source : http://www.huygh.fr

Société de surveillance

Anthologie de textes publiés sur le site de François-Bernard Huyghe

BIG BROTHER ET SOCIÉTÉ DE SURVEILLANCE ?

La surveillance (surveiller, c'est "*observer avec une attention soutenue de manière à exercer un contrôle, une vérification*" suivant le Larousse) a plusieurs dimensions. Cette observation attentive peut jouer trois rôles principaux (qui, bien entendu, interfèrent dans la pratique) :

1° La surveillance d'autorité et de normalité. Elle est souvent ostensible (voire symboliquement affichée) et s'incarne dans la fonction que l'on nomme justement du "surveillant" (que ce soit dans une salle d'examen ou dans une prison) : il s'assure que personne ne triche ou ne se rebelle... Le but est alors de contrôler l'application de la norme préexistante et publique. Norme juridique ou réglementaire, norme technique (par exemple pour certifier que les travailleurs produisent le nombre d'heures et de pièces demandées et que la qualité est conforme aux standards), mais aussi norme politique, lorsque les États totalitaires tentent de s'assurer que personne ne "pense mal" ou, du moins, ne l'exprime. La surveillance joue alors un rôle répressif - repérer et punir ou corriger les fautes, que ce soit chez les hommes ou dans leurs productions - mais aussi un rôle dissuasif. Il importe que le sujet se sache surveillé et croie que ses erreurs et déviations seront repérées. La surveillance est liée à l'idée de discipline : bien exécuter des commandements, agir de façon "correcte". Elle impose une conduite, une obligation de faire ou de ne pas faire. Voire une obligation de ne pas penser dans ses formes extrêmes vouées au repérage des dissidents.
C'est généralement à ce type de surveillance que l'on songe en évoquant le spectre de "Big Brother". Dans le roman d'Orwell, elle fonctionne à deux degrés. D'une part Big Brother observe ce que font les citoyens même aux moments les plus intimes pour repérer les déviants et il châtie vite et fort. D'autre part, il fait savoir sur tous les murs que "*Big Brother is watching you*" afin que chacun se sache épié et jugé à chaque moment comme par une conscience absolue : omniprésente et omnisciente. L'anticipation de la surveillance importe autant que ses résultats a posteriori, la punition.
Autre métaphore souvent employée, celle du Panoptique. Il s'agit d'un dispositif architectural imaginé par Jeremy Bentham au XVIII° siècle et qui permet au gardien d'une prison d'avoir une vue sur chaque recoin de chaque cellule. Là encore, le but est double : déceler les fautes, mais aussi développer chez les prisonniers le sentiment de l'infinie supériorité du surveillant qui, tel l'œil de Dieu, les voit sans qu'ils le voient. Dans l'optique de la philosophie utilitaristes, Bentham pensait que ce dispositif était le plus efficace pour corriger les délinquants et développer chez eux, par l'attente de la punition et de la récompense inéluctables, un sentiment moral. La conjonction de la norme, du dispositif technique de vision et du dispositif humain (corps d'éducateurs, gardiens, forces de l'ordre) produit de l'obéissance. Notons que c'est un système qui fonctionne dans des lieux clos et porte essentiellement sur les comportements des sujets enfermés.
Foucault reprit et popularisa cette notion dans *Surveiller et punir* en 1961 : le Panoptique était pour lui la forme paroxystique d'une société disciplinaire où les individus, traités comme des matricules, encadrés et normalisés passaient d'un lieu d'enfermement à l'autre (l'école, le régiment, l'usine; l'hôpital...), chacun soumis à sa norme et chacun avec son système de surveillance spécifique. Une lecture hâtive de Foucault permet de se faire à bon compte une réputation de philosophe d'inspiration libertaire en fulminant à tout va contre le "*biopouvoir*", le *panoptisme* généralisé ou l'obsession sécuritaire. Fort heureusement, la pensée de Foucault était un peu plus riche et il était le premier à souligner que les sociétés de discipline nées avec la révolution industrielle et succédant aux sociétés où le pouvoir reposait sur la souveraineté, étaient en train de disparaître dans la seconde moitié du XX° siècle. Reprenant ces notions,

Deleuze (lui-même relu par Agamben et Toni Negri) opposera les sociétés disciplinaires aux sociétés de contrôle naissant sous nos yeux et où le pouvoir s'exerce sur des individus non pas enfermés mais circulant dans des milieux ouverts, non pas soumis à une autorité centrale, mais à une multitude de réseaux d'obligations d'échanges et appartenances, non pas par l'apprentissage du comportement, mais par le contrôle de l'information. Nous reviendrons sur ce thème.

2° La surveillance de protection et de décèlement précoce (au sens où l'on surveille le feu ou un bébé). Cette fois, il s'agit de distinguer au plus tôt des signes précurseurs d'un danger (ou dans une moindre mesure d'une opportunité, si l'on raisonne en termes de veille économique notamment). Bien entendu, cette seconde forme de surveillance peut se confondre partiellement avec la première (ou en être la justification). Ainsi une vidéo-surveillance peut être, selon le point de vue, un dispositif préventif ou d'alerte destiné à permettre un sauvetage, une intervention urgente, ou un dispositif dissuasif voire répressif, servant à identifier des coupables. Les dispositifs de surveillance/protection sont plutôt orientées vers les "événements" à prévenir que chargés de conformer les comportements et les individus. Il faut noter que nos sociétés allergiques au risque sont favorables au développement de la surveillance dite protectrice, soit au moyen de signaux d'alerte précoce (appareils détecteurs en tout genre), soit par l'installation en amont de dispositifs dit de traçabilité. Ces derniers sont destinés à titre de précaution à inscrire très tôt dans un processus (par exemple de fabrication en usine, emballage ou transport) des marqueurs qui permettront de reconstituer le trajet d'une marchandise dangereuse ou défectueuse. Les dispositifs de surveillance de ce type peuvent être assurés par des humains (fonction "garde-côte"), mais sont surtout de plus en plus délégués à des machines servant à capter, analyser, alerter, retracer. Ceci est vrai pour une chose, comme un médicament, mais également pour une information. Ainsi des logiciels dits de veille de réputation ou d'anticipation des crises peuvent analyser d'énormes flux d'informations sur le Web pour repérer un signal précoce annonciateur par exemple d'une rumeur ravageuse, d'une panique boursière, d'une attaque médiatique, d'un début de crise,....

3° La surveillance stratégique "agressive". Nous entendons par là le fait d'espionner, d'épier pour surprendre un secret, c'est-à-dire pour surmonter des "défenses" dont des moyens de dissimulation. Par "défenses", entendons les moyens de protection dont se dote un individu ou une institution pour conserver la confidentialité d'une information. Ici l'élément de clandestinité et de surprise est décisif : il ne s'agit pas de savoir ce que fait X ou si tel événement est probable, mais d'accéder à une zone protégée. Elle peut être protégée soit physiquement (un papier dans un coffre), soit par un système informationnel (tel un mot de passe), soit par le comportement d'un acteur (il se cache et/ou demande voire impose le silence ou la discrétion à ses proches, à ses employés...), soit enfin par une disposition normative (une loi sur le secret, un code déontologique, une omerta...). Cette surveillance est bien "agressive" en ce sens qu'elle implique, pour aboutir à ses fins, une forme de lutte, de contrainte, de ruse, le surpassement d'obstacles matériels ou la capacité d'imposer sa volonté à des individus (les faire parler, par exemple). Lorsque A tente de violer le secret de B, soit pour se procurer une connaissance précieuse qu'il détient , soit pour apprendre des vérités sur lui (son comportement caché, ses intérêts, ses alliés..). Ce type de surveillance est souvent destiné à connaître les plans et projets d'un adversaire ou d'un concurrent pour gagner un temps d'avance et mieux le contrer ou le précéder. Une très grande partie de l'espionnage

industriel (ou des procédés illégaux qui se dissimulent parfois hypocritement sous le vocable d'intelligence économique) ou des techniques de surveillance clandestine d'un individu, comme en pratiquent les détectives privés, sont destinés à s'emparer de secrets pour les exploiter directement, en les mettant sur la place publique, en les revendant, en manœuvrant avec cet avantage, etc.

Bien entendu, la trilogie n'est pas très difficile à critiquer tant il existe, répétons le, de formes "mixtes" ou de finalités ambiguës. Ainsi, poser un micro dans l'appartement d'un présumé terroriste, est-ce lutte contre un adversaire (3° cas de figure), écarter un risque d'attentat (2° cas) ou participer à la lutte générale de la société contre le crime (1° cas). Nous serions bien sûr tenté de dire que les trois "s'emboîtent" comme des poupées russes. Nous pensons pourtant qu'il est nécessaire de tenter de décomposer des fonctions de la surveillance avant d'employer des notions aussi générales que "société de surveillance". Ce que nous développerons dans des articles à suivre.

Si la surveillance peut répondre à plusieurs finalités, les instruments par lesquels elle s'exerce sont également multiples.
Ils sont de deux sortes, du moins dès que le processus de surveillance dépasse une relation directe et immédiate : organisations humaines et appareils techniques.

Certes la surveillance peut être exercée par un individu seul, surtout sur ses proches, et s'il emploie des prothèses technologiques. Mais elle est plus souvent le fait de corps de professionnels. La liste est longue, du pion placé par l'éducation nationale dans une salle d'examen au service de contre-espionnage utilisant des satellites, en passant par le détective privé ou les nombreuses catégories de contrôleurs, vérificateurs ou certificateurs dont a besoin l'économie.
D'où la question classique du "qui garde les gardiens ?" : quels sont les garde-fous qui empêchent qu'ils n'abusent de leur pouvoir de savoir pour commettre eux-mêmes des fautes ou des délits ? La réponse tient souvent dans l''auto-organisation d'une profession ou d'une fonction (la formation, les codes de déontologie...) ou tout simplement dans la loi. De même que le droit doit réguler le degré de force qui s'exerce dans les rapports sociaux (pour éviter la violence, la menace ou l'abus d'une position dominante), il appartient à la loi de dire qui a le droit de savoir (et de faire savoir) quoi sur qui. Et de fixer les frontières de ce que l'État doit connaître sur ses citoyens, comme ce que des organisations privées sont en droit de rassembler comme renseignement, pour l'exploiter, le publier ou autre.

Ceci vaut pour les règles gouvernant l'accès aux dossiers médicaux ou fiscaux comme pour celles qui protègent les stars contre les paparazzi, la constitution de dossier comme le viol de l'intimité. Pour ne donner qu'un exemple, une partie du projet de loi dite "Lopsi II" de Michèle Alliot-Marie devrait instaurer agrément par l'État après contrôle de la moralité des dirigeants et des objectifs des "officines". Ce terme péjoratif désigne les agences qu'elles soient de détectives privés, de sécurité ou d'intelligence économique dont les excès ont récemment défrayé la chronique. Une partie du projet devrait porter sur une pratique également connue sous un vilain nom, la "*tricoche* " quand d'autres parlent de "*barbouzerie*" : le fait que des fonctionnaires de police ou de gendarmerie, en activité ou en retraite alimentent lesdites officines d'information confidentielles (écoutes, dossiers fiscaux ou bancaires, Stic, le fichier qui regroupe toutes les "infractions constatées"...).

Certes, on pourrait remarquer qu'il a toujours existé des officines, avec les bons réseaux et les bons tuyaux, au moins depuis que Vidocq fondait la première agence de détectives privés. Cependant le marché du renseignement privé s'est développé jusqu'à employer des milliers de professionnels dans des cabinets et agences de tous genres. Et si ce marché se développe c'est qu'il y a intérêt à savoir (et pas seulement chez les maris trompés ou la patrons de supérettes qui soupçonnent des vols de conserves) : protection des secrets de fabrication, repérage d'activités délictueuses, besoin de connaître le passé ou les intentions d'un investisseur, d'un concurrent, du dirigeant d'une association hostile, préparation d'opérations de déstabilisation par médias interposés, obsession sécuritaire, espoir de tomber sur une affaire bien crapuleuse pour écarter un gêneur, recherche d'informations qui donneront un avantage dans une négociation ou la conquête d'un marché, quête d'informations techniques ou autres dont la valeur s'affirme de plus en plus dans l'économie de l'immatériel. Il y a des dizaines de raisons de se livrer à ces pratiques, mais il y a aussi des dizaines de fichiers ou bases de données, en principe confidentiels, dont la consultation peut présenter un intérêt stratégique, éventuellement monnayable.

Mais si la loi donne ou refuse l'autorisation de savoir (et tout ce qui en découle : le droit de ficher, d'enregistrer, de conserver, de s'organiser pour acquérir certaines informations, les vendre les exploiter..), encore faut-il savoir ce qu'il est possible de savoir. Ici intervient le facteur technique : sans dispositifs de traitement automatique des traces, la surveillance se borne à des actes simples : regarder, fouiller, écouter et interroger.

Les technologies, surtout numériques - celles qui servent donc à saisir, archiver et faire circuler des données issues de ces traces - , changent les règles dans plusieurs domaines. Comme chaque fois, la technologie est utilisée pour vaincre l'espace et le temps (donc pour permettre des performances auparavant impossibles ou plus coûteuses en moyen).

Le facteur temps doit s'envisager dans une double perspective : rapidité des opérations de contrôle, mais aussi durée de vie des données : nombre d'actes qui étaient autrefois éphémères et n'étaient connus que de leurs témoins directs sont maintenant enregistrés pour une durée indéterminée. Nous verrons aussi que la technologie sert à vaincre des résistances humaines, des dispositifs de défenses. Rappelons aussi cette évidence : le temps des technologies est un temps bref, et elles se moquent des frontières, tandis que le temps juridique est lent et que la norme protectrice des libertés individuelles est territoriale et ne s'applique que sur un espace soumis à une souveraineté. Il n'y a pratiquement plus de mois où l'on n'apprenne l'apparition d'un nouvel appareil de contrôle ou surveillance encore plus perfectionné (et susceptible de poser des problèmes éthiques ou juridiques). Une fois ce pourra être un drone, une autre un nouveau système biométrique. La semaine où nous écrivons, il s'agit de la "machine à déshabiller" : le scanner corporel qui devrait remplacer la fouille corporelle dans les aéroports en faisant apparaître nus sur un écran ceux qui passent par un portail.

Le domaine plus évident est celui de l'audition et de la vision à distance. Pour reprendre les exemples toujours cités dans le Panoptique de Bentham, c'est la disposition architecturale qui facilite la surveillance à distance. Dans 1984, un dispositif d'État (des caméras partout, des observateurs en nombre...) dont Orwell ne décrit pas le détail mais que l'on suppose énorme. Dans le film "La vie des autres", l'agent de la Stasi chargé d'espionner un couple

d'intellectuels doit mobiliser du personnel, une pièce entière, de lourds appareils dont des écouteurs à l'esthétique très soviétique. Mais aujourd'hui, dans la réalité, caméras et micros capables de transmettre le son à distance sont à la portée de chacun. Une simple webcam - pas très difficile à dissimuler- et un minimum de câblage permet, par exemple à un patron pas trop scrupuleux, de savoir de chez soi ce qui se passe dans son établissement. Mais le facteur "télé" (télésurveillance, télédiagnostic, téléexpertise dans le domaine de la santé p.e.) est appelé à se développer avec chaque fois les problèmes d'identification, transfert, conservation, droit d'accès aux données...

Complémentaire, le domaine de l'enregistrement et de la transmission. Plus besoin de kilomètres de pellicule film (chère) ou de bande enregistreuse analogique. La numérisation du son, de l'image, et des données leur donne des caractéristiques nouvelles. Devenues des suites de bits électroniques, les données peuvent être stockées en quantités énormes, reproduites à l'identique sans perte de qualité, transférées d'un appareil à l'autre. Et, bien sûr indexées. Accessoirement, elles peuvent être falsifiées avec une finesse inconnue à l'époque où l'on noircissait Trotsky sur les photos argentiques où il figurait à côté de Lénine.

La miniaturisation des appareils capteurs et enregistreurs est également une caractéristique nouvelle : ainsi avec des puces RFID vraiment invisibles (éventuellement introduites dans un objet, voire dans un corps animal ou humain), l'objet espion se glisse partout. Dans ce dernier cas, il ne se contente pas de se rendre indécelable pour rendre son porteur, chose ou être vivant, repérable à distance. Il est aussi porteur d'information et raconte le passé et les caractéristiques de ce qu'il marque. Cette boîte de crème a été achetée à tel rayon, ce véhicule est passé par ici et par là, ce chien a tel numéro d'immatriculation qui permet à n'importe quel vétérinaire de l'identifier. Les nanotechnologies pourraient être une des voies royales de cette miniaturisation généralisée.

Autre catégorie qui se confond souvent avec la précédente : celle des balises en tous genres. Il existe une multitude de marqueurs invisibles ou discrets qui permettent de géolocaliser un véhicule ou un objet. Et si l'objet en question est constamment porté par une personne, soit de force comme les bracelets qui surveillent les déplacements des condamnés, soit par commodité comme un téléphone portable, il devient très facile de savoir qui est où et à quel moment.

Mais la miniaturisation et la dissimulation de véritables "micromachines à espionner", comme des caméras qui se glissent sous des portes ou des enregisteurs de frappe sur un clavier (*keyloger*) progressent. les "boutiques des espions" (*spyshops*) offrent au particulier un matériel qui aurait étonné dans les films de James Bond d'il y a quelques années. La "machine à espionner" peut d'ailleurs être purement algorihtmique : un logiciel glissé dans un outil de communication de la personne surveillée (son téléphone portable, par exemple) peut la rendre traçable dans le moindre de ses déplacements, *interceptable* lors de chacune de ses conversations...

Des instruments de traitement de l'information destinés à interpréter des indices. Ainsi un simple particulier, faisant éventuellement appel à des laboratoires étrangers pour faire des analyses (génétiques p.e.) qui ne seraient pas autorisées en France, peut rivaliser cette fois non plus avec les héros des films d'espionnage, mais avec les "Experts de Miami" et autres

séries TV basées sur la criminalistique (les *forensic sciences* des anglophones). À noter que le même citoyen français pourra se procurer hors frontières quelques logiciels, qui, une fois installés sur le téléphone GSM qu'il désire surveiller, lui retransmettront les conversations (orales ou écrites avec les SMS), les numéros des correspondants, la date et le lieu des appels...

Par ailleurs, certaines informations émergent du traitement d'une multitude de données qui isolément ne présentent guère d'intérêt (Monsieur X a fait tel achat tel jour, a franchi tel portail d'autoroute tel autre jour). Par traitement informatique, le rapprochement de cette pluralité d'éléments peut permettre soit le "profilage" plus fin d'un individu, dont on connaîtra mieux les goûts et les réactions, soit un traitement statistique des grands nombres assignant à telle ou telle catégorie (bon consommateur, potentiellement dangereux, débiteur peu fiable) de masses d'individus.

Si la surveillance est si invisible, cela tient aussi au fait que nous confions nos secrets, mais aussi la réalisation ou l'accompagnement de nombre de nos activités (donc aussi leur mémoire) à des processus invisibles, virtuels, informatisés. Pour notre commodité ou notre sécurité, nous faisons sans cesse appel à des modes de traitement de l'information à distance : pour faire un achat, éventuellement par Internet et via un identifiant, communiquer, nous déplacer... Nous devons en particulier nous identifier, présenter une carte, un badge, taper un numéro de code, effectuer une signature numérique. Par là même, nous signalons à un éventuel système de surveillance ce que nous avons acheté, fait, communiqué, et peut-être même pensé ou désiré. La question de l'identification numérique ou de la signature à distance (avec son corollaire le risque de vol ou de falsification d'identité) est cruciale pour le commerce numérique, par exemple, et les enjeux de ce type de vérifications en termes de sécurité et de liberté sont énormes. La nécessité de "prouver qui l'on est" soit en effectuant certains actes (taper un code par exemple) soit en se révélant porteur de certaines données (p.e. biométriques) tient notamment une grande place dans le plan Numérique 2012 présenté par Éric Besson.
Les contradictions des simples citoyens qui peuvent être un jour indignés de l'établissement d'un fichier officiel, mais le lendemain mettre eux-mêmes en lignne des informations extrêmement intimes sur les réseaux sociaux de type Facebook, ont souvent été soulignées, notamment dans les conférences internationales sur la vie privée. L'interpénétration de l'espace public et de celui de l'intimité ne sont pas le moindre facteur qui favorise la surveillance et le renseignement.

Tout système de surveillance se heurte à des normes - celles qui règlent le droit d'un citoyen a conserver une zone d'intimité, ne serait-ce que pour ne pas risquer de pressions, ou le secret industriel par exemple - mais aussi à des résistances de fait (par exemple celle des internautes qui militent pour l'anonymisation).

Encore faut-il comprendre comment s'organisent ces rapports.

Du comportement au données

Premier cas : la surveillance porte sur le comportement. Le but est de savoir ce que fait ou où se trouve X ou d'observer une catégorie d'individus Y. Cela peut se faire par observation

directe - le fameux dispositif panoptique p.e. -, avec des appareils comme des vidéo-caméras ventuellement dissimulés, en recueillant des témoignages, etc. Dans d'autre cas, la surveillance comportementale n'est pas destinée à une cible nommément identifiée ou une catégorie (les employés, les visiteurs munis de badge, les prisonniers...), mais sert pour repérer dans une foule. Certains logiciels et certaines méthodes permettent par exemple de déceler des comportements suspects : telle personne parmi des milliers d'autres se déplace trop vite ou pas assez, ou suit un trajet aberrant par rapport à la majorité, ou fait tel ou tel geste répertorié comme suspect ; on s'intéressera aussitôt à la personne ainsi ciblée.
S'ajoute la famille des balises ou appareils du même type. Soit en émettant un signal, soit en cherchant à se connecter sur des antennes de communication, en franchissant des dispositifs de contrôle de type portails ou en opérant lui même pour se repérer (un GPS p.e.), un appareil ou une simple puce RFID peut à tout moment indiquer la position de son propriétaire. Mais la connaissance que fournit le dispositif (le fameux ce que fait et où est X) est généralement ignorée de la victime (sauf dans cas comme celui d'un prisonnier qui porte un bracelet à balise dont il sait parfaitement qu'il est destiné à faire connaître ses déplacements).
Soit l'exemple du téléphone et de sa géolocalisation. Celle-ci peut s'effectuer de diverses manières :
Elle peut résulter d'indications fournies à la justice par un opérateur téléphonique, sur le passé (d'après ses factures, X a appelé depuis telle borne à tel moment), sur le présent (X sur écoute est en train de téléphoner de telle zone géographique desservie par telles antennes) et enfin il existe des techniques qui ne portent pas exactement sur le futur, mais qui, du moins, permettent de savoir à tout moment où est le portable de X, même s'il ne l'utilise pas, donc sans doute de déduire vers où il se dirige.

La géolocalisation existe sous forme volontaire (service fourni par l'opérateur, par exemple, aux parents qui craignent que leur enfant ne se perde ou soit enlevé). Quand elle est réalisée sur réquisition du juge, elle sert à situer où est une personne suspecte, mais aussi à retrouver un disparu. Enfin, il est possible à des pirates informatiques, glissant le bon logiciel soit directement sur le téléphone de la victime (un proche sans connaissances techniques très poussées peut le faire), soit chez l'opérateur d'obliger un téléphone à se localiser.

La surveillance du comportement s'exerce par définition sur des gens qui ne cessent de passer d'un espace privé à un espace public (il s'est d'ailleurs élevé tout un débat à propos de la vidéo-surveillance pour savoir où s'arrête l'un et l'autre). Il est des exemples où la question ne se pose même pas : un voisin qui place un caméra cachée dans notre salle de bain ou un propriétaire de local qui en truffe les toilettes ne pourra pas plaider l'innocence. Mais dans de nombreux cas, des actes publics (par exemple X a utilisé son téléphone en pleine rue dans telle ville, tel jour, telle heure, sans se cacher de qui que ce soit) prennent un tout autre sens quand il sont analysés par un dispositif de surveillance ignoré du sujet (X ne sait pas que son téléphone est géolocalisé).

La surveillance peut également porter sur des messages. Ici, le problème se pose en terme différents, puisque chacun peut s'attendre légitimement à ce que son message ne parvienne de son seul destinataire. Il faut un dispositif clandestin pour qu'il puisse être lu ou écouté. Qu'il s'agisse d'une lettre, d'un appel téléphonique ou d'un courrier électronique, chacun s'attend à ce que la loi et des dispositifs technlogiques fiables (cryptage dans le cas ces communications électroniques par exemple) assurent cette confidentialité. Or celle-ci peut être compromise de

diverses manières.
Pour les communications électroniques, la procédure normale légale passe par une réquisition faite à un opérateur ou fournisseur d'accès de rediriger les flux d'électrons vers un dispositif d'interception des forces de l'ordre (sans oublier à titre commémoratif les écoutes pratiquées par "bretelles" sur les vieilles lignes analogiques fixes). Mais il existe des possibilités d'intercepter sans passer par la procédure légale en corrompant des gens chez les fournisseurs d'accès et/ou en introduisant des logiciels dans leurs ordinateurs. C'est ainsi que les journaux ont pu avoir connaissance d'un SMS entre le président de la République et sa seconde épouse (si l'histoire est vraie et si le SMS n'a pas été inventé). Mais c'est surtout ainsi que s'est développé un important scandale en Grèce (presque totalement ignoré par la presse française) : la découverte d'un logiciel espion chez le principal opérateur national. Il permettait sans doute à une puissance étrangère d'être au courant des communications des hommes politiques et de nombreuses personnalités grecques au moment des jeux olympiques d'Athènes.

D'autres méthodes fonctionnent non pas en se plaçant au nœud de circulation des communications (chez l'opérateur ou le fournisseur d'accès Internet), mais au plus près des machines, en piratant des ondes (par exemple, en cas d'utilisation de Blue Tooth ou du Wifi), en faisant pénétrer sur un téléphone ou un ordinateur un logiciel malveillant, tel un cheval de Troie, qui permettra à un étranger d'intercepter tout ce qu'émet ou reçoit le téléphone ou l'ordinateur.

Par ailleurs l'interception d'énormes quantités de messages (et non pas la surveillance d'un individu ou d'un appareil précis) comme dans le cas du système Echelon fonctionne sur le principe de la nasse : pécher énormément de données puis les faire traiter par des robots sémantiques pour retrouver les contenus significatifs. Cette méthode est orientée contenu (mot clés par exemple) et non pas interlocuteur (on surveille X ou Y).

La surveillance du comportement et l'interception des messages ont un complément commun qui a déjà été longuement évoqué : le traitement des traces électroniques. Certains parlent déjà de "dataveillance", un néologisme formé de "data (données) et de "surveillance". Elle recouvre la capacité de contrôler l'ensemble des traces électroniques que nous laissons partout à l'occasion de multiples transactions (achat avec une carte bleue), déplacements (utilisation d'un passe Navigo dans le réseau de la Ratp), ou commutations (connexion à un site, opération à distance avec une banque, une société..), plus bien entendu toute les données qu'autrui accumule sur nous dans une multitude de fichiers.
La conjonction peut être redoutable : fichage général et conservation de mémoires électroniques, plus dataveillance, plus datamining (techniques qui consiste à traiter d'énormes quantités de données d'une multitude de sources pour en déduire par traitement de masse des connaissances sur les comportement de consommateurs, ou d'une catégorie d'individus profilés). Les machines à profiler peuvent fonctionner dans les deux sens : rapprochement de multiples indications convergentes sur un même individu (ce qui suppose de pouvoir faire le lien entre ses identifiants électroniques comme ses login et son identité de personne physique), mais aussi traitement de masse de catégories entières d'individus, notamment dans des buts commerciaux. À la différence de deux catégories précédentes, cette surveillance ne pose pas (ou pas seulement) un problème d'espace privé ou de confidentialité : elle repose sur des propriétés de l'informatique. Celle de conserver des mémoires d'une part (ainsi même si Internet a la réputation d'être le royaume de l'éphémère, rien n'y disparaît vraiment en

réalité). Celle de rapprocher des éléments épars entre un grand nombre de lieux d'archivages, souvent des choses très triviales (X a pris le train tel jour, il a acheté des fleurs tel autre) pour en déduire des connaissances vraiment intrusives ou pour créer des catégories discriminantes (repérage des bons prospects ou de mauvais consommateurs par des entreprises, des banques ou des assurances, par exemple).

BANALISATION

La question de la surveillance des citoyens est soulevée chaque jour par une révélation à propos des caméras vidéo, des puces RFID, des balises et de la géolocalisation, du développement des capteurs, de la biométrie et des analyses génétiques, comme par la banalisation des outils d'espionnage, d'enregistrement ou de traitement de l'information confidentielle. Ou encore, il est question de backdoor, de hacking, de phishing, cyberdélinquance et autres anglicismes et néologismes que tout le monde ne connaît pas encore mais dont tous peuvent être victimes.

Exemple du jour : un article du Monde rappelle les soucis qu'ont à se faire les 70 millions d'utilisateurs très approximativement recensés des Facebook, LinkedIn, Copainsdavant, MySpace et autres HI5 où tant de gens déposent des "profils" et invitent leurs amis à constituer des réseaux sociaux. C'est un terrain de chasse idéal pour les escrocs qui piochent des informations librement accessibles qui leur permettront d'emprunter une identité, quitte, le cas échéant à faire circuler des programmes malveillants déguisés en jeux et permettant de recueillir les données personnelles des naïfs.

L'idée s'est largement imposée que nous nous dirigions vers une société de surveillance conjuguant possiblités technique d'espionner et ficher les citoyens, obsession sécuritaire, biopolitiques, dispositifs panoptiques de prévention des désordres... Un livre comme celui, encore récent, d'Atmand Mattelart "La globalisation de la surveillance" en est assez emblématique.

Plus généralement, la révolution numérique a engendré ou s'est accompagnée d'effets complexes et changeants :

- la traçabilité des opérations numériques et des déplacements des personnes, voire des choses, toute transmission ou transaction tendant à s'inscrire quelque part dans une mémoire conservant les souvenirs d'un passé,
- le fait que, parallèlement, les objets (puces RFID) et les machines deviennent de plus en plus "intelligents" et surtout ont une mémoire de leurs usages quand ils ne deviennent pas "géolocalisables" ou n'indiquent pas où est leur propriétaires
- la multiplication des capteurs servant pour enregistrer le son et l'image dans des conditions jusque-là impossibles, micros, caméras, etc., plus la faculté de stocker ces données sans difficulté
- l'interconnexion de systèmes de communication et de bases qui sont autant d'occasions d'intercepter des données ou de les rapprocher pour en retirer un savoir (donc un pouvoir) sur un individu ou une organisation,
- la découverte incessante de failles sécuritaires dans les systèmes de communication en perpétuel renouvellement : elles stimulent l'ingéniosité des inventeurs de programmes malveillants, et machines ou algorithmes qui servent littéralement à prendre le pouvoir sur d'autres machines à l'insu de leur propriétaire,
- la facilité qu'il y a de violer l'intimité d'autrui, soit en achetant machines ou logiciels, soit en reproduisant des méthodes dont la documentation est très accessible sur la Toile
- la désirabilité des données confidentielles en termes économiques, qu'il s'agisse d'intelligence économique, de marketing, de sécurité, d'espionnage privé ou d'État, de

malveillance, de recherche du sensationnel médiatique (sans même parler de la recherche de l'exploit gratuit ou du vandalisme)
- la montée en puissance des outils dits de « fouille de la réalité » : les méthodes qui permettent d'analyser les échanges et déplacements des individus dans la vie réelle et sur le Web pour retracer leurs interactions sociales
- la disponibilité de données privées, parfois laissées par la personne concernée en toute bonne foi set qui se prêtent à collecte, traitement et exploitation abusive
- la capacité de publier sur Internet des informations, textes ou images, sur quelqu'un anonymement, sans frais et avec de bonnes chances de toucher un public considérable
- la multiplication d'organisations, officines, services, groupes militants ou criminels qui ont en commun de s'emparer d'informations confidentielles pour les exploiter.

La liste n'est pas close : il faut aussi tenir compte de la banalisation des outils de surveillance. Un mari jaloux, un patron soupçonneux, mais aussi une « officine » qui utilise du matériel de haute technologie n'a guère de mal à se procurer ce qu'elle cherche dans des «*spy shops*» (les boutiques de l'espion) sur Internet. En quelques clics, vous pouvez acquérir sur Internet des micros ou caméras cachés, des détecteurs de cellules sexuelles ou de restes de drogues pour savoir ce que votre ado a fait Samedi soir, des moyens de réaliser des tests génétiques pour savoir s'ils sont vraiment de vous, mais aussi un matériel plus coûteux à rendre jaloux de vrais espions ou les personnages des *Experts à Miami* : scanners pour ondes Wifi, micros directionnels... Et si ce n'est pas légal en France, qui va contrôler le paquet postal que vous recevez.

Il est justes de parler de banalisation de la surveillance en un double sens.

Il devient banal d'être surveillé, même si l'on est un citoyen ordinaire qui ne fait l'objet d'aucune mesure de justice, ne détient pas de secrets redoutables ou n'a pas une activité d'une quelconque dangerosité.
Par ailleurs, la surveillance ou l'espionnage potentiels s'applique à nombre d'opérations quotidiennes et triviales : passer par une caisse ou un guichet, donner son identité à distance, accéder à des biens immatériels par un abonnement, que ce soit dans un but d'information ou de distraction, prendre un badge, appeler un proche, se connecter sur Internet, traverser certains espaces publics, acheter un objet ordinaire avec « étiquette intelligente »… Bref, nous découvrons que nous possédons tous des données personnelles sensibles et que le « misérable petit tas de secrets » que nous sommes et dont parlait Malraux intéresse d'importantes machines.

La nature de l'information qui attire la surveillance y compris illégale est en effet très vaste. Cela va depuis des données de transactions qui prennent sens traitées avec des milliers d'autres, ou depuis les indices d'éventuelles infractions mineures jusqu'à des secrets de haute valeur économique technique ou politique. Le préjudice pour les victimes peut varier d'une légère gêne, d'une petite humiliation voire d'une perte d'argent minime (quelques appels à un numéro payant…) jusqu'à une vie bouleversée (à la suite d'une publication ou d'un vol d'identité) ou à une grave affaire d'espionnage industriel.

En corolaire, chacun peut être tenté de devenir surveillant à son tour par précaution, par anxiété, par curiosité, par jalousie…, et de franchir, sans peine et presque sans frais, la frontière qui sépare la protection de ses proches ou de ses biens du viol de l'intimité d'autrui.

Une sorte de privatisation et de prolifération de l'espionnage se dessine ainsi.

Deux pistes à retenir :

- le rapport *Big Brother* / *Little Sisters;* Autrement dit : faut il plus craindre l'État ou les sociétés privées, légales ou criminelles, qui tentent d'exploiter ces données pour le profit ? Les services officiels sont-ils performants pour espionner le citoyen (à supposer qu'ils le veuillent à tout prix et que les garde-fous légaux ne les en empêchent pas en démocratie) ? Voir les exemples traités sur ce site de l'inutilité d'Echelon, de la "Communauté de l'Intelligence", et de la surveillance *high tech* ? à leur propos, nous avions proposé le slogan provocateur "Big Brother est-il un Gros Nul ?". Voir encore de la très relative efficacité des interceptions de télécommunications. Les acteurs privés seraient-ils davantage à redouter ? la question mérite au moins d'être posée. Nous finirons peut-être par moins redouter un État surveillant qu'un État incapable de savoir qui surveille qui. Moins un ordre sécuritaire global qu'un désordre favorable aux stratégies privées de surveillance. De même qu'il monopolise la violence légitime, le pouvoir régalien doit limiter les moyens de violer des secrets. Le contrôle des instruments techniques sur et à partir de son territoire devient cruciale : plus la question est technique plus elle est politique.

- Au total plutôt qu'un schéma Un contre Tous (l'État Big Brother écoutant pour surveiller et prévenir), il faut se représenter une pyramide des « écoutés ». Tout en bas, il y a le citoyen ordinaire, impuissant face au viol banalisé de sa vie privée y compris par des particuliers. Au-dessus, le monde des initiés, pas forcément tous délinquants, mais capables de s'assurer un anonymat raisonnable par quelques techniques de furtivité. Au sommet de la pyramide, les détenteurs de secrets importants, dont on ne sait trop s'ils sont toujours à la merci d'une officine qui met tous les moyens pour les intercepter, ou si les contre-mesures (elles aussi coûteuses et complexes) qu'ils adoptent les protègent. Au total la question technique se révèle aussi être une question stratégique.

- Peur de Big Brother ?
Quand l'État ne peut pas tout écouter

Croyez- vous vraiment que l'État sache tout ? Qu'à l'ère numérique, un service mystérieux doté des moyens et des ordinateurs les plus sophistiqués soit en mesure de voir tout ce que vous faites ou au moins d'écouter toutes vos communications ? Sur ce dernier point au moins, les ennemis de Big Brother ont quelques raisons d'espérer: il y a des limites juridiques, économiques et surtout techniques à "l'écoutabilité" (vilain mot pour vilaine chose).

Les limites juridiques varient considérablement suivant les pays. En France, il existe une séparation canonique. D'une part, les interceptions de communication judiciaires (qui demandent une réquisition d'un juge d'instruction ou d'un procureur dans certains cas), le plus souvent réservées à des enquêtes sur des délits d'une certaine gravité, limitée dans leur objet et leur durée, etc. D'autre part, les fameuses interceptions administratives qui ne sont plus vraiment au bon plaisir du Prince. Certes, il y eut autrefois les écoutes de l'Élysée et le détournement de lignes pour écouter 150 personnalités qui ne menaçaient guère la République (comme Carole Bouquet ou Jean-Edern Hallier). Depuis la loi de 1991, ces pratiques sont encadrées par une commission qui est censée vérifier qu'elles correspondent bien aux cas très restrictifs où quelques ministres peuvent en demander : les écoutes sont contrôlées et quant à leur opportunité, et quant à leur durée (les magistrats allant parfois mettre le casque sur les oreilles pour éviter d'éventuels abus). Le système français n'est certainement pas parfait ; il donne certainement lieu à des abus (comme la fameuse "tricoche", la méthode qui permet à des officines privées, souvent tenues par d'anciens policiers, d'obtenir d'officiers de police judiciaire qu'ils glissent subrepticement leurs demandes d'écoutes parmi les "officielles").

Un hebdomadaire prétendait il y a quelque mois qu'il existait plus de 100.000 écoutes "sauvages" (donc totalement illégales) plus de trois fois les 25.000 "judiciaires" (auxquelles s'ajouteraient les 5.000 "administratives"). C'est possible et c'est invérifiable. Et, quand l'on sait quel type de matériel vendent les "spy shops", les "boutiques des espions" sur Internet, on imagine facilement qu'une officine qui veut faire pirater le téléphone portable d'une personnalité y parvient (non sans frais considérables), mais ces pratiques sont illégales et ne peuvent servir que marginalement et clandestinement d'éventuels services d'État.

La situation légale de notre pays n'est pas la plus inquiétante comparée à quelques autres : les USA où même Obama a du renoncer à sanctionner les écoutes illégales "antiterroristes", l'Italie où on peut lire les écoutes de n'importe quelle personnalité dans la presse, la Suède où une récente loi permet à l'Agence Militaire Suédoise d'intercepter de nombreuses télécommunications (téléphone ou courriel) censés entrer et sortir du pays. Outre les exemples que nous avions évoqués ici, il suffit d'ouvrir un journal pour apprendre que le Liban est secoué par une affaire d'écoutes téléphoniques illégales, tandis que la Tchécoslovaquie se débat avec le problème de la publication des écoutes illégales et que les Grecs ne sont toujours pas venus à bout du "Watergrec ", l'énorme affaire remontant aux jeux olympiques de 2004 : un logiciel espion infiltré chez le principal opérateur du pays et qui avait permis à une mystérieuse puissance étrangère d'écouter l'élite politique du pays. Ce n'est pas faire preuve de chauvinisme de dire que le système de protection des libertés français n'est pas le plus problématique du monde, même s'il existe de multiples façon de contourner

la loi

Les limites financières ont déjà été évoquées ici : jouer les Big Brother coûte cher. Déjà les écoutes judiciaires (un des plus gros postes avec celui des analyses ADN dans les frais de justice) grèvent facilement le budget du ministère de la Justice de plus de 80 millions d'euros. Une surveillance de millions de citoyens coûterait certainement des sommes qu'il serait impossible de financer ou, en tout cas, de dépenser discrètement dans le budget de l'État.

Mais les limitations techniques ? A priori, on pourrait penser que tout ce qui est numérisé est traçable donc écoutable. Et qui n'a lu dans une revue d'informatique un article terrifiant racontant comment un pirate peut transformer votre téléphone portable même éteint en balise pour vous géolocaliser, voire pour transformer votre GSM en micro d'ambiance ?

Dans le cadre d'interceptions légales, tout ce qui passe une fois par l'ordinateur d'un opérateur chargé le router vers son destinataire semble susceptible d'être intercepté. Le même raisonnement vaut également pour un fournisseur d'accès à Internet (les FAI) : sur la Toile, les éléments communiqués voyagent certes par «paquets» et cryptés, mais il y a le plus souvent un point de passage fixe : l'ordinateur du FAI. Celui-ci, dûment requis par le juge, doit en principe être en mesure de retransmettre ce qu'il reçoit. C'est particulièrement évident avec les courriels. Chacun sait que les messages électroniques qu'il a envoyés passent par des boîtes à lettre (ce qui permet de les consulter même d'un ordinateur qui n'est pas le sien, en rentrant sur le site de son fournisseur d'accès). Or les boîtes à lettre numériques, comme les boîtes à lettre physiques sont susceptibles d'être visitées par la police.

Ceci sur le plan des principes. Dans la réalité, la règle "point de passage unique égale moyen de tout savoir" souffre des exceptions : difficulté d'identifier les FAI ou opérateurs dans certains cas (notamment lors d'échanges avec l'étranger, si plusieurs intermédiaires interviennent par exemple pour faire chuter les coûts et que l'appel passe sur le réseau le moins cher), problème d'agir sur des opérateurs hors frontières, incapacité technique de conserver les données chez certains fournisseurs d'accès, apparition d'un nouveau protocole ...

Certains pays tentent d'assurer «l'écoutabilité» des nouveaux systèmes de messageries qui apparaissent sur leur territoire, parfois avec un succès modéré16. Car le politique est souvent en retard sur le technique. Ainsi la fameuse loi "Calea " aus USA.

Soit un exemple d'actualité : le fameux système Skype, 338 millions d'utilisateurs à travers le monde, le plus emblématique des messageries recourant au VOIP (Voice over Internet Protocol). L'utilisateur de Skype peut téléphoner gratuitement d'ordinateur à ordinateur (à condition, bien sûr d'avoir un micro et un casque ou un amplificateur), faire des téléconférences avec plusieurs correspondants, et même voir son correspondant et être vu de lui.

Ceci peut fonctionner d'un ordinateur portable. Ainsi l'auteur de ces lignes pourrait aller au

café du coin avec son ordinateur portable, se brancher sur un réseau Wifi gratuit fourni par le commerçant, et parler avec un correspondant à l'autre bout du monde, s'il ne craignait de déranger ses voisins ou d'être interrompu par le garçon de café énervé par le comportement de son client bruyant. Il pourrait également appeler des téléphones fixes ou mobiles (à coût simplement réduit), envoyer des SMS, bref faire à peu près tout ce qu'il fait sur son téléphone mobile. Il existe des été "téléphones Skype", des combinés qui ne sont pas à proprement parler des ordinateurs, mais permettent de téléphoner sur Skype, partout où ils peuvent se brancher sur Internet.

Pour décrire le processus technique en termes simples : A se branche sur n'importe quel fournisseur d'accès Internet (donc pas forcément du sien), de n'importe quel ordinateur, s'identifie auprès de Skype par une adresse et un code (mais rien ne permet nécessairement de relier son «pseudo» à un possesseur physique puisqu'on peut très bien s'abonner à Skype d'un cybercafé, par exemple, que l'on ne paie rien et que l'on ne présente aucun document). A se connecte à B doté d'un identifiant dans les mêmes conditions. Les paroles de A et de B (voire leurs images s'ils ont décidé d'utiliser de Webcams) sont cryptées par le système Skype et passent de «pair à pair» (P2P pour peer to peer). Les "paquets" de données cyrptées voyagent sur Internet. Il est important de comprendre qu'il n'y a pas l'équivalent d'une boîte à lettre (tout est instantané), ni d'un ordinateur central et que tout passe par un réseau P2P toujours changeant et qui n'est sous le contrôle de personne, même pas de la compagnie Skype.

Conséquence ? Il suffit de voir la presse italienne (mais le problème pourrait parfaitement se poser en France). Le ministre de l'Intérieur, Mr. Marioni vient de financer une recherche sur les moyens d'intercepter Skype (comme l'avait fait en son temps le FCC américain, sans trop de résultats). Selon le autorités italiennes, les mafieux (et en particulier les bandits calabrais de la redoutable Ndranghetta spécialisée dans les enlèvement avec torture) se seraient convertis au VOIP. En Italie où l'opération "mani pulite" contre les politiciens corrompu, la lutte antiterroriste et la lutte antimafia doivent beaucoup de leurs succès à des écoutes téléphoniques, l'affaire est d'importance. Il est vrai qu'en Italie aussi on peut entendre des publications "sauvages" d'écoutes de Berlusconi et que la Rai peut transmettre les conversations entre tueurs de la mafia enregistrée par les micros de la police. Bref, même si Berlusconi tente de faire restreindre les écoutes à des cas de grande criminalité et de terrorisme (et surtout pas aux affaires financières), personne n'a envie que les mafieux puissent communiquer en toute impunité.

Carmen Manfreda responsable de la recherche lancée par l'Italie et qui doit s'étendre à tous les pays européens via l'Eurojust (l'unité de coopération judiciaire de l'Union Européenne) déclare : "La possibilité d'intercepter les communications téléphoniques par Internet un isntrument essentiel de la lutte contre la criminalité organisée."

Où est le problème ? Il est double.

D'une part le système cryptologique de Skype est très "musclé" (pour les spécialistes, il combine les système RSA et AES Advanced Encryption Standard) et cette fonctionnalité ne peut pas être désactivée. Or ce système très solide - donc qui demanderait d'immenses moyens de cryptanalyse - est à peu près à Skype ce qu'est l'équivalent de la formule du Coca Cola pour la célèbre firme : sa raison d'être.

D'autre part le trafic P2P de ce type ne peut être contrôlé : nul ne sait par où il passe, ni où trouve un "nœud" d'interception.

Que pourraient faire les autorités ?

Les Allemands, déjà confrontés au problème, avaient songé à crée un "Cheval de Troie d'État", comprenez un logiciel malveillant, probablement fabriqué par les services secrets avec l'aide de quelques pirates recrutés pour la circonstance, et qui serait rentré chez la société Skype (société de droit luxembourgeois) pour espionner son fameux secret. Outre que la méthode n'est pas très sûre techniquement (il est probable que Skyper prend des précautions), elle n'est politiquement pas très avouable. Et puis comment être sûr que le virus d'État s'appliquerait à tous les systèmes, ne serait pas contré par un antivirus, et s'il réussissait, ne donnerait pas lieu à des abus (cela équivaut, à peu près, à laisser quelqu'un avoir un accès sans contrôle à la plupart des ordinateurs d'un pays (qui prendrait le risque ?).

Et personne ne peut sérieusement penser à interdire la cryptologie dans son ensemble (au risque de paralyser le système financier mondial et d'abolir le secret d'État) ou à interdire les réseaux P2P (pourquoi pas revenir au Telex et aux pneumatiques ?). Du reste les réseaux P2P peuvent s'isoler du reste du Net. Comment interdire tous les Intranet, par exemple ?

Alors ? L'idée italienne équivaut à obliger Skype à livrer son secret, c'est-à-dire lui demander de se suicider. La pression européenne y parviendra-t-elle ?

D'autres, notamment aux USA ont songé à imposer aux fabricants de logiciels d'installer un "backdoor", une porte de derrière réservée aux seules autorités mandatées et leur permettant, naturellement avec toutes les garanties nécessaires, d'avoir accès à tout. On se rappelle que sous les années Clinton, certains songeaient à mettre sur tout ordinateur des "chips" qui les rendraient en quelque sorte visitables à un policier muni du bon mandat.

La solution n'est pas très réaliste non plus : comment convaincre, surtout dans le monde du logiciel de source ouverte, tous les programmeurs de respecter cette obligation ? comment l'imposer à toute la planète et à toutes les législations ? comment l'imposer aux futurs logiciels ? comment empêcher les utilisateurs de se précipiter vers les systèmes sûrs ?

Alors ? En l'état actuel de la technique, et compte tenu que d'autre systèmes que Skype fleurissent et fleuriront, les experts ne voient pas vraiment de solution à la demande italienne. Et quand bien même Eurojust parviendrait à instaurer une coopération entre les autorités européennes et les réseaux de téléphonie VOIP, on voit mal comment imposer cette norme européenne à l'Iran ou aux îles Caïman.

Mais bien sûr, il y a des bruits inverses qui courent sur Internet : la police autrichienne serait capable d'espionner Skype. Selon un ingénieur de Harvard, Skype lui-même pourrait intercepter ses utilisateurs (donc en faire profiter des policiers ?). Un chercheur canadien se serait introduit sur un site Skype et y aurait trouvé près d'un million de messages contenant

des mots clés comme Tibet ou droits de l'homme ?

Bref, comme toujours les vulnérabilités réelles ou imaginaires de la technologie font fantasmer.

Reste pourtant un argument de fond : les organisations criminelles ont toujours su assurer le secret de leurs communications. Parfois par de la "faible technologie" : voir Provenzano le chef suprême de la Mafia réfugié des années durant à Corleone, au nez et à la barbe des milliers de carabiniers qui le cherchaient dans toute la Sicile, et communiquant uniquement par des "*pizzini*", des bouts de papier pelure, tapés sur une machine non électrique et confiés à un gamin de confiance qui les portait à un "soldato" de confiance, qui les transmettait à un homme de confiance... Mais si maintenant la Ndranghetta choisit la haute technologie, il doit y avoir de bonnes raisons

Surveillance

« *Faire que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son action ; que la perfection du pouvoir tende à rendre inutile l'actualité de son exercice.*"
M. Foucault

« Big Brother is watching you ». L'écran fait apparaître le dictateur autant qu'il fait comparaître le spectateur. De là à considérer que la télévision est un appareil totalitaire qui nous regarde pendant que nous le regardons ou qu'une caméra de surveillance dans un supermarché annonce la fin de l'autonomie du sujet, il y a un grand pas, que beaucoup franchissent. Les procédés de surveillance qu'imagine Orwell, comme ceux que décrit Foucault d'après Bentham sont des instruments de contrainte qui agissent autant qu'ils enregistrent. Dans un univers clos (la contre utopie de 1984, ou la prison), ils servent à prévenir la désobéissance. Surtout, ils imposent a chacun la conscience de sa visibilité, pour l'amener préventivement à se discipliner, à se corriger et finalement à consentir. Mais aujourd'hui ?
Dans nos sociétés «cool », le thème de la caméra omniprésente a d'autres connotations. L'idée d'une vie entièrement mise en scène pour être inutilement regardée, inspire aussi bien des films comme Truman show que l'émission intitulée ironiquement Big Brother . Disciplinaire, ou spectaculaire, le dispositif de vision nous obsède .

Aussi importe-t-il moins de savoir si on peut tout surveiller (oui, on peut !) ou si c'est mal (oui, c'est mal !) que de comprendre la logique du phénomène.

Trace

Les nouvelles technologies de l'information et de la communication enregistrent une multitude de traces : ondes, émissions, sans parler des dispositifs destinés à faciliter le repérage des mouvements d'un individu (tel le bracelet qui permet de suivre les prisonniers en permission ou à domicile). La plupart des transactions, ou connexions (achats, consultations, etc.) supposent des échanges de signes. Ces éléments intangibles, témoins de ce qui fut, peuvent être stockés, consultés. Chaque fois que nous utilisons des symboles (à commencer par l'argent) en conjonction avec un appareil numérique, nous engendrons des séries de 0 et de 1 quelque part dans une mémoire. Certains objets familiers témoignent pareillement de leur parcours, donc indirectement de notre histoire à nous, utilisateurs. Une carte de paiement dotée de puce a, selon l'expression de son inventeur, Roland Moreno une mémoire irréversible qui mime la mémoire humaine : ce qu'a « fait » la carte est enregistré, qu'il s'agisse d'une carte bancaire, d'une carte GSM, d'une carte médicale. Elle a comme une vie individuelle (et n'est pas un simple réceptacle d'unités de compte comme une bande magnétique).

Une nouvelle notion est apparue pour rendre compte de tous ces phénomènes : la trace .. Nous passons devant des caméras de surveillance, nos transactions par carte bancaire sont enregistrées avec lieu et heure, le responsable de réseau ou le fournisseur d'accès peut savoir seconde par seconde à qui nous nous sommes connectés. Tout transport, toute communication laisse une mémoire à un péage d'autoroute ou chez un opérateur de télécoms. Nous apparaissons dans des fichiers qui concernent ce que nous avons fait, où nous avons été

(physiquement ou par communications interposées), ils disent donc ce que nous sommes. Un simple téléphone mobile allumé permet de dire où nous sommes, même lorsque nous ne l'utilisons pas, et peut, dit-on, se transformer en micro enregistrant nos conversations non téléphoniques.

Si tout trajet fait trace, personne ne court plus vite que son passé. Mais il n'y a pas que les hommes qui soient traçables : les choses le sont aussi. Une simple étiquette de supermarché raconte l'origine d'un objet, voire l'histoire d'un bœuf qui n'a pas la maladie de la vache folle, etc. Deux facteurs expliquent cette prolifération.

La technologie multiplie les mémoires et les interconnecte . La demande de sécurité renforce cette tendance : éviter la cyberfraude, protéger la propriété, sécuriser les transactions, mais aussi lutter contre une des obsessions de notre monde globalisé, l'épidémie . Dans le monde des réseaux, O.G.M., gènes, virus, produits contaminés, etc. circulent, il faut donc que les marchandises aient aussi une histoire inscrite quelque part. Là encore, il s'agit de suivre des trajets.

Bien qu'elle puisse être un indice pour une éventuelle police de la pensée, la trace informatique concerne chacun d'entre nous, surtout en tant que consommateur individualisable soumis à des stratégies commerciales .

Profil

La trace implique le profil : du rapprochement des traces, dont certaines, séparément sont d'une grande banalité, résulte une image générale. Nous faisons tel type d'achats, nous nous connectons à tel type de site, nous avons été là, nous avons telle habitude alimentaire, pourquoi dissimulerions-nous tous ces petits détails ? Pourtant, rassemblés dans l'ordinateur d'une compagnie adepte du principe du « vous êtes uniques, nous vous offrirons un service unique » engendre des marchands de profils. Ces indices, traités par des logiciels spéciaux dits de datamining autorisent un marketing très fin. En France, la constitution de ces fichiers nominatifs est soumise à déclaration , mais ce n'est pas le cas partout t. Ainsi, la principale régie publicitaire sur Internet, Doubleclick a acquis en même temps que la société Abacus des bases de données concernant 90 % des foyers américains, ce qui a donné lieu à un procès retentissant.

L'actualité a été défrayée par diverses affaires de «mouchards» Pentium III (avec son numéro de série théoriquement lisible à distance), ou encore Windows 98 se sont révélés porteurs d'identifiants. Ceux-ci permettant de suivre les activités du possesseur en ligne, voire pour le second, de dresser une liste du contenu de son disque dur . Certains logiciels sont munis de « trappes » dès leur fabrication. Ils sont conçus « piégés » : les initiés connaissent le « passage secret » qui permet d'accéder aux cœur du système et de le commander.

C'est aussi une technique d'espionnage stricto sensu. L'Iran et quelques autres pays ont ainsi fait les frais de système de cryptologie truqués et il fut récemment question d'une affaire remontant aux années 80 : l'œil de Washington , le logiciel Promis de la société Inslaw, un système commercial de mise en relation de bases de données, qui aurait été détourné à des fins de surveillance. Ce logiciel aurait notamment permis aux services Israéliens de faire la chasse aux Palestiniens suspects. Au moment où nous écrivons ces lignes c'est le système «

Carnivore » d'interception des courriers électroniques par le FBI qui est sur la sellette : des associations le soupçonnent de collecter davantage d'informations que celles que prévoient les mandats judiciaires.

Le logiciel truqué n'est pas le monopole des services spéciaux. Un cousin des « cookies », les logiciels dits « E.T. » (allusion au film de Spielberg où la répugnante créature de l'espace doit « téléphoner maison ») font beaucoup de bruit aux États-Unis : des logiciels commerciaux téléchargés pourraient à l'insu de leur propriétaire vraiment « téléphoner maison », c'est-à-dire prendre le contrôle du modem pour lui faire envoyer les données recueillies à une adresse précise. Les promoteurs de telles initiatives se défendent de recueillir des informations nominales, mais seulement des données statistiques.

Le petit monde de la cryptologie retentit de bruits invérifiables sur des manipulations machiavéliques : même le fameux logiciel PGP (Pretty Good Privacy), symbole même de la résistance des internautes à toute forme de contrôle gouvernemental a été accusé de contenir des failles intentionnelles pour permettre à la NSA ou autre d'en manipuler les clefs. Il est juste de dire que, s'il existe des défauts dans ce logiciel, il n'existe aucune preuve avérée d'un tel complot .

Pour reprendre l'image du trajet, tout internaute peut alimenter un fichier donc un profil pratiquement à chaque stade de ses déplacements : de chez lui, lorsque son ordinateur conserve l'historique de ses connexions, et s'il accepte des cookies ou installe des logiciels dotés de moyens d'identification ou des « E.T. », chez son fournisseur d'accès qui connaît tous ses déplacements sur la Toile seconde par seconde, chez un serveur Internet qui peut enregistrer des questionnaires remplis par les visiteurs et les données fournies par les cookies, sur des réseaux qui échangent des informations sur les visiteurs des sites. Et ceci légalement.

« Je ne suis pas un numéro » hurlait, à chaque épisode, le héros du feuilleton-culte des années 60, le Prisonnier. « Je ne suis pas un profil, je veux être anonyme » devraient crier aujourd'hui ses successeurs.
A côté d'un volet répressif évident (lutter contre les pirates, les reproductions illégales, repérer les usages illicites du matériel dans l'entreprise), le marketing est un des principales motivations de la surveillance. De l'étude comportementale des consommateurs en général, on passe facilement à la proposition personnalisée : ainsi, Monsieur X dont la régie publicitaire a repéré qu'il s'intéresse à tel domaine reçoit des offres ciblées pour certains produits. Pourtant, recevoir un spam , ou une offre commerciale non sollicitée de type supérieur « Monsieur machin, à vous qui aimez le jardinage... » n'est pas le degré le plus grave de l'asservissement des libertés publiques .

Signature

"La vie privée sera à l'économie de l'information du siècle prochain ce que la protection du consommateur et l'attention portée à l'environnement ont été à la société industrielle du XX° siècle. " affirme Courrier International. Défendre son cocon y compris contre Bill Brother ou Big Gates risque en effet de devenir un thème militant.

Contrôler ses traces.

Tout ceci se traduit d'abord sur le terrain du droit. En France, la loi du 3 janvier 1979 sur la date de communication de documents issus des archives publiques, et la fameuse loi du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés ou encore les activités de la CNIL sont les traductions juridiques les plus connues de controverses incessantes pour le droit à l'anonymat. Il y a quelques années l'opinion avait été frappée par l'affaire des clipper chips, ces mouchards que l'administration U.S. voulait imposer sur chaque ordinateur afin de pouvoir retracer les activités délictueuses de leur propriétaire. Ou encore, on se souvient des luttes qui accompagnèrent la diffusion de Pretty Good Privacy (P.G.P.), le logiciel de cryptologie gratuit mis par Fred Zimmermann à la disposition de tous les citoyens, mais qui lui avait attiré des poursuites pour « exportation illégale d'armement » . Il suffit d'utiliser régulièrement son courrier électronique pour être submergé de pétitions appelant à résister à l'inquisition légale. La bataille juridique continue entre les partisans du contrôle (pour combattre les révisionnistes, les pédophiles et autres sur la Toile) et les tenants d'un droit d'expression sans limites.

L'anonymat devient un business comme les autres. L'invisibilité s'achète. Le thème de la nouvelle de Paul Morand, Monsieur Zéro, ne plus offrir de cible, ne plus être connu par aucune autorité, devient une utopie. Outre les panoplies de contre-espion que chacun peut se procurer ou des sites « anonymiseurs » permettent de naviguer sur Internet et d'y envoyer des messages sans que l'on puisse remonter à leurs auteurs. Des équivalents civils du leurre, existent également, à savoir, des faux papiers en tout genre. Soit en profitant des trous de législations nationales (les USA offrent quelques possibilités aux amateurs de seconde identité), soit en se domiciliant hors de portée des systèmes répressifs, soit avec la complicité de certains pays, des sociétés offrent ouvertement de faux passeports (dont ceux de pays disparus), ou des passeports diplomatiques d'États prêts à vendre un titre de consul ou de conseiller honoraire, des cartes de crédits imitées, des cartes de crédits renvoyant anonymement à des sociétés écrans, des comptes dans des paradis fiscaux comme le Delaware ou Belize. Ne parlons ni des sociétés offshore, ni des titres universitaires, ni des permis de conduire. Internet est le paradis de ce petit commerce.

Inversement, l'anti-anonymat, c'est-à-dire la possibilité d'apposer une « vraie » signature prend une importance croissante avec le commerce électronique, etc. La signature, le paraphe que l'on appose pour certifier un contrat, exprime une double affirmation : je m'identifie maintenant (je suis bien M. Untel) et je maintiendrai demain ma promesse (ma signature me sera opposable par vous à qui je la confie librement).

Quel signe unique et durable qui peut se transmettre à distance et donc protéger à la fois contre la falsification d'un voleur d'identité et contre le reniement du signataire ? Les solutions sont en nombre restreint. Soit le signataire possède une chose unique qui l'identifie, telle une carte, qui se montre ou émet un signal particulier à distance, soit le « signataire » démontre un savoir qui lui est propre suivant le principe du mot de passe. Dans ce dernier cas, la preuve est une « performance » : être capable de taper les bons chiffres ou de comprendre un message qui démontre que vous possédez une certaine clef.

La cryptologie, par des systèmes dits asymétriques, des façons ingénieuses de réaliser une performance qui démontre que l'on possède la clef d'un code et que l'on est qui l'on prétend, sans rien laisser transparaître de ce qu'est cette clef. Une autre voie de recherche porte sur un autre code, le code génétique et sa manifestation visible : notre corps. Il s'agira alors de

transmettre une mesure biométrique de l'iris de notre œil, de notre empreinte digitale ou de toute autre image corporelle. Il existe aussi un procédé de signature numérique à distance : un stylo enregistre le trajet exact de la main ; le signataire peut fournir non le résultat de son geste (une empreinte, un tracé d'encre toujours imitable sur un bout de papier), mais quelque chose qui tient à la fois de la performance conventionnelle et de l'identité biologique : son impulsion nerveuse.

Au-delà du problème d'une trace volontaire non falsifiable, se dessine un enjeu crucial. L'identification numérique n'est pas qu'une garantie contractuelle, c'est un permis d'accès. Dans un monde de réseaux et de connections, la question de « qui entre où » par électrons interposés, détermine la sécurité des mémoires informatiques. C'est ce que pressentait Gilles Deleuze lorsqu'il écrivait : " Les sociétés disciplinaires ont deux pôles : la signature qui indique l'individu, et le nombre ou numéro matricule qui indique sa position dans la masse.(...) Dans les sociétés de contrôle, au contraire, l'essentiel n'est plus une signature ou un nombre, mais un chiffre : le chiffre est un mot de passe, tandis que les sociétés disciplinaires sont réglées par des mots d'ordre. "

Traquer, traiter

Surveiller, et après ? La collecte d'information peut avoir diverses finalités (voir plus bas), encore faut-il qu'elle soit exploitable. Encore faut-il que la mauvaise information ne chasse pas la bonne, que le banal n'étouffe pas le significatif. Encore faut-il, tout bêtement, que le surveillant sache quoi faire de ce qu'il sait. L'éternel problème : l'information n'est pas la connaissance, se pose ici sous un aspect quantitatif, le plus brut, celui des gigaoctets.

C'est une difficulté que connaissent les espions. « L'espionnage consiste essentiellement à passer au crible des montagnes d'informations rassemblées au hasard, dans l'espoir de découvrir une pierre précieuse qui éclaire le tout, un maillon permettant de relier. » disait le chef de l'espionnage est-allemand, Markus Wolf . Savoir n'est rien, encore faut-il savoir ce que l'on sait et croire ce qui est vrai. Les renseignements vrais (comme l'annonce de l'opération Barbarossa par Victor Sorge) peuvent être soit noyés sous des informations fausses, soit refusés parce qu'elles dérangent les convictions de leur destinataire.

La crédibilité de l'information, problème psychologique voire moral, illustre le principe selon lequel « s'informer fatigue ». Mais, le repérage dans une masse de données est, sous bien des aspects un problème technique. Repérer sera un maître-mot, pas seulement pour les espions ou les spécialistes de l'intelligence au sens large. Ainsi, la question du « mot-clef » bien connue de tout archiviste ou de tout internaute qui désire attirer un maximum de visiteurs sur sa page personnelle : comment classer, quels déclencheurs choisir pour décider que tel document doit être corrélé à tel autre ? À l'occasion de l'affaire Echelon (voir encadré) on a cru entrevoir comment les « grandes oreilles » faisaient pour ne pas être submergées par des millions de communications . La NSA disposerait de logiciels « renifleurs », capables de repérer non seulement des mots significatifs isolés, mais de les relier, voire de comprendre leurs équivalents à mots couverts , paraphrases et substituts. Du coup, des associations entreprirent en 1999 d'affoler la machine en saturant la Toile de messages absurdes contenant des termes comme « plutonium », « Saddam Hussein », « tuer le président des États-Unis », etc. . Retour à la technique classique du leurre.

De plus, la technique de sélection et corrélation de mots représentera un enjeu de pouvoir pour ne pas » archiver à en mourir » suivant la belle expression de Michel Melot . Et peut-être verrons-nous demain (on y travaille déjà) des logiciels renifleurs d'images. Dotés de la capacité qu'a tout cerveau humain de reconnaître la même personne sous divers angles et avec diverses variations ; ils identifiaient comme nous reconnaissons le visage d'un ami de face ou de trois quart, s'il porte une casquette ou des lunettes, etc... Les mémoires numériques devront aussi apprendre des règles d'oubli. Une documentation numérique n'est pas physiquement accessible mais ne peut être retrouvé que par des identifiants (l'équivalent d'une adresse, d'un titre, d'un index). Une information non corrélée ou mal indexée est une information morte. Trop d'information tue. D'où l'importance du pouvoir de dire sur quels critères sera infligée la peine d'oubli numérique. Ceci vaut pour les informations, mais aussi pour les hommes dont le pouvoir social est proportionnel à leur «nombre de leurs connexions».

Mesures d'évasion

Truands et les terroristes savent que la police, la gendarmerie ou les services de renseignement (pour les terroristes au moins) cherchent à savoir ce qu'ils se disent. Ils ont donc développé de multiples stratégies de dissimulation. Le but est de s'assurer que leurs messages ne sont pas écoutés ou lus, ou qu'ils ne sont pas compréhensibles. Il s'agit aussi souvent de s'assurer qu'ils ne sont pas localisés rapidement.
Le facteur temps est ici fondamental : le narcotrafiquant Escobar a été pris parce que les services américains ont pu immédiatement situer par triangulation l'endroit d'où il employait un téléphone mobile (et pourtant, il en changeait à chaque communication). On peut penser que si la NSA avait la latitude et longitude exacte d'un téléphone satellite utilisé par ben Laden quelque part dans les zones tribales du Pakistan, l'Us Air Force y lancerait un missile en quelques minutes…
Pour prendre un exemple plus proche : si les policiers avaient pu situer en temps réel de quel cybercafé Fofana «le barbare» appelait les parents d'Ilan Halimi qu'il avait enlevé, ils seraient intervenus immédiatement.

Longtemps la seule façon de converser à distance et en secret était d'utiliser des cabines téléphoniques. Sinon, deux individus surveillés pouvaient s'écrire ou convenir d'un code (par petites annonces, par exemple), ce qui était long et incommode.

Désormais, les possibilités d'échapper aux interceptions (nous parlons bien ici du contenu des communications) ont augmenté à proportion de la complexité technologique.

Outre l'emploi de la VOIP que nous avons évoqué (et auquel la Ndranghetta se serait convertie) et l'utilisation de réseaux sécurisés, comme ce serait le cas pour les membres du gouvernement et de hauts fonctionaires, les solutions ne manquent pas :

Un langage conventionnel (dire pomme pour héroïne et poire pour cocaïne…), d'une langue étrangère rare ou d'un argot mal connu (système utilisé notamment par les gangs criminels carcéraux) : même si les enquêteurs se doutent de quoi l'on parle, comment prouver devant le tribunal que les gens qui ont échangé tant de grammes de nanan contre tant de tata sont des trafiquants de gramme ?

- La connexion depuis un lieu public tel un cybercafé sans laisser son identité. Certes, les patrons de ces établissements sont obligés de conserver les données un certain temps. Mais savoir trois jours après que l'ordinateur de troisième rangée a droite a envoyé un mail à telle heure à telle adresse ou a navigué sur tel site, n'aide pas à savoir le contenu des messages, ni surtout à identifier ou arrêter l'utilisateur. Sans compter qu'il existe des techniques dites « d'anonymisation » de ses connexions que l'on trouve fort bien expliquées dans les brochures de Reporters Sans Frontières (destinées, il est vrai, aux dissidents pas aux truands)

Recours à des logiciels de cryptologie dont certains sont disponibles sur Internet et excédent la longueur de clé autorisée en France (pour dire la chose de façon très simplifiée : plus la clé de cryptologie est longue, plus les bits d'information composant le message ont été comme battus, plus il est difficile de les décoder).

- Stéganographie : insérer un message dans les pixels d'une image (comme des micropoints invisibles au sein de documents plus vastes chers aux romans d'espionnage des années 60, mais ici de façon numérique). La stéganographie équivalent du camouflage pour les messages, permet également d'insérer des messages invisibles dans les espaces libres de fichiers informatiques où personne ne songe à aller les chercher.

- Utilisation de terminaux non repérés : téléphones mobiles volés, empruntés, ou achetés sans laisser son identité comme le prévoit la loi française (mobiles acquis à l'étranger ou auprès d'un vendeur peu regardant). Par ailleurs, on peut légitimement penser que des gens qui sont capables de se procurer de la drogue ou des armes automatiques sont en mesure de trouver des téléphones non repérés. Et s'ils avaient le moindre problème, il vient d'apparaître des téléphones improprement dit «jetables», chargés et dotés d'un numéros, tout prêts à être utilisés qu'il est possible d'acheter sans laisser son identité (en revanche, il faudrait laisser une trace au moment de recharger sa carte). Les téléspectateurs noteront que dans des feuiletons américains de type «Les experts», les enquêteurs disent parfois «Impossible de repérer le numéro, il téléphonait d'un jetable» : c'est une phrase que pourront désormais prononcer nos policiers.
- Stratégie de dissémination : utiliser plusieurs ou cartes SIM (qui sont les identifiants de l'abonné), éventuellement des numéros étrangers pour que les efforts des enquêteurs se dispersent devant tant de complication. N'oublions pas qu'il doit demander une autorisation par ligne.

Dépôt d'un message en tout «lieu» numérique convenu accessible par les réseaux , suivant le principe de la « boîte à lettre morte ». Ainsi, depuis un accès public, chacun peut ouvrir un compte gratuit et anonyme sur une messagerie, déposer un texte en brouillon, surtout ne pas l'expédier et communiquer son identifiant (login) et mot de passe à tout complice. Celui-ci, à son tour ira lire et répondre sur le brouillon. Ce dernier n'ayant jamais circulé échappe à tous les systèmes sophistiqués, fussent-ils ceux de la NSA. Même le vieux Minitel pourrait servir à cet usage.
Parfois par de la "faible technologie" : voir Provenzano le chef suprême de la Mafia réfugié des années durant à Corleone, au nez et à la barbe des milliers de carabiniers qui le cherchaient dans toute la Sicile, et communiquant uniquement par des "pizzini", des bouts de papier pelure, tapés sur une machine non électrique et confiés à un gamin de confiance qui les portait à un "soldato" de confiance, qui les transmettait à un homme de confiance...
· L'« anonymisation » des mails. Il existe également des services de navigation ou de courrier anonymes, des *proxys* d'anonymisation. Dans les deux cas, le processus consiste à interposer un ordinateur entre celui de l'usager et le reste du réseau : cela permet de réexpédier le message sans en révéler l'origine ou de naviguer sans laisser de trace.
· Des méthodes plus sophistiquées permettent de brouiller l'adresse IP de son ordinateur (ce chiffre qui identifie tout ordinateur, connecté et partant son propriétaire) en multipliant les adresses ou d'emprunter des ordinateurs distants pour leur faire effectuer des tâches ou encore de faire transiter son message par plusieurs serveurs intermédiaires en effaçant ses traces derrière soi (quitte à détruire la carte mère de l'ordinateur relais par où on a transité). L'usage de ces techniques est réservé à de véritables experts. De la même façon un bon pirate peut prendre possession du téléphone mobile ou du PDA d'autrui à distance pour lui faire envoyer des messages. Mais ce n'est ni simple ni commode.

L'information n'est pourtant pas si rare : des « techno-libertaires » ou les défenseurs de la vie privée sur Internet peuvent, avec les meilleures intentions du monde, fournir des armes aux criminels. Ainsi Philip Zimmermann s'était rendu célèbre il y a quelques années en livrant gratuitement au public le logiciel PGP (Pretty Good Privacy, un algorithme de cryptologie). PGP permettait aux internautes d'acquérir un « intimité passablement satisfaisante » en codant leurs courriels. Zimmermann a réédité son exploit dans le domaine de la VOIP. L'algorithme censé protéger les communications téléphoniques des interceptions illégitimes qu'il a inventé pourrait également les mettre à l'abri des interceptions légales. De la même

façon, des brochures de Reporters Sans Frontières destinées aux dissidents politiques dans les pays qui contrôlent Internet décrivent des méthodes qui permettent de surfer anonymement, d'envoyer des courriels sans être repéré, de tenir un blog sans être identifié.

Nous avons nous-même participé à un colloque sur les nouvelles technologies où un scientifique canadien a présenté un système d'anonymisation permettant en principe à des dissidents (chinois en l'occurrence : ceci se passait juste avant les jeux olympiques de Pékin) de se faire «parainner» par un correspondant étranger : en correspondant avec eux (et non avec un site «anonymiseur» vite repéré par la police, les internautes du pays surveillé disposaient d'une passerelle pour naviguer ou communiquer sans que leurs commutations soient traçables de leur pays d'origine. Ce système serait évidemment utilisables par des criminels aussi bien que par des dissidents.

La liste n'est pas exhaustive et ne tient pas compte de bruits non vérifiés sur des «brouilleurs de bornes» utilisés par des truands (ils appellent de A et c'est la borne de B qui s'affiche en cas de géolocalisation) ou de brouilleurs d'Informations Relatives aux Interceptions (X appelle Y et c'est l'IRI de Z qui s'affiche). Ni des dispositifs de téléphones hypersécurisé «inécoutables» avec des clefs de cryptologie très robustes, des téléphones ou télécopieurs de sécurité, boîtiers de sécuristion des communications, détecteurs de micros, brouilleurs de téléphones portables ou de GPS62.
Dans le domaine informatique, il existe une multitude de dispositifs censés protéger les entreprises ou les simples particuliers et qu'un truand ou un terroriste pourrait utiliser aussi bien contre l'inquisition policière logiciels de chiffrement, de localisation d'ordinateur, de contrôle des clefs USB, de scellement, anti- logiciels espions...

De façon plus générale tout ce qui touche à la cryptologie et aux méthodes pour échapper à la surveillance électronique inspire nombre de sites et forums et nourrit un imaginaire centré sur les « zones d'autonomie temporaire », les « *hackers* à chapeau blanc » (les « bons » pirates informatiques qui n'agissent que par amour du jeu et de la liberté), la mythologie cyberpunk… Des groupes formels ou non font volontiers circuler l'information, mènent une action qui se voudrait de résistance à Big Brother. Ce monde utopique et disparate partage la même obsession du secret, de l'évasion, de la création de réseaux parallèles. Dans l'immense majorité des cas, il n'a rien à voir avec la criminalité. Mais c'est un milieu en ébullition, toujours à la recherche d'une riposte technologique contre le Système : s'il existe une possibilité de communiquer secrètement et de faire la nique aux « grandes oreilles » de la NSA, et autres systèmes de contrôle, c'est là qu'il s'inventera et se répandra. Dans un registre moins politisé, une multitude de publications électroniques exposent l'état de l'art en matière de cryptologie, sécurité et surveillance. Tout cela peut constituer des sources d'information pour contrer la vigilance policière.
Dans ces conditions, les enquêteurs devraient désepérer : comment imaginer qu'un criminel même débutant ignore tout ce qui précède et ne s'assure pas de la confidentialité des ses communications ?
Une partie de la réponse pourrait tenir dans l'adage policier : «S'ils étaient si malins, nous n'en prendrions jamais».
Aucune de ces techniques d'évasion n'est totalement sûre : de bons enquêteurs peuvent peut-être se procurer les numéros utilisés (ne serait-ce que par leurs correspondants s'ils sont eux-mêmes sur écoute). Ou encore, cela s'est vu dans certaines affaires, ils peuvent décider de placer sur écoutes toutes les cabines sur un certain trajet que des truands seraient susceptibles

d’utiliser. Mais dans tous les cas, le résultat est le même : davantage de réquisitions, davantage d’écoute.
Autre facteur souvent évoqué par les praticiens : le temps. Vous pouvez vous retenir quelques jours, employer des procédures compliquées, vous méfier de tout..., mais un jour, au bout d’une semaine ou d’un mois, vous vous sentirez en confiance, vous oublierez la possibilité de la surveillance et vous utiliserez votre téléphone mobile habituel pour dire des choses compromettantes.