.

PHILLIPS, L.T. (2001), « A Crisis of Security and Economics », *Regulation,* 24(4), pp. 53-56.

POIRSON, H. (1998), « Economic Security, Private Investment and Growth in Developing Countries », IMF Working Paper WP/98/4.

RABY, G. (2003), « The Cost of Terrorism and the Benefits of Cooperating to Combat Terrorism », allocution présentée à la conférence *Secure Trade in the APEC Region (Star)* le 24 février.

SANDLER, T. (2003), « Collective Action and Transnational Terrorism », *The World Economy,* 26(6), pp. 779-802.

SANDLER, T. et W. ENDERS (2004), « An Economic Perspective on Transnational Terrorism », *European Journal of Political Economy,* à paraître.

SHEFFI, Y. (2001), « Supply Chain Management Under the Threat of International Terrorism », *The International Journal of Logistics Management,* 12(2), pp. 1-11.

STEVENS, B. (2004), « The Future Demand for Security Goods and Services: Shaping Factors », présent ouvrage et Forum de l'OCDE sur l'avenir sur « L'économie de la sécurité : quels arbitrages dans une société ouverte et mobile ? », Paris, 8 décembre 2003.

SUNSTEIN, C.R. (2003), « Terrorism and Probability Neglect », *The Journal of Risk and Uncertainty,* 26(2/3), pp. 121-136.

TRAJTENBERG, M. (2003), « Defense R&D Policy in the Anti-Terrorist Era », NBER Working Paper Series 9725.

WALKENHORST, P. et N. DIHEL (2004), « Trade Impacts of Increased Border Security Concerns », *International Trade Journal,* à paraître.

WOLGAST, M. et W. RUPRECHT (2003), « Weltweiter Terror und Versicherungswirtschaft: Ökonomische und politische Herausforderungen », *Ifo Schnelldienst,* 56(1), pp. 11-14.

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Chapitre 8

Les technologies de la surveillance : tendances et répercussions sociales

par

David Lyon
Département de sociologie, Queen's University
Canada

Introduction

Au XXI[e] siècle, les populations des riches sociétés technologiquement avancées ne sont pas les groupes d'individus clairement anonymes, indépendants, autonomes et souverains que suggèrent les visions mondialistes et les idéologies consuméristes dominantes. Nul besoin d'être sociologue pour constater que nos vies sont structurellement soumises à nombre de circonstances, processus et pratiques qui sont souvent concernés par la surveillance (dans l'acception la plus large du terme). Nous ne pouvons pas nous attendre à obtenir des billets du distributeur bancaire sur la foi d'un code d'identification personnelle fantaisiste, à embarquer à bord d'un avion sans une vérification approfondie de notre identité et de nos bagages, à utiliser un téléphone portable sans que personne ne puisse repérer le lieu et le moment de l'appel, ou à quitter notre poste à l'usine avant la fin de la journée sans que notre employeur en soit averti. Ces différents exemples décrivent, en un sens, autant de situations d'un monde où prévaut la surveillance.

Les attentats du 11 septembre 2001 ont eu de larges répercussions sur les activités militaires et les dispositifs sécuritaires internationaux ; ils ont aussi entraîné une sensibilisation aux pratiques répandues et envahissantes d'une surveillance quotidienne. À n'en pas douter, l'identité de ceux qui collectent des données sur les personnes et le sort qui est réservé à ces données ont des répercussions, tant banales que traumatisantes, sur nos vies. D'un côté, le courrier commercial informatique non désiré peut être très gênant ; de l'autre, la justice est prise en grave défaut lorsque ce qui n'est au fond qu'un profilage racial automatisé place des innocents en prison ou, pire, les livre à la torture[1]. L'individu moyen, dans sa vie de tous les jours, peut connaître l'un ou l'autre type d'expérience non souhaitée parce qu'il vit dans une société de la surveillance.

S'il importe de s'intéresser à l'avenir de la société de la surveillance, le vocable même soulève bon nombre de questions. Il présuppose que des « sociétés de la surveillance » existent et qu'on peut commenter leur avenir. Si l'on en croit différentes recherches historiques et sociologiques importantes qui ont été menées dans le domaine (Rose, 1999), on peut soutenir que l'existence de sociétés de la surveillance est avérée, au sens où des sociétés bureaucratiques et technologiques avancées encouragent le traitement détaillé de données personnelles à des fins particulières. Ce phénomène connaissant une expansion rapide, traiter de leur avenir est un sujet digne

d'intérêt. L'économie politique des renseignements personnels est un domaine d'analyse et d'action publique essentiel, un lieu central du changement social qui n'est parvenu sur le devant de la scène qu'avec la toute dernière génération.

Il existe des tendances identifiables, dont la détection présente un intérêt pour les citoyens, les travailleurs, les consommateurs et les voyageurs ordinaires, ou bien pour les décideurs, les responsables des données sur les personnes (« personnelles ») ou les militants sociaux ou politiques. L'expansion du traitement de données personnelles est une tendance en elle-même, mais certaines autres caractéristiques de la surveillance présentent aussi un intérêt. Son organisation se fait de plus en plus autour de bases de données consultables ; elle est donc algorithmique et actuarielle. Mais elle contribue aussi de plus en plus à la gouvernance, à un niveau tant microsocial que macrosocial, et les deux sont reliés (Rose, 1999). Une autre tendance concerne l'intégration et la convergence systémiques, via lesquelles des agences traitant des informations personnelles à des fins différentes se partagent des données selon des protocoles divers.

L'avenir des sociétés de la surveillance n'est donc pas couru d'avance.

La présente contribution comporte quatre parties. La première aborde le sens du vocable « société de la surveillance », à qui il n'a fallu que ces 20 dernières années pour gagner ses galons universitaires, et même devenir à la mode. La surveillance contemporaine y est définie comme l'attention sérieuse et systématique portée à des détails personnels à des fins d'influence, de gestion et de contrôle. Si les technologies nouvelles ont une importance extrême, on montrera que la surveillance ne s'y limite pas : le contexte politique, économique et socioculturel revêt une importance vitale pour bien comprendre le phénomène. On montrera aussi que les conséquences du 11 septembre ont accéléré l'essor des tendances à la surveillance.

La seconde partie est consacrée à l'étude de l'une de ces grandes tendances, que nous appelons (au Projet Surveillance[2]) la « catégorisation sociale » utilisée comme moyen de « discrimination numérique ». Cette étude repose sur l'utilisation de bases de données consultables, et non seulement concerne un nombre croissant de secteurs, mais aussi facilite l'emploi de méthodes similaires dans des secteurs différents et jusqu'ici distincts. L'exemple le plus évident est l'usage que les autorités ont fait des techniques de gestion de la relation clientèle après le 11 septembre. Si la surveillance implique la catégorisation sociale – c'est-à-dire le fait de ranger les groupes de population en catégories pour les traiter de manière différenciée – alors de nouvelles formes d'analyse et de nouvelles réactions sont nécessaires.

Ce thème se prolonge dans la troisième partie, qui aborde ce que l'on peut considérer comme la nouvelle politique de surveillance. En termes d'action et

de réglementation publiques, la surveillance vue comme une catégorisation sociale nécessite soit une extension des préoccupations relatives à la vie privée, soit un vocabulaire nouveau pour mobiliser les réactions appropriées. Là aussi, néanmoins, il convient de prendre en compte un contexte plus large, à savoir le développement d'une politique plus générale de l'information (relative aussi aux droits de la propriété intellectuelle, à l'accès à l'information et à différents autres thèmes) englobant la surveillance. Au-delà de l'important domaine de la politique et de la réglementation formelles, où l'accent doit être mis entre autres sur la responsabilité des opérateurs plutôt que sur la simple sensibilisation de l'usager, il faut absolument s'intéresser à l'émergence de nouveaux groupes et mouvements sociaux qui comptent la critique de la surveillance au nombre de leurs objectifs.

La quatrième partie traite de scénarios d'avenir, en commençant par un scénario dystopique dans lequel sont magnifiées les tendances négatives actuelles à la catégorisation sociale et à l'approche préventive. Les droits de l'homme, la protection des données et le respect de la vie privée sont fortement mis à mal. Un scénario plus positif, que certains considèreront comme utopiques, est ensuite abordé. On imagine assez aisément un monde dans lequel l'attention portée aux données personnelles a pris une place bien plus centrale dans l'organisation de la vie. Peut-être faudra-t-il un événement majeur – un Tchernobyl informationnel – pour cette prise de conscience, mais il se peut aussi que les effets cumulés de la pression législative et politique finissent par atténuer les aspects négatifs des dispositifs institutionnels actuels de surveillance. Quoi qu'il en soit, il faudra à la fois une solide évaluation éthique, une analyse sociale et des mesures publiques déterminées pour atténuer le risque d'avènement d'avenirs dystopiques.

1. La société de la surveillance

La société de la surveillance est un phénomène quotidien et réel des sociétés du Nord, mais aussi de plus en plus du Sud. Pourtant, le totalitarisme ne règne pas en maître, pas davantage que les régimes autoritaires – deux systèmes de gouvernement habituellement associés à la notion de société de la surveillance. Dans ces conditions, que signifie ce vocable ? Nous entendrons simplement par là, dans ces lignes, les sociétés dans lesquelles l'identification, la vérification, la surveillance, le suivi et l'enregistrement routiniers, systématiques et universels des activités, communications et échanges quotidiens sont devenus un fait courant et banal. La surveillance est déclenchée par des événements et des comportements qui font partie des petits détails de la vie quotidienne – appels téléphoniques et transferts de fonds, courses dans les supermarchés et même lèche-vitrines (sous l'œil attentif de caméras) – et repose sur une infrastructure croissante de systèmes informatiques et de communications électroniques avec et sans fil.

Ainsi, nous ne ferons pas d'amalgame entre société de la surveillance et totalitarisme, et n'irons pas même jusqu'à lui revendiquer un caractère menaçant ou pernicieux. La société de la surveillance est un aspect du début du XXI^{e} siècle qui est en devenir sous sa forme actuelle depuis moins de 20 ans. Les équipements de surveillance sont mis en place pour apporter une commodité, un confort, une efficience, une productivité, une rapidité et une sécurité qui ne sont normalement pas considérés avec dédain ou dégoût. On ne sait pas clairement si ces apports sont des valeurs ou des objectifs de base, mais au moins ils ne sont pas intrinsèquement indésirables, et certainement pas redoutés. Les pratiques de surveillance occupent tout un spectre allant de l'attention extrême au contrôle extrême (même si parfois l'attention implique le contrôle, et même la coercition). Quelque innocentes que ces pratiques puissent sembler, elles sont toutes susceptibles d'encourir analyses et critiques éthiques, sociales et politiques.

Parmi les exemples de surveillance contemporaine figurent :

- Les images vidéo de chalands dans les magasins, les gares ou stations des moyens de transport, ou la rue.
- Les enregistrements textuels détenus par l'administration (fisc, santé, etc.).
- Les codes d'identification personnelle (PIN) qui sont utilisés à différentes fins, mais surtout pour les transactions financières.
- Les étiquettes d'identification par radiofréquences (RFID) apposés sur les vêtements par les fabricants pour suivre les articles, mais qui sont aussi, par définition, associés aux individus portant ces vêtements.
- Les appareils biométriques assurant la reconnaissance du visage, de l'iris ou des empreintes digitales utilisés en association avec des cartes d'identification, notamment dans les aéroports ou aux frontières.
- Les systèmes de navigation qui permettent de suivre les véhicules ou les téléphones portables équipés pour un positionnement d'urgence à l'aide de la technologie du GPS (positionnement satellitaire mondial) ; l'interception des communications par des écoutes ou des enregistrements de l'activité Internet ou du courrier électronique.

La liste est loin d'être exhaustive. Bien entendu, ces éléments n'ont pas d'existence autonome. Par exemple, les codes PIN et la biométrie servent à identifier et vérifier dans le cadre de dispositifs plus vastes d'enregistrement, de suivi ou de surveillance des comportements. La surveillance telle qu'elle est définie dans ces lignes englobe toutes les formes de « veille » et de supervision qui ont été mentionnées ci-dessus, ainsi que la surveillance dépourvue de support technologique : la surveillance n'est pas née avec les nouvelles technologies ! Cependant, elle est devenue, à l'époque moderne, de plus en plus technologique, passant des armoires de dossiers des

bureaucraties officielles à l'informatisation de la fin du XX^{e} siècle. C'est au sein des systèmes de surveillance que les éléments détaillés isolément dans ces lignes prennent leur importance.

De même que ces systèmes comportent des équipements particuliers d'identification, les systèmes de surveillance font eux-mêmes partie d'entités plus larges. Plus précisément, ils constituent un aspect important de ce que nous appelons aujourd'hui la « gouvernance ». Ce point est très important car associer la « société de la surveillance » aux technologies peut être trompeur à l'extrême. D'un côté, toute qualification d'une société peut laisser penser que sa caractéristique principale est dans le qualificatif, à savoir ici société de la surveillance. Pire, elle peut suggérer qu'une formation sociale entièrement nouvelle, une époque radicalement originale, est née. En fait, la situation est bien plus trouble et embrouillée qu'une expression aussi nette que « société de la surveillance » ne le suggère. D'un autre côté, l'accent mis sur les nouvelles technologies peut aussi donner de nombreuses impressions trompeuses. Deux exemples majeurs de telles erreurs : les changements sociaux seraient provoqués par l'évolution technologique, et les technologies pourraient être débattues sans ambiguïté soit en tant que catégorie (disons, informatique ou biotechnologique), soit en termes d'efficacité.

Parler de la société de la surveillance n'est qu'un moyen rhétorique d'attirer l'attention sur un aspect particulier du monde contemporain, même si cet aspect a acquis une importance sociale croissante ces dernières décennies. Le concept de surveillance devient un prisme d'observation des relations sociales (exactement comme la « société de quartiers », la « société du risque » et la « société en réseau »). Mais ce concept n'est ni autonome ni autosuffisant : les sociétés de la surveillance ne peuvent être appréhendées qu'en termes de changements politico-économiques et culturels bien plus larges survenus durant le XX^{e} siècle. Ce n'est certainement pas par accident que le vocable n'est apparu que dans les années 80 sous la plume (ou peut-être sur le clavier) d'historiens (Flaherty, 1989) et de sociologues[3] qui pensaient discerner des altérations sans précédent du paysage social et politique de mauvais augure pour les compréhensions classiques du rôle de l'État et de l'application de la loi en particulier. L'usage du concept de surveillance est encore plus justifié aujourd'hui ; non seulement l'État et son administration, mais aussi les entreprises commerciales et, en fait, la population elle-même dans sa vie quotidienne, sont impliqués dans des pratiques de surveillance.

D'un autre côté, parler de technologies revient à indiquer que les pratiques de surveillance ont un support. La surveillance est associée à toutes sortes de supports non technologiques, mais les types de surveillance qui occupent aujourd'hui le devant de la scène sont de nature technologique. Si la surveillance mutuelle des villageois ou des citadins était la règle dans les sociétés traditionnelles, complétée périodiquement par des actions étatiques

ou religieuses, la surveillance s'est beaucoup centralisée à l'époque moderne. Cette évolution a eu lieu dans des organisations bureaucratiques de l'État-nation, de l'appareil militaire et de l'entreprise capitaliste (Dandeker, 1990 ; Higgs, 2001). Les « technologies de l'information » de la bureaucratie ont été les principaux mécanismes de surveillance jusqu'à la fin des années 60. L'informatisation a alors contribué à élargir la surveillance à d'autres domaines et les nouvelles télécommunications ont fourni les moyens de ce que nous connaissons aujourd'hui : des systèmes de surveillance automatisés en réseau.

La question de la technologie est cruciale. S'il est parfaitement erroné d'imaginer que la technologie puisse jamais être un moteur du changement social, les technologies n'en ont pas moins, pour plusieurs raisons, une importance certaine. L'économie politique des technologies de la surveillance voit les grandes entreprises se battre pour des contrats liés aux nouvelles branches d'activité nées du 11 septembre. La mondialisation signifie que des processus du même ordre sont en route dans de nombreux pays en même temps, et il existe aussi une pression en faveur de l'harmonisation des systèmes, dans l'espoir d'obtenir une sécurité maximale. Socialement, l'acceptation de nombreuses technologies nouvelles de surveillance, dont de proches cousines sont souvent introduites dans un premier temps dans le monde de la consommation ou du travail, est forte. Culturellement, l'horizon se dégage pour l'autorisation de l'automatisation d'activités jadis exclusivement en face à face, comme les contrôles douaniers. Quand, pour toutes ces raisons et d'autres encore, les nouvelles technologies deviennent les truchements de la surveillance, elles ont des répercussions substantielles. Par exemple, les enregistrements informatiques sont traités avec plus d'égards que les comptes personnels, les seuils anciens d'acceptation du profilage sont franchies, et la notion de « management » commence à prendre le pas sur celle de « moralité ».

Agglomérons maintenant ces deux éléments : la société actuelle de la surveillance dépend des nouvelles technologies. Il s'agit là d'une assertion qui semble innocente (annoncée par Marx, 1988), même si ses ramifications peuvent donner à réfléchir aux lecteurs de Kafka, George Orwell et Margaret Atwood[4]. L'erreur est d'imaginer que la société de la surveillance est d'une certaine façon constituée de ces technologies. Elle compose une société dans laquelle certains types de veille, à la fois littéraux et (plus souvent) figuratifs, sont devenus les moyens privilégiés de maintien – de création même – de l'ordre social. Ces régimes à base de surveillance et d'information sont rendus matériellement possibles par les technologies électroniques, mais ce sont leurs répercussions sociales et culturelles qui sont réellement significatives. Automatiser le contrôle, comme le soulignent Michalis Lianos et Mary Douglas (2000), c'est créer des contextes d'interaction non négociables (que faire face à

un code PIN inopérant ?), transformer des « citoyens respectueux de la loi » en « usagers efficients » et modifier des différenciations catégorielles tout en favorisant certaines relations de pouvoir (celles des institutions qui les utilisent).

Lorsque nous analysons les relations de pouvoir relatives à la multitude d'institutions qui utilisent désormais des formes de contrôle automatisé, nous percevons l'importance de la gouvernance. L'idée de gouvernance a vraiment pris son envol à partir des travaux de Michel Foucault sur la « gouvernementalité » et sert à examiner une pléthore de technologies de pouvoir et de stratégies de contrôle qui, aujourd'hui, gouvernent notre conduite de jour en jour. Elle fait aussi référence aux changements effectifs qui se produisent depuis les années 70, lorsque le rôle de l'État a été réduit au profit à la fois des mécanismes du marché et d'autres organes – depuis ceux de la société civile locale jusqu'aux organisations transnationales d'envergure planétaire.

Cette analyse omet de mettre l'accent sur une institution en tant que telle (l'État-nation, par exemple) pour privilégier une sorte d'objectif grand angle permettant de prendre en compte l'étendue et la complexité des mécanismes de contrôle, et leur apparition dans des lieux jusque là inhabituels. Ainsi, loin de ressembler à la classique structure pyramidale descendante des États totalitaires – ou à quelque nouvelle mégamachine technologique dernier cri – il s'agit d'un contexte de contrôle fluctuant, fragmentaire, contesté et peu structuré. Richard Ericson et Kevin Haggerty (2000) appellent cela l'« assemblage surveillant » (d'après Gilles Deleuze). Pour eux, l'axe essentiel consiste à établir la décomposition de l'individu en bits de données à des fins de collecte, de stockage et d'accès via des transactions commerciales telles que des paiements par carte ou via des images numérisées telles que celles des passeports de dernière génération. Ce sont les matières premières de la production d'identités qui représentent des individus au sein des circuits de contrôle contemporains.

Bien sûr, l'idée selon laquelle la gouvernance ou l'assemblage n'a pas de centre, ou est contradictoire et flexible, ne signifie pas qu'il est impossible d'y discerner des profils. Nikolas Rose (2000), par exemple, estime que l'on peut répartir les stratégies contemporaines de contrôle en deux grandes « familles » : celles qui régulent les individus en les « prenant dans les filets » de circuits d'inclusion, et celles qui agissent sur les pathologies en gérant des circuits d'exclusion. Il suggère que les documents d'identité tels que les permis de conduire et les passeports sont les meilleurs exemples des premières. Ces documents procurent une identité virtuelle et relient leur porteur à une base de données, tout en lui donnant accès à des privilèges et des prestations. Après le 11 septembre, ils sont devenus encore plus importants (et controversés) en raison des nombreuses cartes nouvelles qui sont proposées et créées pour tracer les passagers dans les aéroports ou

fournir une preuve infalsifiable que leur porteur ne constitue pas un « risque pour la sécurité ». Tout cela est lié au souci croissant d'une responsabilisation personnelle face à la sécurité et à une fracture grandissante entre les espaces « sûrs » et les espaces « dangereux ».

Entre-temps, les circuits d'exclusion sont réservés à ceux qui, pour une raison ou une autre, ne parviennent pas à gérer leur propre bien-être et leur propre sécurité, ou qui sont considérés comme des individus à risque. Plutôt que d'envisager leur mise au pas ou leur conversion, cette approche se contente de réguler les niveaux de déviance. Elle est managériale et, à un certain degré, actuarielle. Si elle cible habituellement les pauvres, les sans-abri et les chômeurs, elle peut connaître des extensions spectaculaires dans des moments particuliers – les suites du 11 septembre en sont un exemple central. Il est cohérent par rapport à la stratégie d'exclusion de considérer certains individus comme particulièrement dangereux ; la médiatisation des suspects du 11 septembre éclipse les processus d'exclusion en cours notamment au Royaume-Uni et aux États-Unis. Comme dans le cas des stratégies d'inclusion, les nouvelles technologies de surveillance sont les moyens de collecte de l'information pour lesquels des classifications et des opinions peuvent être appliquées au cas par cas.

Avant de nous pencher sur quelques-unes des caractéristiques de la surveillance contemporaine, faisons quelques commentaires sur certaines conséquences culturelles des modes de gouvernance qui dépendent de cette surveillance, notamment depuis le 11 septembre. Trois conséquences en particulier viennent à l'esprit, avec le développement de cultures de la crainte, de la suspicion et du secret.

La crainte est une caractéristique indéniable, si ce n'est générale, de la sphère culturelle d'aujourd'hui (Glassner, 1999). Dans le contexte de la consommation, les détaillants craignent la chute supposée des ventes qu'entraîneraient les déambulations de sans-abri ou d'adolescents autour de leurs boutiques, et sont favorables à la surveillance vidéo comme moyen dissuasif. Certains piétons ordinaires des centres villes ont à ce point absorbé les horreurs relatées par la presse et la télévision locales qu'ils craignent eux aussi de se promener dans les rues dites dangereuses.

À la base de la recherche de matériel de surveillance grand public, désormais aisément disponible dans les magasins et sur Internet, se trouve le souhait de se débarrasser de ces craintes. En ce XXI^{e} siècle, la crainte est un facteur dominant de nombreuses préoccupations des ménages et des quartiers. On peut apparemment acheter sa tranquillité en acquérant des articles tels que des « caméras pour nounous » grâce auxquelles les parents peuvent surveiller, dans une « fenêtre » de leur écran informatique au bureau, leurs enfants confiés à une garde à domicile (ce qui fonctionne aussi,

évidemment, comme une forme de surveillance des gardes d'enfants). On peut même se procurer un article bien commode : un « soutien-gorge électronique » (« Techno Bra ») capable de détecter sur l'instant les agressions sexuelles et de déclencher une alarme. Le positionnement commercial de la majeure partie des équipements de surveillance est l'apaisement des craintes et de l'angoisse de ceux qui ignorent les statistiques réelles des agressions et ne lisent que les grands titres alarmistes sur les dangers.

À un niveau sociétal, la crainte est devenue un thème dominant depuis le 11 septembre. On craint un « ennemi intérieur » dont les caractéristiques « racialisées » ont produit une suspension sans précédent des libertés civiles, avec l'usage généralisé de nouvelles technologies de surveillance pour créer des catégories de suspicion (Parenti, 2003 ; Lyon, 2003a). Les craintes ont été attisées, de manière indubitablement intentionnelle, par la mise en place de dispositifs sécuritaires renforcés, par la référence permanente aux alertes de niveau orange et rouge et par la recommandation constante faite aux citoyens ordinaires de devenir les « informateurs » des services opérationnels et policiers. De tels comportements sont supposés s'ajouter aux systèmes complets de renseignement et de surveillance dont les budgets ont connu un grand essor depuis les tristes événements du 11 septembre.

Tout ceci prend place, comme nous l'avons indiqué plus haut, au sein de contextes culturels où la crainte est un facteur important. La crainte est multiforme, et monte et baisse au gré des histoires collectives et individuelles, ici nourrie par la médiatisation, là atténuée grâce à l'implication de tous, à des engagements et à la clairvoyance. Comme le dit Frank Furedi (1997), nos sociétés sont craintives car «… l'évaluation de toute chose du point de vue de la sécurité est un exercice structurant de ladite chose ». Nous percevons le monde comme dangereux, ne nous fions pas à autrui, et sommes sceptiques sur le résultat effectif des possibles interventions. Pourtant, les sortes de craintes qui nous intéressent sont spécifiques à des environnements (aéroports, rue) et à des catégories d'individus (prostitué(e)s, toxicomanes, sans-abri, « terroristes », etc.). Malgré l'existence possible d'une certaine « culture de la crainte » générique, il est important de préciser les individus, les lieux et les instants associés à tel ou tel type de crainte (Tudor, 2002).

Si les cultures de la crainte doivent être considérées comme une cause et un effet palpables de régimes de la surveillance en plein essor, ces derniers sont étroitement liés à des cultures de la suspicion. Cette terminologie est employée par Onora O'Neill dans son ouvrage, paru en 2002, intitulé A Question of Trust, qui l'utilise pour décrire une des principales incidences du 11 septembre. Elle est proche des questions de gouvernance, en ce que toutes sortes d'organes administratifs, dont certains sont loin d'être chargés de l'application de la loi, se livrent à des activités de surveillance. Dans le cas des suites du 11 septembre, cependant, les incitations publiques à la surveillance

sont nombreuses, ainsi que les espoirs d'une transmission des informations sur les individus aux organismes chargés de l'application de la loi et de la sécurité. La crainte suscite la suspicion vis-à-vis des étrangers en général [des pédophiles potentiels à toute personne qui semble « déplacée »[5] (Norris et Armstrong, 1999)], mais après le 11 septembre, cette suspicion s'est centrée sur les personnes au type « moyen-oriental » ou « arabe ». De nombreux appels ont été reçus par les centres mis en place après le 11 septembre, et de nombreux renseignements ont été spontanément fournis aux autorités par les citoyens et les entreprises.

Au-delà des éléments transmis aux services chargés de l'application de la loi, néanmoins, des données personnelles ont été utilisées pour des formes de contrôle de sécurité interne à des organisations. Ainsi, par exemple, des entreprises embauchent des consultants et des détectives privés pour procéder à des évaluations des menaces de risque posées par des candidats, et des organismes de gestion de cartes bancaires ont refusé de réactiver les comptes de personnes portant un nom suspect. Dans ces cas, aucune donnée n'est transmise aux autorités ; les processus d'inclusion et d'exclusion sont conduits au sein des organisations concernées, qui ne sont ni publiques ni policières. Déjà, les cultures existantes de la suspicion ont dégénéré, stimulant directement les activités d'application de la loi et créant des colonies de contrôle dans des domaines qui n'étaient pas encore associés aux mécanismes formels de maintien de l'ordre social.

Les cultures de la crainte reliées au besoin accru de sécurité et l'incitation à la suspicion exprimée par des vagues croissantes de collecte de données personnelles sont entourées d'un climat de secret de plus en plus fort. Au nom de la sécurité, on a fermé l'accès à certaines sources d'information, et il est devenu de plus en plus difficile de savoir ce que deviennent les informations personnelles présentes dans les listes de suspects, voire les personnes auxquelles ces informations font référence. Ainsi, l'existence d'une troisième culture – celle du secret – est aujourd'hui patente dans tous les pays qui tentent de gérer les suites du 11 septembre.

Cette culture du secret est bien entendu renforcée par les événements du 11 septembre, tandis que la crainte et la suspicion tendent à accompagner la majeure partie de la surveillance contemporaine, aussi bien avant qu'après le 11 septembre. Un peu comme à l'époque du maccarthysme aux États-Unis, toutes sortes d'individus sont devenus suspects. Toute forme d'« anti-américanisme » ou de sentiment « anti-entreprise », y compris la contestation antimondialiste et le syndicalisme, peut être considérée par certains comme faisant partie d'un continuum violent et séditieux. L'identité des groupes visés est souvent tenue secrète ; ceux dont les données personnelles sont colligées ne sont pas informés qu'ils sont considérés comme suspects. Les données sont souvent recueillies de manière fort peu transparente, et transmises entre

les services de police de pays différents. C'est ainsi que les activités sur Internet de militants anti-OMC qui s'étaient servis d'Internet pour préparer leur manifestation à Seattle ont été fournis à la police montée canadienne royale de manière à lui permettre de scrupuleuses vérifications lors du passage aux frontières des militants se rendant à Québec en 2002.

Comme nous l'avons indiqué plus haut, ces trois « cultures » sont loin d'être nées avec le 11 septembre. La crainte et la suspicion en particulier ont une relation symbiotique avec les nouvelles technologies de surveillance qui non seulement dévoilent des détails de la vie personnelle aux différents organismes à qui ils sont utiles, mais aussi automatisent le processus de classification et de catégorisation. Le travail de discrimination entre deux individus sur la base d'un profil informatique ou d'une représentation de données se fait via un processus que l'on peut utilement qualifier de « catégorisation sociale ».

2. La surveillance en tant que catégorisation sociale

Les êtres humains ont toujours été discriminateurs et objets de discrimination : ce constat est plus que banal dans la vie de tous les jours. Nous sommes classés selon notre âge à l'école, puis plus tard selon nos compétences, notre nationalité, nos diplômes, etc. Toutes ces catégorisations ont une composante aléatoire mais, en temps normal, nous connaissons les critères de décision. Ainsi, en cas de litige – sur un diplôme, une ville de naissance, une affaire d'âge –, notre intervention informée peut apporter la solution. L'accès aux moyens d'évaluation est public et nous connaissons les conséquences, dans un sens ou un autre, de la classification.

Au XXI^{e} siècle, la discrimination s'est automatisée, ce qui s'est traduit par une opacité relative des processus de catégorisation, proportionnelle à leur informatisation. Là où existent des infrastructures d'information avancées, elles servent à accomplir la tâche de classification. La clé de ces activités, comme l'a très clairement souligné Lawrence Lessig dans *Code and Other Laws of Cyberspace* (1999), est l'existence de bases de données consultables. Des données personnelles peuvent être stockées sous une forme compatible avec un tri automatique sur la base de n'importe quel critère ou de plusieurs critères, de manière à pouvoir aisément distinguer une catégorie de personnes d'une autre. Plus on collecte de détails personnels et plus on peut relier de bases de données différentes, plus la typologie résultante, au moins en principe, sera affinée. Il s'agit du modèle de surveillance « Google » où, comme le mot « googol »[6] le suggère, il est possible d'opérer un nombre apparemment illimité de permutations.

L'accès à un traitement plus rapide et à des ressources informationnelles plus riches est considéré comme le meilleur moyen de vérifier et de surveiller

les comportements, d'influencer des individus et des groupes, et d'anticiper et prévenir des risques. Le grand secteur dans lequel s'est développée une telle catégorisation sociale n'est pas l'application de la loi ou l'administration (même si on utilise leurs données), mais le marketing. Au cours des deux ou trois dernières décennies, on a assisté à l'apparition rapide de tout un secteur consacré à la catégorisation des populations selon une typologie géodémographique. Au Canada, une entreprise appelée Compusearch organise les données relatives à la population en groupes, de U1 pour l'« élite urbaine » à R2 pour le « prolétariat rural », et les subdivise en groupes plus petits. U1 comprend le groupe des « fortunés » : ce sont des « familles composées de cadres supérieurs et professions libérales d'âge moyen très aisés ; logées dans de grandes maisons onéreuses, peu hypothéquées et situées dans des quartiers haut de gamme de grandes villes ; dont les enfants sont déjà préadolescents ou adolescents »[7]. U6, le groupe des « stressés des grandes villes », est assez différent : il concerne les « habitants de quartiers urbains intra muros dont le revenu moyen du foyer est avant-dernier dans l'échelle des revenus ; vivant probablement dans les zones les plus défavorisées du pays… ; célibataires, en couple ou composant une famille monoparentale ; avec une composante "ethnique" significative mais mélangée ; et un niveau de chômage très élevé ».

Ces groupes sont combinés avec le code postal pour diviser et trier les populations en fonction de leurs profils de dépenses, puis traiter les catégories résultantes en conséquence. Celles qui ont un intérêt pour les responsables marketing bénéficient de services de meilleure qualité, de promotions plus intéressantes et d'une attention spéciale, tandis que ceux dont le profil de données laisse à penser qu'ils ne dépenseront pas autant doivent se contenter d'informations moins fournies, d'un service inférieur et d'offres moins attrayantes. Les clients sont ainsi classés selon leur valeur relative pour l'entreprise en fonction des indicateurs disponibles ou utilisables. Face à son client, l'agent commercial peut tout à fait connaître non seulement son lieu de résidence et son style de vie, mais aussi des données telles que son origine ethnique [aux États-Unis, Acxiom croise les noms avec des données démographiques pour attribuer les lettres B aux Noirs, J aux Juifs et N aux Japonais (Stepanek, 2000)].

C'est pourquoi on demande son numéro de téléphone ou son code postal au client qui règle sa note à l'hôtel. Pendant qu'il patiente au comptoir, ses données personnelles sont enregistrées de manière à noter sa valeur pour l'entreprise. En 2003, un journal britannique a expliqué comment se déroulait ce processus dans les centres d'appels : lorsqu'un client téléphone pour commander des produits ou utiliser le service après-vente, son appel est automatiquement orienté vers tel ou tel opérateur en fonction du code postal que révèle le numéro appelant. Les appels provenant de zones de codes postaux à hauts revenus sont routés vers des opérateurs formés à la prestation

de services de haute qualité, d'offres commerciales optimales et de renseignements les plus complets. Les appels de clients dont le code postal semble peu prometteur en termes de statut social aboutissent à un enregistrement vocal leur demandant de patienter jusqu'à ce qu'un opérateur soit disponible, lequel, si le client a attendu jusque là, tentera de mettre un terme à la conversation aussi promptement que possible (*Sunday Times*, 2003).

Les bases de données consultables et leur potentiel de catégorisation donnent lieu à d'autres utilisations : interventions policières, tentatives d'éradication de la fraude en matière d'aide sociale ou de prestations sociales et, désormais, antiterrorisme (Lyon, 2003b, en particulier le chapitre 1). Il est intéressant de noter, en ce qui concerne cette dernière activité, que les services chargés de l'application des lois et règlements ont commencé par faire appel aux sociétés d'études de marché pour les aider à bâtir des systèmes de profilage des « terroristes » potentiels. La « gestion de la relation clientèle », l'une des grandes techniques de marketing utilisant les bases de données, s'est trouvée un nouveau segment de marché à la suite du 11 septembre (Lyon, 2003c). Dans chaque secteur, la tendance est à la prédiction et la prévision des comportements et, comme le soutiennent même certains, à la « justice actuarielle », dans laquelle la communication de la connaissance des probabilités joue un rôle croissant dans les évaluations des risques (Ericson et Haggerty, 1997). Des méthodes du même ordre sont à la base des efforts de production de systèmes fiables de reconnaissance faciale et d'autres systèmes biométriques, qui sont tous passés sur le devant de la scène publique depuis le 11 septembre.

Le constat tout simple que l'on doit tirer de l'exploration de la catégorisation sociale est que les identités organisationnelles qui ont proliféré à l'époque moderne sont désormais beaucoup plus poussées et ont plus d'effets sur la société. Nous sommes tous reliés, par l'intermédiaire de nos données personnelles, à un grand nombre d'organisations et d'agences (en le sachant pour certaines et sans le savoir pour d'autres) au sein d'un réseau relationnel complexe et toujours mouvant. Dans le nouveau climat, les données « privées » telles que la propriété immobilière, les domaines Internet et les numéros de téléphone portable sont de plus en plus interfacées avec les données « publiques » des services de police. Le risque s'est individualisé au fil de la restructuration politico-économique de ces trois dernières décennies, et ce processus s'est accompagné d'un renforcement de la catégorisation et de la classification des profils de risques. Les opportunités et choix individuels sont déterminés en relation avec les évaluations des risques et les analyses de rentabilité, ce qui fait de la catégorisation sociale un puissant moyen de discrimination des différentes classes d'individus. En un sens, elle aide à créer de nouvelles classes sociales, constituées non seulement grâce aux mesures

classiques de la profession et du revenu, mais aussi par des analyses des styles de vie et des profils de consommation.

Ce processus de catégorisation sociale croissante n'est pas intrinsèquement funeste (nous nous prêtons sans regimber à un tri multiforme qui va du passage aux toilettes au placement dans les salles de spectacles et aux files d'attente dans les aéroports), mais contribue à la fois à une tyrannie potentielle et à une démocratisation accrue. Comme l'observent Geoff Bowker et Susan Leigh Star (1999), il est vraiment facile pour les bâtisseurs d'infrastructures d'y instiller leurs partis pris, et de permettre le règne par défaut de l'inertie bureaucratique (de la paperasserie) ou de la complexité organisationnelle. Ce thème a été étudié par des sociologues, entre autres par Oscar Gandy pour le marketing, Clive Norris pour la surveillance vidéo, Steve Graham pour les infrastructures et les services urbains, et Richard Jones pour les activités de police et de contrôle. Des techniques similaires sont utilisées dans des contextes très différents, mais au profit d'une convergence accrue entre systèmes, un fait qui a notamment été exploité au sein du ministère de la Sécurité intérieure des États-Unis.

La catégorisation sociale est aussi facilitée par l'emploi d'identifiants universels tels que les cartes nationales d'identité intelligentes qui sont, en ce début de XXI^{e} siècle, en cours de test ou de mise en œuvre dans différents pays. Si de telles cartes ne contribuent pas de façon inévitable à une discrimination inéquitable potentielle, il serait surprenant, étant donné les objectifs de leur émission (combattre l'immigration illégale, la fraude aux prestations sociales, les activités terroristes, les manifestations altermondialistes, le trafic de drogues et ainsi de suite), que leur usage ne donne pas lieu à quelque profilage néfaste. La catégorisation sociale gagne du terrain chaque fois qu'un identifiant commun, qu'il s'agisse d'un permis de conduire, d'un code postal, d'un numéro de sécurité sociale ou d'une carte d'identité, est utilisé : on dispose chaque fois de nouvelles possibilités de rapprochement et de mise en relation de données, qu'il est ensuite possible d'analyser par approches successives et de manipuler de manière à différencier des groupes et procéder à d'autres traitements discriminants reposant sur des évaluations automatisées.

3. Les politiques de surveillance

La protection des données et le respect de la vie privée dominent les débats sur la « société de la surveillance ». La reconnaissance de la nature et des conséquences sociales de la catégorisation, et donc du besoin de transparence et de responsabilisation notamment, ne se fait que lentement. Des menaces sérieuses pèsent sur la vie privée. Il existe une éthique en matière de communication de données personnelles – autrement dit,

d'« autodivulgation » – selon laquelle les individus devraient être autorisés à communiquer des renseignements sur eux-mêmes sur une base volontaire, restrictive et confiante (ou, mieux, contractuelle). Des idées de cette nature sous-tendent d'ailleurs les principes d'une information loyale qui forment désormais le socle des législations et des politiques de protection des données et de la vie privée de nombreux pays de la planète.

Le vocable de « vie privée » ne parvient cependant pas à tout englober. D'autres problèmes se posent : l'usage excessif de techniques d'exploration des données, l'établissement de profils de risques et de la catégorisation sociale, la discrimination et l'exacerbation d'inégalités – mais aussi les flux transfrontières de données personnelles, les risques d'erreurs, la mauvaise utilisation d'informations pour la catégorisation, et ainsi de suite. Il est vrai qu'une législation prévoyant la protection de la vie privée et des données peut couvrir ce genre de problèmes (voir par exemple Bennett et Raab, 2003), mais la question est de savoir si le résultat obtenu peut ou non être satisfaisant. La vie privée est un utile slogan mobilisateur dans les sociétés individualistes, où la première question posée est « Qu'est-ce que cela change pour moi ? ». Mais les thèmes soulevés ici sont irréductiblement de nature collective, et il est difficile de traiter tous les problèmes posés en référence à un concept dont le développement a été essentiellement individualiste[8].

Une erreur classique se répète *ad nauseam* dans de nombreux contextes ; elle révèle l'ampleur de la méprise qui entoure aujourd'hui la surveillance. Le raisonnement fréquemment avancé est que si nous n'avons rien fait de mal, nous n'avons rien à cacher, et donc rien à craindre. Excellent principe, bien entendu. La jurisprudence occidentale nous a incité à croire en la présomption d'innocence, au respect des droits de la défense, et en l'idée que c'est seulement lorsque la culpabilité a été prouvée par un tribunal que la sanction appropriée est infligée. Le problème est que les choses ne marchent pas ainsi, notamment dans le contexte de la catégorisation sociale, en tant qu'aspect d'un assemblage complexe de pratiques de gouvernance. Opposées aux revendications personnelles d'une innocence individuelle, les pratiques de la surveillance sont profondément sociales, au sens où les individus sont regroupés en catégories, que ce soit de consommateurs ou de délinquants potentiels. C'est l'appartenance ou l'affiliation souvent involontaire d'un individu à certains groupes qui fait toute la différence. Et plus les systèmes sont intégrés et recoupés, plus il devient possible de créer des catégories dans lesquelles on peut capturer des informations personnelles qui conduisent à la singularisation d'une personne en tant que menace, suspect ou cible.

C'est pourquoi les orientations politiques de la surveillance commencent à changer – et c'est pourquoi, si l'on veut contenir les côtés potentiellement négatifs de la surveillance, elles doivent changer. Un éventail de plus en plus large d'études montre que l'accent mis sur les intrusions individuelles et les

violations de la confidentialité est inadapté à la tâche. Les questions de vie privée telles qu'on les entend habituellement ont leur importance, mais ne s'intéresser qu'à elles revient à occulter le sujet du contrôle de l'utilisation des données personnelles. Ainsi, la thématique élargie doit aborder le mode de codage des systèmes, l'identité des créateurs des catégories et les conséquences sur le commun des mortels d'une telle catégorisation sociale.

La raison pour laquelle ces sujets pourraient bien susciter la controverse est que les forces alignées pour recueillir et traiter les données personnelles sont de plus en plus puissantes. La surveillance commerciale du consommateur est désormais une activité multinationale se chiffrant en milliards de dollars. Des bénéfices gigantesques sont engrangés non seulement en amassant et en traitant des données personnelles, mais aussi en en faisant commerce. Les pouvoirs publics, de leur côté, continuent à collecter des données pour des services spécifiques, mais aussi à faciliter des systèmes – tels que l'administration électronique – dont les aspects relatifs à la surveillance sont peu compris, voire reconnus : un système qui utilise un identifiant universel pour procurer l'accès à des renseignements et des services publics offre également des possibilités sans précédent de surveillance et de profilage collectifs et individuels.

Depuis le 11 septembre, un processus en particulier est en plein essor – celui qui consiste à faciliter les croisements de bases de données commerciales et publiques ou policières. On a pu déjà s'en apercevoir dans des domaines tels que l'E911 et des services similaires qui transforment les téléphones portables dotés d'une capacité GPS en instruments de contact d'urgence. Au Royaume-Uni, la loi de réglementation des pouvoirs d'investigation (Regulation of Investigatory Powers Act, datant de 2000, c'est-à-dire antérieure au 11 septembre 2001) prévoyait elle aussi de tels croisements. Mais le programme CAPPS II (Computer-Assisted Passenger Pre-Screening, ou Préfiltrage informatisé des passagers) et d'autres initiatives du même calibre ne font que pousser plus loin de telles interactions intersectorielles. C'est pourquoi cette période qui suit le 11 septembre est si cruciale pour le développement d'une nouvelle politique de l'information adaptée aux dimensions émergentes du problème.

Quelle que soit la solution proposée à long terme, la question demeure de savoir quelle est la meilleure démarche pour atténuer la propagation des aspects injustifiés et néfastes de la surveillance contemporaine. La réglementation en est une parmi d'autres ; elle avance dans la saine direction d'une plus forte responsabilisation de ceux qui traitent des données personnelles. Une telle démarche a toujours été plus caractéristique des réglementations européennes que nord-américaines, même si l'on pourrait soutenir qu'avec la Loi sur la protection des renseignements personnels et les documents électroniques (PIPEDA), dont l'entrée complète en vigueur est

survenue le 1er janvier 2004, le Canada amorce aussi un mouvement dans cette direction[9]. Il est vital d'améliorer la législation pour créer une culture de précaution relative aux données personnelles, et pour résister à l'appétit vorace et insatiable qu'elles suscitent, un appétit qui est encouragé par des cultures de la crainte et de la suspicion de même que par des cultures d'entreprise droguées au marketing personnalisé.

Au XXIe siècle, cependant, au moment où la politique de l'information acquiert une position plus centrale, d'autres acteurs tels que les nouveaux mouvements sociaux, les ONG, les associations de consommateurs et les associations d'internautes prennent conscience de son importance. On décèle des signes du fait que le climat consécutif au 11 septembre sert à alerter des cercles plus larges sur les questions posées par la surveillance, questions qui sont liées à d'autres types d'initiatives. Les mouvements antimondialisation commencent à considérer la surveillance comme une dimension importante de l'action publique, et œuvrent fréquemment au-delà de leurs frontières nationales. Il convient de saluer l'apparition d'évolutions transnationales de ce type, tout en prenant conscience des nouvelles questions qu'elles soulèvent quant à l'ampleur des similitudes que présentent les cultures de la surveillance et du respect de la vie privée selon la nation, la culture et le groupe ethnique. La mondialisation des données personnelles est un processus qui ne peut être compris et appréhendé que dans un contexte à la fois local et mondial[10].

Les grandes questions qui se posent concernent l'opposition entre sécurité et libertés démocratiques, le contraste entre efficience et baisse du contrôle des renseignements personnels, et le champ et les conséquences d'une réglementation par les pouvoirs publics. En ce qui concerne la première question, les médias n'ont pas cessé de présenter la sécurité et les libertés démocratiques comme des alternatives exclusives l'une de l'autre, plutôt que des éléments potentiellement complémentaires. Pour la deuxième, la notion d'efficience a usurpé les objectifs sociaux qui convenaient, suggérant que le « contrôle des renseignements personnels » était d'une certaine façon une « valeur » équivalente. Quant à la troisième, une réglementation étatique est souvent considérée comme le principal instrument réglementaire, alors que les organisations et organismes locaux disposent de nombreuses possibilités d'autoréglementation *dans un cadre* garanti par la loi. Compte tenu de ce qui précède, qui montre à la fois la généralisation des nouvelles techniques de catégorisation sociale et la relative opacité des « représentations de données » (c'est-à-dire des personnes fichées), il est impératif que la politique de l'information soit traitée au titre d'un débat public sur les questions d'opportunité et de choix.

4. Les scénarios de surveillance

Après avoir manifesté un scepticisme certain à l'égard de scénarios qui s'efforcent, finalement, de prédire l'avenir, il convient néanmoins de tenter d'indiquer les directions potentielles vers lesquelles nous entraînent les tendances actuelles. Le doux rêve selon lequel la sociologie pourrait prédire l'avenir semble s'être évanoui. À l'évidence, aucun sociologue n'avait prédit que 1989 serait l'année décisive du démantèlement du communisme, ou que 2001 deviendrait synonyme d'attentats à New York et Washington. Néanmoins, il suffit de décrire les événements et de les replacer dans une séquence signifiante et tendancielle pour justifier la prétention d'une contribution de la sociologie sous la forme de suggestions de solutions substitutives. Nous en présenterons deux ici : l'une dystopique et l'autre davantage porteuse d'espérance.

Commençons par la tendance dystopique. Notre monde actuel n'est pas, dans la plupart des cas, celui de *1984*, même s'il faut bien dire qu'aucun scénario responsable de surveillance ne peut se permettre de faire fi de cette référence classique. George Orwell a mis en avant de très nombreuses caractéristiques primordiales des sociétés de la surveillance, et les a placées dans le contexte de la décence réciproque des êtres humains et de l'intuition élémentaire que la vérité est essentielle pour que la société soit saine (Slater, 2003). Mais il ne pouvait prévoir l'ampleur de l'implication d'organisations non étatiques dans les pratiques de la gouvernance du quotidien, ni une évolution technologique qui, par exemple, donnerait aux autorités la possibilité d'utiliser des bases de données consultables pour créer des catégories de suspects. Son instinct éthique social était le bon, et on ne saurait lui reprocher de ne pas avoir prédit telle ou telle évolution technologique ou politique. Mais il nous incombe d'aller plus loin qu'Orwell – et que certains clichés orwelliens tels que celui de « *Big Brother* » – si nous voulons saisir les éléments d'une dystopie de la surveillance du XXI^{e} siècle.

Si le contrôle de la criminalité en situation et l'usage commercial de bases de données sont devenus aussi importants que nous l'avons suggéré, ils doivent être les principales caractéristiques d'un avenir dystopique. Ils ne sont pas dystopiques simplement parce que les nouvelles technologies semblent avoir pris le dessus jusqu'à, peut-être, menacer d'ôter à l'être humain certains rôles décisionnels essentiels, mais en raison de tendances plus marquées mises en lumière ici. Le simple usage des technologies nouvelles n'est pas en soi une menace ; c'est plutôt le rôle qu'on leur permet de jouer qui soulève des questions sur la viabilité d'un avenir de l'homme. Comme nous l'avons vu, des fragments de données personnelles sont maintenant concaténés pour créer des représentations d'individus auxquelles se réfèrent leurs identifiants. Pour de nombreuses raisons pratiques, ces images et ces profils substitutifs sont

considérés comme suffisants pour déterminer des traitements. Dès lors, l'impasse est faite sur les notions conventionnelles de responsabilité : la moralité cède la place à la gestion.

Il est assez légitime de se demander, à l'orée de ce XXI[e] siècle, si on n'est pas en train de franchir un cap dont il sera très difficile de revenir. Bien entendu, la relation entre les citoyens et l'État ne cesse de subir des modifications mineures, et la fin du siècle dernier a déjà été le théâtre d'une certaine altération de cette relation par laquelle les citoyens ont commencé d'être inféodés à une « mondialité » informe et une réalité d'État. Il semble, par exemple avec l'introduction de la prise d'empreintes de nombreux citoyens non américains aux frontières des États-Unis, que ce seuil soit en passe d'être atteint, dans la mesure où les données corporelles prennent davantage d'importance que la classique description de la personne et que le traditionnel document d'identité. La situation des États-Unis est simplement plus connue ; le même processus se rencontre dans maints autres contextes nationaux. Le corps humain, qui a très longtemps été considéré comme intimement associé et inextricablement lié à la personne, est aujourd'hui vu comme une source fiable et autonome de données, au point que le droit d'entrer sur un territoire puisse être accordé ou refusé sur cette base. D'un point de vue politique, ces corps sans voix ont une place douteuse et inquiétante.

Simultanément, les recours technologiques règnent en maître. Ils constituent le principal moyen d'empêcher l'individu non éligible ou le porteur de risques d'accéder à des sites ou des situations. Dans chaque cas, la complexité des personnes est réduite à des images de données, la justice à des calculs, la moralité à la gestion. La culture du contrôle, avec ses tendances soit à gérer, soit à diaboliser le coupable présumé, découle clairement de l'environnement sécuritaire né du 11 septembre. Comme le soutient David Garland (2001), ces tendances sont aujourd'hui centrales au Royaume-Uni et aux États-Unis, où le contrôle de la criminalité en situation à l'aide de la surveillance (entre autres) est probablement plus avancée que partout ailleurs dans le monde. Leur caractère n'est pas dystopique parce que les technologies seraient en situation de maîtrise ou les tentatives d'abaisser les niveaux de criminalité fondamentalement erronées, mais bien plutôt parce que les approches technologiques et managériales sont privilégiées au détriment de démarches qui prennent la personne ou la justice en compte.

Si ces types de tendances restent non maîtrisés, nous vivrons dans un monde de plus en plus inconnu – ou de moins en moins agréable. La crainte, le secret et la suspicion bourgeonnent, car les nouvelles technologies sont vues comme salvatrices. (Il suffit de penser au nombre d'entreprises de haute technologie qui se dénomment elles-mêmes « Solutions***** ».) Là encore, la quête d'assistance technologique n'est pas erronée en elle-même. Le

problème est plutôt l'apparente absence de volonté de nombreux gouvernements et de nombreuses entreprises de faire examiner des pratiques et des procédures nouvelles tout à fait susceptibles de favoriser une évolution vers des situations sociales et politiques hautement indésirables. Il ne fait pas de doute qu'elles diminuent les possibilités de développement du social, et restreignent le champ du politique.

Un autre scénario pourrait être décrit comme « utopique ». Ce terme n'est utilisé ici qu'au sens d'un futur préféré, pas nécessairement impossible, et issu des conditions présentes. De nombreuses utopies prennent comme postulat un cataclysme ou une révolution quelconque qui marque une scission entre l'ancien monde et le nouveau ; peut-être d'ailleurs devrions-nous faire de même dans notre scénario de rechange. On craint la forme que pourrait prendre une telle évolution radicale ; il est pourtant vrai, malheureusement, qu'aucune réglementation ni législation n'est édictée sans mort d'homme – aussi clairs et impérieux qu'aient pu être les signes précurseurs.

Il y a de bonnes raisons que le tollé populaire et la forte dynamique politique dénonçant les aspects négatifs de la surveillance prennent d'énormes proportions sans la survenue d'un Tchernobyl des données personnelles, mais si ce cataclysme se produisait, on pourrait espérer que le préjudice causé reste tout à fait limité. La tendance nouvelle au bridage de la surveillance s'accorderait bien avec le malaise qui a conduit à l'abandon des programmes TIA et CAPPS II aux États-Unis en 2003. Les organisations impliquées dans la maîtrise de la propagation de mesures de surveillance inutiles et dans l'opposition à leurs abus collaborent déjà de manière bien plus forte, à la suite notamment de différentes réunions mondiales tenues dans les premières années du XXI^{e} siècle, où ont été débattus les intérêts à la fois des entreprises privées responsables et des catégories représentées par les ONG. On entrevoit déjà certaines organisations se montrer beaucoup plus précautionneuses avec les informations personnelles, surtout les plus sensibles ; alors que la vulnérabilité des données personnelles est de plus en plus signalée, de grandes entreprises et des instances publiques pourraient leur emboîter le pas. Des audits des données personnelles sont déjà régulièrement conduits au sein d'organisations, et des conventions transfrontières sur les mouvements de données personnelles limitent fortement les possibilités de transmission des données d'une juridiction à l'autre.

Par ailleurs, dans le scénario utopique optimiste, les contrôles éthiques et la participation démocratique s'exerceraient au cours du processus d'élaboration des nouveaux systèmes de surveillance. Parfois déjà, les informaticiens coopèrent avec les sociologues et les décideurs pour garantir l'éthique du codage et la transparence des catégories vis-à-vis non seulement

des usagers des données, mais aussi des personnes fichées. Il s'agit là d'un domaine des sociétés du XXI[e] siècle dites « de l'information » qui pourrait connaître une croissance potentiellement énorme. Des projets éducatifs pourraient, aussi, s'assurer que les programmes de formation à l'informatique soient axés sur le développement des compétences non seulement de traitement et de manipulation des données, mais aussi de traitement raisonné de toutes les formes d'informations personnelles. Aux deux extrémités de l'échelle sociale, les gens sont si nombreux à constater les prémices des répercussions de la surveillance sur leur vie que la législation a de bonnes chances d'être prise en compte et respectée. Certains pourraient même commencer à envisager une ère où la modestie technologique serait considérée comme tout aussi souhaitable que l'avant-garde technologique, et où les objectifs sociaux passeraient devant les visées économiques.

Ces différents éléments sont bien entendu soumis aux spécificités du contexte national et des conditions culturelles. Les besoins et les attentes varient mais, comme l'a montré l'expérience de la Directive européenne sur la protection des données, il est possible de trouver une base commune.

5. Conclusions

La surveillance est un thème essentiel de l'analyse sociale et politique de ce début de XXI[e] siècle. Elle est aussi une arène cruciale pour le contrôle éthique et le débat sur l'action publique. Elle s'inscrit dans une politique plus large de l'information qui promet de s'étendre au moment où les organisations dépendent de plus en plus des infrastructures d'information. Mais il faut également bien appréhender l'économie politique de l'information qui englobe la surveillance. L'information, et tout particulièrement l'ensemble des renseignements personnels, ont acquis une valeur prodigieuse aux yeux des entreprises qui cherchent à orienter le consommateur vers leurs produits et aux yeux des pouvoirs publics qui sont soucieux, surtout depuis le 11 septembre, de bien adapter leurs dispositifs de sécurité. Le fait que ces deux catégories d'acteurs très puissants militent fortement en faveur de l'accès à des sources toujours plus larges de données numériques, et qu'elles s'associent pour en faire la promotion lorsque leurs intérêts coïncident, signifie clairement que la lutte visant à garantir la présence de garde-fous suffisants pour protéger les individus sera âpre.

Comme nous l'avons indiqué dans l'introduction, l'avenir des sociétés de la surveillance n'est pas du tout une affaire courue d'avance. Ce qui se passe de jour en jour n'est pas le résultat de quelque destinée technologique ou processus social implacable. Bien que ces lignes ne soient pas le lieu d'un tel débat, soulignons que les technologies présentent souvent des compromis ou des limitations qui les empêchent de remplir les espoirs placés en elles. Outre

la rationalité bureaucratique, les organisations obéissent à de nombreux facteurs. L'être humain – cette « représentation de données » abstraite – est savant et réfléchi, parfaitement capable de réagir intelligemment à l'essor des systèmes de surveillance, notamment lorsque ceux-ci semblent fonctionner de manière inéquitable ou inadaptée. Autrement dit, les contingences sont telles qu'aucune prédiction définitive sur les sociétés de la surveillance n'est possible ni souhaitable. Simultanément, prendre du recul pour envisager la direction à long terme des tendances discernables est un exercice utile.

Cela signifie sans ambages qu'il convient de déployer tous les efforts possibles pour comprendre les sociétés de la surveillance et intervenir en leur sein à plusieurs niveaux. Il faut intensifier la recherche pour détailler les conséquences de l'expansion de la surveillance, en particulier dans les domaines de la biométrie, de la génétique, des identifiants universels, de la vidéo (CCTV), des dispositifs de localisation (GPS, RFID) et des flux transfrontaliers croissants de données personnelles utilisées pour l'ordre public et le commerce. Il est également essentiel de mener des recherches dans les domaines de l'éthique et de l'action publique, de manière à fonder les débats des gouvernements et autres autorités sur les tentatives de réglementation des flux de données personnelles, là encore, notamment après le 11 septembre. Il faut aussi prendre des initiatives éducatives, à la fois au niveau général dans les établissements d'enseignement secondaire et tertiaire et spécifiquement au sein des facultés informatiques des universités, de manière à encourager la compréhension contextuelle des processus quotidiens par la prise en compte d'informations personnelles. Des groupes et des organisations agissant aussi bien à un niveau très local que mondial devront travailler à des environnements de gestion des données personnelles marqués par la prudence technologique et un sens aigu de l'équité et de l'ouverture aux autres.

Si l'avenir de la société de la surveillance n'est pas couru d'avance, les orientations actuelles donnent à penser qu'il est nécessaire d'agir de manière urgente, concertée et informée dans différents domaines pour que la puissance de la surveillance ne serve que des buts humains et justes, et exclure ainsi qu'elle puisse engendrer autant de risques qu'elle est supposée en limiter. S'il existe des risques palpables à assumer – avec, c'est d'accord, l'aide de la technologie – dans l'environnement mondialisé et instable du XXI^{e} siècle, il faut bien considérer que parmi eux se trouvent des risques qui sont transmis et augmentés par la technologie. Les entreprises et les pouvoirs publics doivent se rendre compte que rien n'est perdu et que de nombreux résultats vitaux pourraient être obtenus s'ils faisaient bien attention aux conséquences sociales et politiques de l'automatisation du traitement des données personnelles. L'avenir des sociétés démocratiques vivables dépendra en partie du sort réservé à la protection des données et aux libertés civiles : il

faudrait qu'elles ne soient plus considérées comme de simples impedimenta du processus de vente des technologies et de promotion de la sécurité.

Notes

1. Le Canadien Maher Arar, qui a été détenu 374 jours en prison après avoir été déporté en Syrie parce qu'il avait été pris à tort pour un activiste d'Al-Qaida, en est un exemple. Il aurait été torturé. Ce cas n'en est qu'un parmi beaucoup d'autres dans le monde.
2. Le Projet Surveillance est une initiative de recherche en sciences sociales de la *Queen's University* de Kingston, Ontario, Canada (il bénéficie actuellement d'un budget pour 2000-2007).
3. Il semble que le terme a été utilisé pour la première fois par Gary T. Marx en 1985.
4. L'auteur a en tête les salutaires romans de Franz Kafka, *Le procès ;* George Orwell, *1984 ;* ou Margaret Atwood, *La servante écarlate.*
5. Ce critère « déplacé » est une justification courante, par exemple, des dispositifs de surveillance publique vidéo.
6. Le googol est un nombre égal à 1 suivi de 100 zéros.
7. « *Psyte Market Segments* » par le TETRAD : *www.tetrad.com/pcensus/com/py951st.html.*
8. Mais voir à ce sujet les travaux de Priscilla Regan (1995), qui soutient que la vie privée elle-même ne peut être correctement comprise que du point de vue de ses dimensions sociales.
9. Mais voir par exemple Chris Conrath, « Privacy clock strikes midnight », ITWorld Canada.com, *www.itworld.ca/Pages/Docbase/ViewArticle/aspx?id=idgml-5f6a819b-3e80-4bd2-bc04-9be18fc69103.*
10. Le principal programme en cours au titre du Projet Surveillance de la *Queen's University* est une étude coopérative internationale de la mondialisation des données personnelles, envisagée sous l'angle des sciences sociales et de l'action des pouvoirs publics.

Bibliographie

BENNETT, Colin et Charles RAAB (2003), *The Governance of Privacy*, Ashgate, Londres.

BOWKER, Geoffrey C. et Susan Leigh STAR (1999), *Sorting Things Out: Classification and Its Consequences*, MIT Press, Cambridge, Massachusetts.

DANDEKER, Christopher (1990), *Surveillance Power and Modernity*, Polity Press, Cambridge.

ERICSON, Richard et Kevin HAGGERTY (1997), *Policing the Risk Society*, University of Toronto Press, Toronto.

ERICSON, Richard et Kevin HAGGERTY (2000), « The Surveillant Assemblage », *British Journal of Sociology*, 51 (3).

FLAHERTY, David (1989), *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill.

FUREDI, Frank (1997), *Culture of Fear: Risk-Taking and the Morality of Low Expectation*, Cassel, Londres et Washington, p. 4.

GARLAND, David (2001), *The Culture of Control*, University of Chicago Press, Chicago.

GLASSNER, Barry (1999), *The Culture of Fear: Why Americans are Afraid of the Wrong Things*, Basic Books, New York.

HIGGS, Eric (2001), « The Rise of State Surveillance in England », *Journal of Historical Sociology*.

LESSIG, Lawrence (1999), *Code and Other Laws of Cyberspace*, Basic Books, New York.

LIANOS, Michalis et Mary DOUGLAS (2000), « Dangerization and the End of Deviance: The Institutional Environment » dans David Garland et Richard Sparks (dir.), *Criminology and Social Theory*, Oxford University Press, Oxford.

LYON, David (2003a), *Surveillance After September 11*, Blackwell, Malden ; Polity Press, Cambridge.

LYON, David, dir. (2003b), *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, Routledge, Londres et New York.

LYON, David (2003c), « Technology vs. Terrorism », *International Journal of Urban and Regional Research*, 27 (3), p. 666-678.

MARX, Gary T. (1988), *Undercover: Police Surveillance in America*, University of California Press, Berkeley.

NORRIS, Clive et Gary ARMSTRONG (1999), *Towards the Maximum Security Society*, Berg, Londres.

O'NEILL, Onora (2002), *A Question of Trust*, Cambridge University Press, Cambridge.

PARENTI, Christian (2003), *The Soft Cage: Surveillance in America from Slavery to the War on Terror*, Basic Books, New York.

REGAN, Priscilla (1995), *Legislating Privacy*, University of North Carolina Press, Chapel Hill.

ROSE, Nikolas (1999), *Powers of Freedom*, Cambridge University Press, Cambridge.

ROSE, Nikolas (2000), « Government and Control » dans D. Garland et R. Sparks (dir.), *Criminology and Social Theory*, Oxford University Press, Oxford, p. 183-208.

SLATER, Ian (2003) Orwell: *The Road to Airstrip One*, McGill-Queens University Press.

STEPANEK, M. (2000), « Weblining », *Business Week*, 3 avril, *www.businessweek.com:/2000/00_14/b3675027.htm/*.

SUNDAY TIMES (2003), « Are You a Second Class Consumer? », 9 octobre.

TUDOR, Andrew (2002), « A (Macro) Sociology of Fear? », *The Sociological Review*, 51(2).

ISBN 92-64-10773-8
L'économie de la sécurité
© OCDE 2004

Annexe

Liste des participants

Président : **Michael OBORNE**
Directeur, Unité consultative auprès du Secrétaire général, OCDE

Francis ALDHOUSE
Deputy Information Commissioner
Royaume-Uni

David BAXTER
Director, Strategic Relations, Group Technology & Engineering
BT Group
Royaume-Uni

Andrew BRIDGES
Attorney at Law
Wilson Sonsini Goodrich & Rosati
États-Unis

Tilman BRÜCK
Head, Department of International Economics
German Institute for Economic Research (DIW Berlin)
Allemagne

Dagfinn BUSET
Adviser, Emergency Planning Unit
Rescue and Emergency Planning Department
Norwegian Ministry of Justice and the Police
Norvège

Anne CARBLANC
Sécurité de l'information et de la vie privée
Direction de la science, de la technologie et de l'industrie
OCDE

Lutz CLEEMANN
Managing Director
Allianz Zentrum für Technik GmbH
Allemagne

Shana DALE
Chief of Staff and General Counsel
Office of Science and Technology Policy
Executive Office of the President
États-Unis

Bernard DIDIER
Directeur technique et du développement d'affaires
Division sécurité
SAGEM SA
France

Manuel HEITOR
Professor, Department of Mechanical Engineering
Centre for Innovation, Technology and Policy Research
Portugal

Steve HODGES
Technical Director Europe
Auto-ID Lab
Institute for Manufacturing
Cambridge University Engineering Dept
Royaume-Uni

Kevin HURST
Policy Analyst, Office of Science and Technology Policy
Executive Office of the President
États-Unis

Urho ILMONEN
Director, Corporate Relations and Chief Security Officer
NOKIA Corporation
Finlande

Richard A. JOHNSON
Senior Partner
Arnold and Porter
États-Unis

Hiroshi KOJO
Engineer, Corporate Planning Divison
Honda Motor Co. Ltd
Japon

Staffan LARSSON
Director, Head of Analysis Division
NUTEK
Suède

Hyung-Jong LEE
Deputy-Director
Economic Organization Division
Ministry of Foreign Affairs and Trade
Corée

Patrick LENAIN
Conseiller auprès du Chef de Département
Département des affaires économiques
OCDE

David LYON
Professeur de sociologie et
Directeur, Projet surveillance
Queen's University
Canada

Yasuhisa MAEKAWA
Executive Vice President of Honda Motor Europe and
President of Honda R&D Europe
Royaume-Uni

Luigi MEZZANOTTE
CEO
LC Sistemia S.p.A.
Italie

Rudolf MÜLLER
Deputy Head of Directorate
State Secretariat for Economic Affairs (SECO)
Suisse

Clive NORRIS
Professor
Department of Sociological Studies
University of Sheffield
Royaume-Uni

René OOSTERLINCK
Chef du Département navigation
Agence spatiale européenne (ASE)

Jean-Guy PAQUET
Président-Directeur général
Institut national d'optique, Québec
Canada

Gerald QUIRCHMAYR
Professor of Computer and Information Science
University of Vienna, Austria and University of South Australia
and The Bob Hawke Prime Ministerial Centre
Australie

Herwig SCHLÖGL
Secrétaire général adjoint
OCDE

Nam-Niol SEO
Director, Crisis Management Center
National Security Council
Corée

Alfio TORRISI
Senior Executive Vice President
Strategic Planning and Budgetary Control
Istituto Poligrafico e Zecca dello Stato
(Stationery Office and Government Mint)
Italie

Frederik VON DEWALL
General Manager and Chief Economist
ING Group
Pays-Bas

Secrétariat de l'OCDE

Unité consultative auprès du Secrétaire général

Barrie STEVENS
Adjoint au directeur

Pierre-Alain SCHIEB
Conseiller
Responsable des projets sur l'avenir

Concetta MIANO
Assistante

LES ÉDITIONS DE L'OCDE, 2, rue André-Pascal, 75775 PARIS CEDEX 16
IMPRIMÉ EN FRANCE
(03 2004 03 2 P) ISBN 92-64-10773-8 – n° 53478 2004