Introduction

« Derrière Winston, la voix du télécran continuait à débiter des renseignements sur la fonte et le dépassement des prévisions pour le neuvième plan triennal. Le télécran recevait et transmettait simultanément. Il captait tous les sons émis par Winston au dessus d'un chuchotement très bas. De plus, tant que Winston demeurait dans le champs de vision de la plaque de métal, il pouvait être vu aussi bien qu'entendu. Naturellement il n'y avait pas de moyens de savoir si, à un moment donné, on était surveillé. Combien de fois, et suivant quel plan, la Police de la Pensée se branchait elle sur une ligne individuelle quelconque, personne ne pouvait le savoir. On pouvait même imaginer qu'elle surveillait tout le monde, constamment. Mais de toute façon, elle pouvait mettre une prise sur votre ligne chaque fois qu'elle le désirait. On devait vivre, on vivait, car l'habitude devient instinct, en admettant que tout son émis était entendu et que, sauf dans l'obscurité, tout mouvement était perçu…Dans le passé, aucun gouvernement n'avait le pouvoir de maintenir ses citoyens sous une surveillance constante. L'invention de l'imprimerie, cependant, permit de diriger plus facilement l'opinion publique. Le film et la radio y aidèrent encore plus. Avec le développement de la télévision et le perfectionnement technique qui rendit possibles, **sur le même instrument, la réception et la transmission simultanée, ce fut la fin de la vie privée.** »

Georges Orwell, 1984

L'ambition de cet ouvrage est de faire naître chez le lecteur une certaine prise de conscience du versant bien souvent méconnu des nouvelles technologies et d'Internet. Les arguments et les exemples développés iront pratiquement tous dans la même direction, celle d'un risque à terme d'une surveillance généralisée et omniprésente. Ce parti pris nous a semblé des plus naturels en ce sens que les médias nous confortent à longueur de journée dans la pensée unique d'un Internet totalement libre. Ce qui était vrai à une certaine époque, deviendra, si nous n'y prenons garde, l'antithèse des ambitions des pionniers du réseau. Se voulant anticipatif, au risque de faire certaines erreurs de pronostic, ce livre voudrait « réveiller » à temps ceux d'entre vous qui croient encore en la valeur des « **libertés individuelles** » afin que vous puissez agir sereinement, mais aussi rapidement, en permettant, chacun à son échelle et suivant ses capacités, de poser des actes et d'éviter de faire de notre monde une prison où **l'esclavage numérique deviendrait la norme**. Internet est un magnifique outil. C'est peut être la seule fois où, au fil des pages, bien que convaincu, nous l'écrirons. Libre aux hommes, et donc à vous, de n'en tirer que le meilleur.

1 - Le 11 septembre : déclencheur fondamental du contrôle des citoyens

« L'image, la toute puissante image, avait définitivement triomphé du mot dans la communication de l'information, et elle ouvrait aux désinformateurs des perspectives nouvelles et apparemment illimitées »

Vladimir Volkoff, Petite histoire de la désinformation

C'est la stupeur. Personne n'y croit sur l'instant. Trop irréel, trop gigantesque. Et pourtant, sur tous les écrans de la planète, c'est la même histoire qui s'écrit : les deux tours jumelles du World Trade Center, symbole de la toute puissance américaine, s'écroulent devant tous les yeux terrifiés. Le bilan est lourd : on dénombre officiellement 2749 victimes. L'attentat est revendiqué Al-Quaïda. La guerre au terrorisme international est alors très vite lancée. Il n'y a pas d'autres réflexions à avoir, il faut éradiquer la « vermine ». Georges W Bush dans une rhétorique macabre déclarera « si vous n'êtes pas avec nous, vous êtes contre nous ». Un quasi-consensus mondial émerge et tous les moyens pour lutter contre le terrorisme seront bons, et les Etats-Unis, touchés en plein cœur, deviendront vite le leader dans cette course poursuite effrénée.

S'il était très difficile dans les premiers temps, au vu des événements, d'être contre le fait d'utiliser absolument tous les moyens nécessaires pour qu'une telle catastrophe ne se reproduise, on peut aujourd'hui, avec le recul, être plus critique quant aux politiques menées depuis ce jour dans nos démocraties occidentales.
L'Amérique imposera très vite, par mesure de protection, un contrôle drastique à ses frontières. L'administration Bush commencera à réclamer des informations (noms, numéros de carte de crédit, numéros de téléphone…) contenues dans les passenger name records (PNR), les fichiers de réservations des compagnies aériennes, et ce bien sur, officiellement, pour permettre d'identifier d'éventuels terroristes avant leur intrusion sur le continent américain.
Les attentats de Madrid et de Londres, n'ont fait que persuader l'opinion publique que la seule voie possible était désormais d'attendre sagement que les services de sécurité, au niveau local et international, mettent tout en œuvre pour combattre « tous ces ennemis extérieurs ». Et qu'on leur donne tous les moyens nécessaires, peu importe lesquels.

Retenons cependant ces chiffres : **le 11 septembre à causé moins de 3000 victimes**, et James T. Morris, directeur du Programme alimentaire mondial (PAM) à l'ONU annonçait en Janvier 2005 que **tous les jours, ce sont 18 000 enfants qui meurent de la faim, soit un enfant toutes les 5 secondes**[1] **!** Ceci « s'ajoute aux 850 millions de personnes qui, déjà, souffrent de la faim dans le monde. Au niveau global, la malnutrition est sans conteste le problème le plus meurtrier… En 2005, nous allons dépenser de 700 à 800 millions de dollars pour aider à nourrir les populations au Soudan ». Dans le même ordre d'idée de ce funeste et morbide décompte, Gérard Chaliand, directeur du centre d'étude des conflits, a évalué à

[1] www.liberation.fr 11/01/2005

moins de 10.000 le nombre de décès dus au terrorisme international depuis la fin des années 1960.
Ces chiffres sont peut être incomparables, les morts provenant d'une part d'idéologies fanatiques et les seconds d'un « gâteau » mondial bien mal réparti. Pourtant, le gigantesque arsenal déployé au niveau international contre ces intégristes, avec les budgets colossaux que l'ont connaît (rien que les Etats-Unis consacrerait chaque année au renseignement 30 à 50 milliards de Dollars[2] !), mais surtout avec la panoplie de mesures juridiques et sécuritaires, parait tout à fait disproportionné dans une lutte contre quelques groupuscules terroristes. Imaginons simplement les bienfaits et les vies sauvées que l'on envisager pour l'Afrique, si l'on employait les budgets pharaoniques des agences de renseignement à ce continent qui se meure loin de nos yeux d'occidentaux. Et pourtant apparemment nos gouvernements ont déjà fait ces choix.
Alain Weber, avocat et responsable de la commission Informatique et libertés de la Ligue des Droits de l'Homme (LDH), critique aussi la situation : « Quelle que soit l'émotion que suscitent les attentats, nous ne devons pas tomber dans le piège des terroristes et faire usage d'un législation aussi scélérate que les actes que l'on cherche à combattre »[3]. Peter Schaar, coordinateur des « CNIL[4] Européennes » est aussi très clair : « dans de nombreux pays européens, **la lutte contre le terrorisme sert d'excuse à la mise en place de mesures qui n'y sont pas directement liées**… Il est crucial que chaque mesure soit légitimée par des preuves évidentes[5]. »

Mais l'argument terroriste, bien que majeur et savamment orchestré par les grands médias pour établir une véritable psychose populaire n'est plus maintenant le seul à cette justification de mesures liberticides. La fraude, qui est la cause de pertes importante au niveau économique et de tensions au niveau social (immigration non désirée…) est en passe de renforcer l'argumentaire. Selon un appel commun de plusieurs syndicats et associations Françaises[6] en mai 2005, « le caractère à bien des égards incantatoire, voire purement fallacieux, des arguments avancés pour justifier le recours à ces nouvelles technologies, vient conforter l'impression qui se dégage du caractère purement formel du débat initié. » Plus précisément, en parlant du phénomène des fraudes, « le ministère de l'intérieur, de son propre aveu, ne paraît pas en état d'en évaluer précisément l'ampleur, qui reste à établir par des études objectives. Sans avoir démontré la réalité du problème, il propose de recourir à une solution coûteuse à la fois financièrement et en terme de libertés publiques. »

La thèse de ce livre est donc la suivante : les attentats (relayés ensuite par des arguments de lutte contre toute forme de fraude, d'insécurité, d'agressions…), combien affreux ont-ils été, avec leur lot de souffrances tant pour ceux qui sont partis que pour ceux qui restent, pourraient être le prétexte idéal aux puissants de ce monde pour justifier le recours à des politiques ultra sécuritaires pour contrôler l'ensemble de la population. Invraisemblable ? A vous de juger.

[2] Tous fichés (Jacques Henno)
[3] L'express 5/09/2005
[4] Commission Nationale Informatiques et Libertés
[5] www.zdnet.fr 13/03/2006
[6] La ligue des droits de l'Homme, le Syndicat de la Magistrature, le Syndicat des Avocats de France, l'association Imaginons un Réseau Internet Solidaire, l'intercollectif Droits et Libertés face à l'informatisation de la société et l'Association française des juristes démocrates.

1.1 Internet ou le canular du « toujours plus de liberté » ?

« La vraie trahison, c'est de suivre le monde comme il va et d'employer l'esprit à la justifier »

Jean Gehenno

Précision nécessaire, au cours de cet ouvrage, c'est de l'Internet au sens large dont il est question, c'est-à-dire de tous les échanges qui passent par les « tuyaux » du réseau des réseaux (web, irc, téléphonie (VoiP), télévision via Adsl…). D'autres, comme nous y reviendrons plus tard, appelle cela « la convergence ».

L'Internet, prenons le cas Français qui sera plus parlant, a, dès ses prémices, mis l'accent dans sa communication sur toujours plus de liberté et de **transparence** pour l'utilisateur. Les FAI (fournisseurs d'accès à Internet) ne s'y sont pas trompés. Toute leur politique marketing est axée là-dessus. « Free » est l'exemple typique de cette tendance à laisser penser qu'Internet est par-dessus tout le royaume de la liberté. L'opérateur Alice y va aussi de sa formule : « Avec Alice, tout est clair ».

Un véritable esthétisme des TIC (Technologies de l'Information et de la Communication), à grands renforts de slogans, d'affichages et de pubs télévisées est en tout cas en train de naître sous nos yeux, transformant l'homme en un véritable Dieu, capable de défier l'espace et le temps et toutes les limitations humaines dans son nouvel environnement technologique. Et qui voudrait s'y opposer ? Qui ne trouverait pas extraordinaire d'avoir accès en toute liberté à la connaissance, aux échanges et à la communication ?
Et pourtant…

1-1-1 Une infrastructure de traces

« Un homme avertit en vaut deux »

Sagesse populaire

Sans rentrer dans un débat technique qui n'est pas notre propos ici, un éclaircissement succinct de la manière dont fonctionne le réseau semble nécessaire.
En effet sur Internet, chaque machine (ordinateurs, serveurs, et de plus en plus d'appareils communicants) est identifié par un numéro appelé adresse IP (Internet Protocole) du type 192.32.23.45 par exemple. Chaque fois qu'un internaute se connecte à un site web, ce dernier récupère dans ses « logs » (sorte de journal récapitulatif des connexions qui prend la forme d'un petit fichier « texte ») l'adresse IP de l'ordinateur de l'internaute en question, l'heure à laquelle il s'est connecté et déconnecté du site (et donc la durée de connexion au site), et tout un tas d'autres informations plus ou moins négligeables (version du navigateur Internet, résolution…). Il faut voir que ce dont il est question ici dans **les « logs » est l'information « minimale » que récupère tout site web sur les internautes**. Or il peut faire beaucoup plus. Ce qui s'appelle sympathiquement les « **cookies** » (on

retrouve ici bien le paradoxe du monde Internet où *en apparence*, tout est *sympathique*), permet par exemple à un site web (marchand le plus souvent) de « tracer » les habitudes de l'internaute et d'en savoir plus sur son comportement en ligne lorsqu'il visite le site en question. Logs et cookies ont pratiquement toujours existé sur le web et sont le signe que **tout internaute quel qu'il soit laisse des traces de son passage sur la toile**[7]. **C'est dans la structure même d'Internet de reconnaître un ordinateur par un identifiant (adresse IP)** pour qu'il soit accepté par le réseau.

Les « **Cookies** » sont de petits fichiers au format texte qui sont enregistrés à la visite d'un site web (le plus souvent marchand) sur le disque dur de l'ordinateur de l'internaute. Ils sont utilisés très fréquemment par les gens du marketing pour avoir un maximum de renseignements sur les comportements du consommateur potentiel. Avec des cookies bien paramétrés on peut connaître les sites les plus visités, les habitudes de navigation…etc., et ce totalement légalement et sans avoir à passer par les fournisseurs d'accès. Néanmoins les cookies restent assez inoffensifs comparé à la puissance aujourd'hui des spywares et autres adwares (nous les aborderons plus tard) beaucoup plus intrusifs.

Or jusqu'à maintenant pour reconnaître, par exemple, un ordinateur d'un particulier, son fournisseur d'accès (type Wanadoo) lui **allouait pour le temps de sa connexion** une adresse (adresse IP) pour que cet ordinateur puisse communiquer, c'est-à-dire émettre et recevoir des informations avec le reste de la toile Internet. On parlait alors à ce moment là d'**adressage « dynamique ».** En effet **le protocole IP dans sa version 4**, ne disposant pas d'un nombre suffisant d'adresses pour attribuer à chaque machine de la planète un numéro spécifique, recourait à ce stratagème pour contenter les Internautes. Ainsi à chaque connexion, l'utilisateur disposait techniquement d'une adresse IP à chaque fois différente pour surfer sur la toile, ce qui lui garantissait au passage un certain anonymat.

[7] Voir concrètement quel type de traces vous laissez sur le site : www.anonymat.org/vostraces/index.php

Or, la version 6 du protocole IP (IPv6) est en passe de remplacer la version 4, créée il y a plus de 20 ans. Cette version est ressentie aujourd'hui comme inadaptée aux contraintes de l'Internet et à l'explosion du nombre d'adresses IP, notamment en raison de son mode d'adressage qui prévoit une allocation d'espace de 32 bits alors que le protocole IPv6 permettra un adressage de 128 bits. En clair, le protocole IP dans sa version 4 limitait le nombre d'adresse IP à environ 4 milliards pour l'ensemble de la planète. Avec IPv6, ce nombre sera exponentiellement accru, puisque avec un mode d'adressage à 128 bits, **IPv6 disposera de 2 puissance 128 (plusieurs milliards de milliards) d'adresses IP**. Ainsi, en raison de la multiplication des appareils qui arrivent sur le marché et qui requièrent une connexion, les astuces de type adresses IP dynamiques (version 4) ne suffiront bientôt plus. Dans le monde, c'est à peu près 63 nouveaux utilisateurs par minute que l'on connecte à Internet. « Le passage à IPv6 permettra notamment d'augmenter le nombre de machines connectées au réseau », précise t-on à l'AFNIC[8]. IPv6 va permettre à beaucoup plus d'appareils de toutes sortes - notamment mobiles - de se connecter à Internet et d'échanger plus de données. Avec l'avènement de l'IPv6, annonçait-on aux « Rencontres d'Autrans 2006[9] », **le nombre d'appareils pouvant potentiellement être mis en réseau devient presque infini**, à tel point que certains se sont laissés aller à évoquer la "disparition de l'Internet" tel qu'on le connaît.

Nous sommes actuellement dans la période de transition, largement sous médiatisée et pourtant ô combien importante pour l'Internet de demain, faisant cohabiter les deux versions (IPv4 et IPv6) en parallèle et permettant une montée en charge des connexions et des débits.

Cette palette ouvre certes de nouveaux horizons en termes de modèles métier : fort de ces nouveautés, l'ensemble des terminaux existants (électroménager, portable, PC, appareil photo etc.) pourraient se voir allouer des adresses IP fixes, auto configurables lors de leur mise en ligne permettant d'exécuter à distance des services "temps réel" et sur mesure (comme des traitements autour de la traçabilité des appareils par exemple). Par ailleurs, d'autres types d'équipements se voient attribuer des adresses IP, comme les consoles Sony PS2 qui sont dotées d'un équivalent de Windows avec d'ores et déjà la possibilité d'activer IPv6 et de pouvoir gérer l'interconnexion des jeux. Dès le départ, la PS2 a été conçue pour supporter IPv6.

En fait, comme le souligne un consultant présent aux rencontres d'Autrans 2006 **«l'internet sera tellement dilué dans notre quotidien que nous ne le verrons plus »**, le réseau devenant omniprésent dans la vie quotidienne, de la maison à l'entreprise, en passant par l'école, le médecin, les transports en commun ou les magasins. Des exemples sont déjà apparus dans ce sens avec la dissimulation des antennes relais de téléphones portables dans des arbres factices, créés pour l'occasion. Même programme avec les lampadaires (il en existe plus de 55.000 à Paris) qui vont héberger, sans que l'on puisse les voir, des bornes WiMax qui à terme permettront des communications haut débit avec tous les appareils nomades. Le concept pourra aussi s'avérer très performant dans les zones rurales. "Sous un seul lampadaire/WiMax, on peut faire surfer 300 personnes en même temps", calcule Jean-Paul Rivière, président d'Altitude Telecom et pionnier du Wimax. Et tout cela au

[8] Association Française pour le Nommage Internet en Coopération
[9] Colloque de réflexion sur le futur de l'Internet se réunissant chaque année dans l'Isère, http://wiki.autrans.net/

nom de la lutte contre la pollution visuelle. Du coup, Internet devient invisible.

Mais ne nous y trompons pas : **l'infrastructure de traces du réseau est bien plus présente que jamais**. Certains spécialistes, toujours à Autrans reconnaissent que la plus grande « réussite » de l'Internet, c'est qu'il va disparaître dans le temps. « Quand une technologie est mature, elle devient transparente. Par ces mots, il ne faut pas comprendre la disparition d'Internet dans le sens de sa destruction, mais comme **un élément omniprésent qui va se fondre dans le décor et qui sera au centre de notre vie**. »

Précisons à ce moment-là de l'exposé qu'Internet **recèle donc la possibilité**, dans son infrastructure-même et depuis sa conception, de tracer n'importe qui ou n'importe quoi, et ceci d'une manière d'autant plus paradoxale que cette traçabilité est quasi invisible aux yeux de l'utilisateur. Et ceci de plus en plus étroitement avec la montée en puissance du protocole IPv6 qui pourra suivre de près tout « l'appareillage nomade » de l'homme moderne.

Possibilité qui ne deviendra un jour paranoïa que si tout le monde (Etat, administration, services de renseignement, secteur privé et particuliers) décident de se mêler de la vie privée de tout le monde, comme peut le faire penser par exemple la tendance qu'annonce déjà les émissions de télé-réalité. Nous n'en sommes heureusement pas là. Le choix est encore devant nous. Nous ne sommes pas obligés de passer par ce « tout » sécuritaire pour évoluer.

1-1-2 La convergence, absente de tout débat citoyen :

« The Show must go on »
Queen

Ce qui vient d'être exposé dans le chapitre précédent est un sujet sur lequel les citoyens que nous sommes n'ont jamais eu à s'exprimer car on nous l'a toujours présenté comme un débat uniquement technique, une discussion d'ingénieurs en quelque sorte. Or c'est bien tout le contraire, puisque nos libertés fondamentales y sont ici en jeu. L'engouement pour Internet ne doit pas faire oublier que, préalablement, il est nécessaire de le penser, de réfléchir à une éthique, afin qu'il ne devienne pas un outil de contrôle de l'individu. Pourtant on se retrouve dans un débat de techniciens qui ont simplement peur d'une pénurie d'adresses. Selon eux, la solution vient, on l'a vu, avec IPv6 en attribuant à chaque citoyen de la planète une ou même plusieurs adresse IP distinctes. Or c'est bien de la que pourrait venir le danger. On se retrouverait alors dans un scénario Orwellien ou chaque citoyen, grâce à un identifiant unique (aujourd'hui avec l'IP, demain par la biométrie) serait fiché, tenu en laisse par sa vie privée. Dans le même ordre d'idée, au rythme où vont les volontés d'économies de nos gouvernements, les informations personnelles concernant chaque individu, jusqu'alors disséminées dans de multiples bases de données (Sécurité Sociale, Trésor Public…), pourraient, par exemple, se retrouver un jour centralisées.

En effet, et Jean Marie Messier en avait bien parlé à l'époque lorsqu'il était sous le feu des projecteurs avec Vivendi : on assiste aujourd'hui à **une « convergence »**

des réseaux. **Toutes les communications sont en passe de circuler via le réseau Internet** et l'IP: les conversations (VoiP, Voix sur Wi-Fi…), le web, les images, la musique, la télévision… Cela est bien sur très excitant. Pour une somme très modique, chacun peut avoir accès aujourd'hui à la communication avec un grand C (communication téléphonique illimitée, Internet haut débit, bouquet satellite…). Simple supposition, ce pourrait être via ces différentes « box » (livebox chez France Telecom, Freebox chez Free, etc.), dont on ne connaît pas exactement le contenu, qu'un début de surveillance pourrait être susceptible d'éclore[10]. Ne préfigureraient elles pas au premier avatar technologique de ce qu'on pourrait appeler (il faudra trouver un nom à cela) une « centrale de renseignement » personnel, ou une « police de la pensée » chère à Orwell. En effet, qu'est ce qui empêcherait dès lors un gouvernement (totalitaire ou très curieux ?) de tout connaître de ces citoyens, et ce jusqu'au fin fond de leur vie privée.
Effectivement, contrairement à la télévision qui est une technologie que l'on nomme « push » (l'information est comme « poussée » vers vous), **Internet et son protocole IP, en sens inverse permet que vous deveniez « émetteur » d'information** : c'est vous aussi qui envoyez de l'information au réseau. Vous n'êtes plus uniquement récepteur. Tout le danger est bien là. Si l'on ne s'en tient qu'aux différentes « box », elles renseigneraient par exemple sur les goûts de tel individu en observant ses programmes TV préférés, ses sites Internet favoris, ses conversations gratuites au téléphone… Mais tout cela n'est en fait qu'un début : des sociétés comme Cisco (nous le verrons en détail dans le chapitre sur « La maison de demain ») ont prévu qu'à très court terme, la « domotique » allait rentrer dans chaque foyer, composé de multiples appareils « intelligents » et tous reliés aux réseaux Internet. Pour prendre un exemple, le frigo, relié au réseau local de la maison (lui même relié au réseau Internet) pourra avertir ses habitants qu'il faudrait acheter du jus d'orange et une molette de beurre, et qu'avec leur accord, il peut les commander et les faire livrer au domicile en moins de 4 heures grâce à un site Internet de commerce électronique. Ce qu'on prenait encore comme de lointaines anticipations il y a une dizaine d'années est à nos portes aujourd'hui.
Le délire est déjà bien amorcé quand on lit l'exemple suivant : la FCC (Federal Communications Commission) aux Etats-Unis à décidé en octobre 2005 que le FBI[11] pouvait écouter les communications VoIP (c'est ce qu'on appelle la téléphonie illimitée en France, qui en fait passe par le réseau Internet, d'où sa gratuité). Ce choix implique que les utilisateurs ne pourront plus utiliser que les programmes susceptibles d'être mis sur écoute. Les programmes de cryptage, s'ils sont utilisés, doivent donc offrir une « porte de derrière » (qu'on appelle plus communément « **backdoor** ») permettant d'écouter la conversation.
Au Canada, dans la foulée des arrestations de présumés terroristes à Toronto en 2006, les Conservateurs de Stephen Harper s'apprêtent à relancer un ancien projet de loi de l'ex-gouvernement Martin, selon lequel les compagnies de télécommunications devraient être équipées de manière à faciliter l'interception de contenu téléphonique et virtuel[12].

On risque ainsi de voir disparaître la vie privée. Et alors direz-vous ? Qu'est ce qui

[10] Un rapport du Département de recherche sur les menaces criminelles contemporaines (DRMCC) de 2006 recommande au Ministère de la Justice de « s'assurer avec les opérateurs de communication que leur système permet la mise en place et le renvoi effectif des interceptions. Pour cela, il explique que le point crucial pour intercepter des communications sur Internet est **l'équipement par lequel le FAI connecte l'abonné à la Toile** et donc par lequel passent les paquets IP. » (Source : www.01net.com du 06/10/2006)
[11] www.vunet.be 04/10/2005
[12] www.branchez-vous.com 10/06/2006

pourrait bien m'arriver si quelqu'un apprenait la marque de mes Corn Flakes préférés ? Et bien en connaissant la vie privée de quelqu'un, on peut découvrir par la même occasion ses peurs les plus profondes, et un régime d'apparence démocratique, mais en réalité dictatorial pourrait tout à fait utiliser cette faille pour mettre les êtres humains en esclavage. Oui, rendre les gens esclaves de leurs propres peurs, ce serait un scénario tout à fait plausible. C'est bien là la dualité de « Big Brother », ce Grand Frère qui d'un côté, sous mine d'état providence faisant figure de protecteur, nous tient en fait en laisse car il connaît tout de nous. En fait, la rétention d'information sur la vie privée pose et posera toujours le problème de leur utilisation. Tant que les personnes ayant accès à ces informations sont désintéressées, il n'y a pas de problèmes. Mais qui peut assurer que ce soit toujours le cas. Qui n'a rien à cacher ? Personne. On est toujours susceptible d'être le « mauvais » pour quelqu'un : « trop intelligent », « trop riche », « trop coloré »… Il y aura toujours quelqu echose qui ne plaira pas à quelqu'un. C'est ce qui fait tout l'intérêt de la défense pour les libertés individuelles.

La **backdoor** ou porte de derrière est utilisée à la fois par les pirates informatiques et les grandes agences de renseignement pour pénétrer dans les ordinateurs. Présente le plus souvent par l'intermédiaire de quelques lignes de codes dans des programmes informatiques, la « backdoor » va autoriser ainsi un accès clandestin à toutes les données de l'ordinateur. Il est ainsi probable que les grandes agences de renseignement, au nom du « patriotisme économique » font par exemple installer sur des logiciels communément utilisés par le grand public (nous ne citerons personne…) ou par les professionnel (notamment des logiciels de bases de données) de telles portes qui leur permettront plus tard un accès aussi discret qu'infaillible aux informations qu'elles souhaitent acquérir.
Le grand public a pu faire sa connaissance lors de la sortie du film « Wargames » (de John Badham, 1983). Le concepteur du programme de sécurité thermonucléaire aux états unis avait en effet créé une backdoor sur son système. Il n'en fallut pas plus à un jeune lycéen pour y pénétrer par hasard et déclencher un conflit E.U./URSS sur les écrans des services de défense américains…

1-1-3 L'économie et le marketing, chevaux de troie du contrôle total

« Il n'est pas de vrai liberté d'expression sans liberté de s'exprimer sous couvert d'anonymat »

No logs Network

Les firmes privés, agissant dans l'Internet et l'informatique, mais aussi bien au-delà, ont commencé à comprendre (certaines depuis des années), plus ou moins influencés par les services de sécurité étatique, tout l'intérêt d'«en savoir beaucoup plus » sur le consommateur.
Presque tout à commencé avec la révolution du data-mining (dont nous reparlerons un peu plus tard), largement soutenue par les grandes surfaces dans les années 90. En effet à l'époque les grandes enseignes avaient entre leurs mains de véritables masses d'informations sur leur clients dont elles ne savaient jusqu'alors pas tirer

partie. Grâce au data-mining et à la mise en relation de la carte de fidélité des clients avec tous leurs achats, les grandes surfaces ont pu tirer des enseignements nouveaux. Ainsi, elles se sont rendues compte par exemple que les jeunes femmes faisant leurs courses le samedi matin, achetant un pack de lait et habitant tel quartier (c'est une des multiples informations personnelles que détiennent les cartes de fidélité) allaient à plus de 90% se fournir aussi en produits surgelés ! Le data-mining fait effectivement resurgir de l'analyse des « entrepôts de données » des **corrélations qu'il aurait été impossible de voir « à l'œil nu ».** L'importance de l'ordinateur, qui prête main forte à l'homme dans tout ce processus d'investigation, est fondamental car sans lui rien n'aurait pu être mis en relief. Le recours systématique aux machines et à cette « intelligence artificielle » peut aussi être vu comme tout à fait inquiétant dans les « nouveaux liens » qu'il permet d'établir. Par exemple, le dernier-né de la société Unica spécialisé dans les logiciels d'aide au marketing, dénommé Affinium Detect, permet à ses utilisateurs (pour l'instant essentiellement des banques, la grande distribution et les opérateurs télécoms) de détecter tout changement dans les habitudes de ses clients. Pour les banques, cela pourra être un dépôt sur un compte, plus important que celui fait l'année précédente. Le moteur détecte aussi l'absence d'événement, comme la non-utilisation de fonction GPRS sur un téléphone dernier cri, le tout sur plusieurs dizaines de milliers de transactions[13]. Difficile donc dans le monde numérique qui s'annonce de paraître autre chose qu'un mouton de panurge : tout comportement déviant est aujourd'hui analysé. Et demain, qui sait, suspecté ?

En savoir toujours plus (sur le consommateur), c'est l'évolution même de la science du marketing, qui ne serait pas dangereuse, si elle ne devenait pas systématique comme elle commence à l'être aujourd'hui en utilisant la puissance des méga bases de données, allié à la « connectivité », qu'offrent, en somme, les nouvelles technologies.
En Octobre 2005, un développeur Américain, Greg Hoglund condamne dans son blog l'éditeur de logiciels Blizzard, d'avoir, non seulement intégré à la nouvelle version de Warcraft (un jeu très populaire sur PC et consoles) un petit programme capable de savoir si un joueur triche ou pirate le jeu, mais également présentant toutes les caractéristiques d'un **spyware** (logiciel espion) avec beaucoup plus d'incidence sur la vie privée. Selon l'EFF (l'electronic Frontier Fondation, association américaine très focalisée sur tous les problèmes de vie privée numérique, dont nous aurons l'occasion de reparler à plusieurs reprises) « Blizzard appelle [ce programme] un système « anti-tricherie ». Nous appellons cela une invasion massive dans la vie privée… Si Hoglund est dans le vrai, Blizzard a une conception très vague de la vie privée : nous pouvons regarder vos informations personnelles, mais si nous ne les collectons pas, il n'y a pas d'intrusion ? Cela ne fonctionne pas ainsi ! »[14]
Mais les conditions d'utilisation, rappelées par les éditeurs lors de l'installation d'un programme ne sont-elles pas là pour informer les utilisateurs ? L'EFF reconnaît que les internautes devraient lire les contrats qui se présentent à eux, mais elle blâme aussi les sociétés qui rendent ce type de littérature (volontairement) très obscure, compliquée et longue à lire. « Sans contrainte sur ce qu'une société peut cacher dans ces énormes volumes juridiques, **de plus en plus de compagnies vont comprendre qu'elles peuvent envahir notre vie privée électronique pour n'importe quelle raison** » dénonce l'EFF. « Une telle pratique, au final, entraînera

[13] www.01net.com 28/07/2006
[14] www.zdnet.fr 21/10/2005

non **seulement l'accès à nos données personnelles**, mais aussi à **la prise de contrôle de nos ordinateurs ».** La CNIL avait d'ailleurs en avril 2005 largement ouvert la brèche en France en autorisant un syndicat professionnel, le Sell (Syndicat des éditeurs de logiciels de loisirs) à traquer les pirates de jeux vidéo sur Internet.[15]
Ainsi, et de plus en plus, les entreprises, sous couvert juridique, adoptent pour des raisons de soi-disant lutte contre le piratage, des pratiques qui s'immiscent dans la vie personnelle des citoyens. Mais l'exemple précédent sur les logiciels ne doit pas faire croire que seules les sociétés informatiques se lancent dans cette nouvelle quête du Graal. Il faut voir qu'avec la virtualisation progressive de la vie en général, toutes les entreprises pourront aussi bientôt s'y amuser.

La traduction la plus fréquente pour « **spyware** » et « **adware** » est « mouchard ». Parfois en effet les éditeurs de logiciels freeware (diffusés gratuitement) ou shareware, pour rémunérer leur développement, signent des accords avec des régies publicitaires et autres agences de marketing. En contrepartie, ils doivent installer de petits utilitaires en plus du logiciel souhaité. Le problème est que l'utilisateur ne maîtrise absolument pas leur action : ils sont soupçonnés de collecter et de transmettre des données personnelles, provenant de l'analyse de la navigation de l'internaute, des formulaires remplis lors de l'installation…etc. Certains mouchards établissent eux-mêmes la connexion Internet pour transmettre leurs informations ou récupérer les publicités à afficher. Enfin, ils se révèlent très difficiles à désinstaller.
Selon Webroot, les machines du grand public seraient infectées par 25,4 spywares. 80% des ordinateurs dans le monde seraient infectés[16].

Début novembre 2005, plusieurs plaintes, dont une de l'état du Texas, ont été déposées contre la maison de disque Sony BMG, accusée d'utiliser avec ses CD, des dispositifs de protection contre les copies multiples, qui portent atteinte à la vie privée. Toujours selon l'EFF, Sony BMG doit reconnaître qu'un logiciel présent sur chaque CD, appelé MediaMax pose ce problème du respect de la vie privée car il transmet des informations sur les habitudes des usagers via une connexion Internet, dès lors que le CD est lu sur un ordinateur connecté. L'EFF rajoute que « les fans de musique ne devraient pas avoir à installer sur leur ordinateur des logiciels potentiellement dangereux et s'immisçant dans leur vie privée, simplement parce qu'il veulent écouter de la musique achetée légitimement ». Apparemment les programmes espions concernaient 4,7 millions de disques, dont déjà 2,1 avaient été vendus[17].
Le phénomène des blogs n'échappe pas à cette tendance de vouloir en savoir toujours plus. En France, de grandes radios comme Europe2 ou Skyrock incitent leurs auditeurs à se créer des blogs via leurs sites Internet. Rappelons que le blog est une sorte de journal personnel ou l'internaute expose ses passions, ces centres d'intérêts et dévoile ainsi tout ou partie de son intimité sur le réseau. Etonnant de la part de ces firmes de mettre en place un service gratuit qui à priori ne rapporterait rien ? Dans la réalité, ces blogs commencent à être analysés par des outils statistiques de data mining et link analysis (voir plus loin) et permettent de connaître extrêmement bien le public qui les rédige. C'est en fait une mine d'or d'informations

[15] www.01net.com , 21/04/2005
[16] www.atelier.fr 25/08/2005

dont les radios commencent à percevoir toutes les possibilités et surtout comment en tirer profits avec leurs annonceurs.

Mais la science du marketing, littéralement « l'action de mettre des produits sur le marché », évolue elle-même dans ses concepts les plus fondamentaux grâce au TIC. Ainsi on entend parler de plus en plus de l'émergence du « géomarketing ». L'idée est simple : proposer aux entreprises d'étudier leur zone de chalandise grâce à un outil cartographique regroupant données sociodémographiques, géographiques et commerciales. Ainsi, en se déplaçant sur une carte de France virtuelle (comme avec Google Earth), beaucoup plus parlante que des tableaux de données, les « marketeurs » pourront effectuer des analyses de zones d'activité, de potentiel de consommation et de comportement, à l'échelle d'un département, d'une ville et même d'un quartier. L'entreprise peut ainsi connaître la typologie des catégories socioprofessionnelles présentes, leur niveau de revenus, la taille totale du marché, et les comportements des habitants. Il est, alors que cette technologie n'est que balbutiante, par exemple possible « de préciser les trajets professionnels les plus fréquents dans une région, les fréquences de passage à la banque ou les habitudes culturelles », détaille Jérome Guilmont, directeur de projet chez Asterop. Et de rajouter : « Et cela sur l'ensemble du territoire, lequel a été divisé pour l'occasion en 657 catégories consuméristes dites « zones de vie ».
On voit bien dans cet exemple les dérives sémantiques possibles : alors qu'il ne s'agit au départ que d'un projet purement « économique » pour aider les entreprises à mieux connaître leur marché et vendre plus efficacement, on pressent qu'il ne faudrait pas grand-chose pour qu'une cartographie aussi évoluée, et en liaison avec d'autres bases de données sur nos vies personnelles, dérive en un véritable outil totalitaire. Autant il est difficile de croire qu'une surveillance puisse être établie sur la seule analyse des adresses IP brutes (c'est-à-dire une suite de nombres sans liaison avec un individu donné) qui demanderaient un travail de Romains aux analystes plongés dans une infinité de lignes de chiffres, autant on peut penser que des outils beaucoup plus visuels, comme celui décrit ici, pourrait réellement représenter un big brother en puissance.
Dans le même ordre d'idée, des solutions de géolocalisation des internautes arrivent sur le marché. Plus lié à la notion de « déplacement » que le géomarketing (mais avec les avancées technologiques peut être que ces disciplines en viendront-elles à fusionner ?), il s'identifie littéralement comme un procédé qui permet de déterminer la position d'un internaute à partir de son adresse internet IP. D'après Marie Alexander, PDG de Quova, société leader dans ce domaine qui développe depuis six ans la plus grande base de données de géolocalisation au monde (les concurrents s'appellent MaxMind ou DigitalEnvoy), « à partir de l'adresse IP, nous pouvons déterminer avec un taux de fiabilité de 99,9% le pays d'origine de l'internaute, mais aussi sa ville, avec un taux qui varie entre 85% (pour un pays en voie de développement) à 97% (pour un pays développé). Au-delà, il est nécessaire de demander plus d'informations sur sa position géographique (code postal, adresse...) ou bien d'utiliser d'autres techniques de triangulation, basées par exemple sur des points d'accès d'un réseau Wi-Fi ou les antennes d'un réseau cellulaire (*les informations GPS venant des téléphones mobiles Internet constituent une autre technique sur laquelle planchent les experts, ndlr*) »[18]. D'après la manager, il existerait 4 raisons purement économiques au développement pour les entreprises

[17] www.cyberpresse.ca 22/11/2005
[18] www.lexpansion.com 08/12/2006

de la géolocalisation. En premier lieu, fournir du contenu ciblé et dans leur langue aux Internautes. Deuxièmement, respecter les droits de rediffusions strictement, comme pour la Coupe du Monde ou le Tour de France, ou dans un autre domaine comme pour les films ou les chansons. Selon elle, « avant la géolocalisation, aucun site n'aurait osé le faire de peur de poursuites. Maintenant, cela ouvre de nouvelles perspectives de revenus, à la fois pour le propriétaire de l'oeuvre et le diffuseur. » La troisième raison est plus classiquement la lutte contre la fraude. Enfin, quatrièmement, connaître le lieu de résidence de l'internaute permet de faire en sorte qu'il respecte de fait la réglementation en vigueur dans son pays comme l'interdiction de vendre des produits pharmaceutiques en dehors de celui-ci.
Ces arguments, à priori économiquement respectables, sont en fait, généralisés à l'ensemble du Web, des bombes à retardement concernant nos libertés individuelles. Est-on prêt à sacrifier, pour des raisons de personnalisation poussée et d'une juridiction n'admettant plus que le « Zéro faute », une telle intrusion dans nos vies privées ?

1-1-4 La mégalomanie Internet : l'exemple Google

« Au nom des tunes,
Au nom du Fils,
Au nom du Nasdaq,
Au nom du bénéfice »
Zebda

Comme nous l'avions évoqué dans le chapitre précédent, la puissance de méga bases de données, couplée aux capacités actuelles de connexion mondiale créent un univers parallèle à notre réalité primaire, celle avant l'invention des TIC. L'un des véritables problèmes se situe dans les « portes d'entrée » à cet univers. En effet, pour pouvoir y pénétrer vous devez passer le plus souvent, à moins de connaître directement le lieu où vous désirez vous rendre, par des moteurs qui font des recherches pour vous et vous rapatrient l'information ainsi demandée. Or tous les algorithmes, c'est-à-dire les programmations mathématiques, qui permettent de remonter une information pertinente à l'écran ne se valent pas, loin de là. C'est sur cela, il y a quelques années, que Google a fait la différence. En 2003, et ce sont les derniers chiffres donnés par cette entreprise qui entretient le secret autour d'elle, près de 250 millions de requêtes (de questions) étaient posées quotidiennement au moteur de recherche, toute langue confondu.. Aucune autre entreprise au monde ne peut se dire autant sollicitée !
Et toute la force de Google et de son business (et de quelques autres outsiders comme Yahoo ou Microsoft, avec Msn) se situe là : **TOUT SAVOIR**, en collectant toutes les informations mondiales et en les organisant grâce à son réseau secret d'ordinateurs (on parle de plus de 175000 machines !) qui les rend accessibles à tous les internautes. C'est d'autant plus d'actualité que le moteur affiche 80% de part de marché sur le territoire Français. « Silicon.fr »[19] pose d'ailleurs la question : «cette domination serait-elle aussi écrasante si les internautes avaient conscience que Google conserve autant de données les concernant » ? Selon un sondage mené par le Ponemon Institute, il faut savoir que 77% des internautes interrogés ne savent pas

[19] www.Silicon.fr 25/01/2005

que Google enregistre et stocke des informations à leur sujet quand ils font des recherches.
Tout savoir, à la limite dans les grandes généralités des connaissances humaines, après tout ne serait qu'une ambition d'encyclopédiste. Le véritable ennui avec Google (et les autres prétendants), c'est que son cœur de business, par un marketing complètement mégalo, car élaboré à une échelle mondiale et systématisé par les bases de données, est d'établir le profil de chaque internaute de la planète en liaison avec toutes ses activités sur la toile. « **Le business de Google, c'est vous** » résume Xavier Dalloz, un consultant spécialisé en technologie de l'information. Kevin Bankston, avocat de l'EFF aux E.U. confirme : « Son modèle commercial est fondée sur l'observation des internautes. C'est dangereux. »

Tous les grands « moteurs » se battent pour un seul Graal : la connaissance des produits que les gens achètent, des musiques qu'ils écoutent, des amis qu'ils fréquentent. Bref de leur vie. Les données personnelles valent de l'or. Et en effet nos requêtes sur la toile sont très révélatrices de nos personnalités. Cela devient très inquiétant lorsqu'on sait que Google peut aller beaucoup plus loin et propose déjà une offre (GMail) de messagerie avec une capacité de 2,5 Go pour chaque Internaute (et avoir ainsi toutes les possibilité d'analyser tous nos mails, que l'on efface plus car on a la place), une messagerie instantanée (Google Talk), le logiciel Picasa qui permet de scanner toutes ses photos sur son disque dur et des les organiser et les partager, un service de SMS… et bien d'autres[20] comme Google Earth (la terre numérisée jusqu'à votre propre habitation) ou Google Print (qui envisage la numérisation de tous les ouvrages de la planète). Google ne cache pas non plus qu'il installe sur chaque ordinateur qui le consulte, un « cookie » qui expire en… 2038. Le groupe californien a annoncé que ses nouveaux services garderaient en mémoire les requêtes, les historiques ou encore les habitudes d'achat en ligne. Bien sur, il explique que tout ceci n'est utilisé uniquement pour « améliorer la qualité des services et pour mieux comprendre comment les utilisateurs interagissent ». En fait, avec l'ensemble de ces prestations, Google peut faire du « profiling » ultra précis de tous les internautes, avec pour ambition, pour l'instant, de les utiliser pour permettre aux annonceurs de cibler très précisément leurs acheteurs potentiels. « Il y a deux fantasmes sur Google, analyse Franck Poisson, ancien patron de Google France. L'un est vrai, l'autre est faux. Celui qui est vrai c'est Google Big Brother. Oui, ils ont votre adresse IP ; oui, ils connaissent votre historique de recherche et lisent vos mails. Tout cela est vrai. En revanche, ils ne peuvent pas tout faire en même temps. Par exemple, leur alliance avec Sun pour promouvoir un système d'exploitation concurrent de Windows, je n'y crois pas beaucoup. »

La quête est planétaire : dans des notes destinées aux analystes financiers début mars 2006 et qui n'aurait jamais du tomber dans les mains du public[21], la firme avoue ses objectifs : « Chez Google, (…) l'approche que nous retenons consiste à élaborer des produits et des services **à l'échelle du monde**,(…) à considérer l'utilisation de la technologie comme une opportunité à saisir pour résoudre tous les problèmes qui n'ont jamais été résolus auparavant, tous les problèmes qui n'ont jamais eu besoin de l'être jusqu'à présent… Chez Google, nous avons conscience de n'être qu'au début de la réalisation de notre mission qui consiste à organiser l'information

[20] Pour avoir une idée sur tous les projets que Google concocte pour nous, vous pouvez en avoir un aperçu synthétique en vous rendant sur : http://fr.wikipedia.org/wiki/Google#Services_en_ligne
[21] http://adscriptum.blogspot.com/2006/03/google-definitive-strategy.html

mondiale et faire en sorte qu'elle soit universellement accessible et utilisable… Pour l'internaute, Google doit devenir une habitude au même titre que se brosser les dents. »

Et quand les projets deviennent trop gigantesques pour quelques cerveaux humains, certains déraillent : « Faites-nous confiance. Nous savons ce que nous faisons. Si vous vous y opposez, c'est que vous n'avez rien compris », déclarait Adam Smith, le directeur de projet de Google Print. Un entrepreneur de la Silicon Valley, qui souhaite garder l'anonymat, raconte aussi : « J'ai récemment rencontré des gens de Google pour leur soumettre une idée. J'en suis sorti avec l'impression que j'avais visité un état totalitaire. C'est comme si tous les employés étaient tellement contents de travailler pour Google qu'ils sont devenus débiles. Personne ne veut faire de gaffe. » Larry Page et Sergey Brin, les deux fondateurs de Google, que beaucoup de gens dans la Silicon Valley qualifient facilement « d'arrogants, idéalistes et naïfs » malgré leur talent d'entrepreneurs indéniable, ont fait afficher d'abord sur les murs du « Googleplex » (les locaux ultramodernes de Google), puis dans le document d'introduction en Bourse de la firme, le slogan « Ne faisons pas le mal ». En sont ils vraiment persuadés ? Difficile d'adhérer à ce credo lorsque vous êtes une entreprise avec des actionnaires à satisfaire. Et depuis le Patriot Act de l'après 11 septembre, Google doit satisfaire également le gouvernement et les agences de renseignements sans broncher. Il est loin le temps où les start-up de la côte californienne avaient pour idéal de créer un Internet totalement libre et débarrassé de tout contrôle financier.
Gage d'immortalité ou de mégalomanie, le mot « google » est rentré dans le dictionnaire Oxford : « Utiliser un moteur de recherche, particulièrement google.com. » ![22]

2- La science de la manipulation

« Je n'ai aucune raison de croire que celui qui m'enlèverait mes libertés, ne m'enlèverait pas, une fois en son pouvoir, tout le reste. »

John Locke

Le Gixel, Groupement des industries de l'interconnexion des composants et des sous-ensembles électroniques qui emporta le prix Orwell Novlang aux Big Brother Awards 2004, a censuré en Janvier 2006 son "Livre Bleu", qui lui avait précisément valu d'être primé pour son acceptation tout azimut des technologies de surveillance et de contrôle, et **sa volonté de conditionnement de la population**, et notamment des enfants et de leurs parents, aux "bienfaits" de la biométrie, de la vidéosurveillance et autres technologies de "contrôle".

On y lisait ainsi que pour « placer l'Europe au top niveau mondial en sécurité des personnes, des biens, sécurité de l'État et des frontières, protection contre le terrorisme », et parce que « la sécurité est très souvent vécue dans nos sociétés

[22] Ce chapitre a été écrit à l'aide de nombreuses références à un article du « Point » n°1729, novembre 2005 ; Dossier « Le monde selon Google »

démocratiques comme une atteinte aux libertés individuelles, **il faut donc faire accepter par la population les technologies utilisées et parmi celles-ci la biométrie, la vidéosurveillance et les contrôles.**

Plusieurs **méthodes devront être développées** par les pouvoirs publics et les industriels pour faire accepter les techniques de biométrie. Elles devront être accompagnées d'un **effort de convivialité** par **une reconnaissance de la personne** et par l**'apport de fonctionnalités attrayantes** :

- Éducation dès l'école maternelle, les enfants utilisent cette technologie pour rentrer dans l'école, en sortir, déjeuner à la cantine, et les parents ou leurs représentants s'identifieront pour aller chercher les enfants.
- Introduction dans des biens de consommation, de confort ou des jeux : téléphone portable, ordinateur, voiture, domotique, jeux vidéo.
- Développer les services « cardless » (sans à dire sans l'utilisation d'une carte, à la banque, au supermarché, dans les transports, pour l'accès Internet, ...), mais par un recours direct à la biométrie. »

« La même approche ne peut pas être prise **pour faire accepter les technologies de surveillance et de contrôle**, il faudra probablement **recourir à la persuasion et à la réglementation** en démontrant l'apport de ces technologies à la sérénité des populations et en minimisant la gène occasionnée. Là encore, l'électronique et l'informatique peuvent contribuer largement à cette tâche".[23] »

Voilà une manière pour le moins de présenter les choses sans ambiguïté !

2-1 « Les bonnes excuses » pour toujours plus de contrôle

« On a soif d'idéal,
Attirée par les étoiles, les voiles
Que des choses pas commerciales"
Foule sentimentale, Alain Souchon

L'actualité, relayée par les grands médias de masse, et en particulier télévisuels nous offre quotidiennement des spectacles tragiques. Affaires de meurtre, de disparition, de pédophilie, et dans un autre ordre de vols, de contrefaçons, de trafics… Le discours, qu'on a du mal à réfuter, tant certains comportements relatés paraissent contraire à nos idéaux démocratiques, incite les citoyens à se faire à l'idée qu'il faut « **lutter contre** » toutes ces plaies et que tous les moyens sont bons pour y parvenir.

Prenons l'exemple des imprimantes laser, qui ont fait couler beaucoup d'encre fin 2005. Pour soi-disant « lutter contre la contrefaçon de devises et de documents officiels », confie-t-on chez Xerox France, on apprend que depuis 10 ans les imprimantes laser couleur sont dotées d'un système de marquage invisible. HP France indique que ce sont « le département américain de la Défense et vingt sept banques internationales qui ont réclamé la mise en place de ce dispositif ». Le

[23] www.bigbrotherawards.eu.org

marquage permet de retrouver le numéro de série de l'imprimante. Il s'agit par exemple, toujours chez Xerox, d'une mosaïque de points jaunes imprimés dans une grille de 15 colonnes de large et 8 lignes de haut, placée en bas du document[24]. PC World rapporte le cas du gouvernement néerlandais qui a réussi ainsi à mettre fin à un trafic de billets de train en 2004.

Les grands médias s'enthousiasment régulièrement de cette lutte des tenants du bien contre les tenants du mal (par exemple le fameux « axe du mal » du Président G.W.Bush), et tendent à orienter de cette manière les opinions. Et **c'est comme cela qu'une technologie**, comme celle décrite dans l'exemple des imprimantes, **se fait facilement adopter par la population**, alors qu'au fond il faut souvent y voir une véritable atteinte à la vie privée. L'EFF qui milite pour « la défense des libertés individuelles dans le monde numérique » reconnaît qu'au-delà du fait que le procédé ait été caché pendant des années est un problème en soi, le traçage de documents, par exemple de pamphlets politiques[25], est une véritable atteinte à la liberté d'expression. « Sans votre accord, un acte que vous croyiez privé peut devenir public », explique l'EFF.

Un autre bel exemple de « toujours plus de contrôle » : la lutte **contre** toute **forme de violence**. Les organisateurs du Mondial de Football (9 juin – 9 juillet 2006) ont ainsi mis en place un système de billets équipés d'une puce contenant beaucoup d'informations personnelles sur le détenteur du sésame. La puce RFID (pour Radio Frequency Identification, nous y reviendront largement plus tard), doit empêcher soi-disant **le marché noir** et **l'accès à des billets aux hooligans** répertoriés par la police. Le comité d'organisation du Mondial (WMOK) a été honoré notamment pour « sa batterie de questions d'inquisiteurs lors de la commande de billets » par les Big Brothers Award 2005.

Les aveugles et déficients visuels ont permis à la RATP au mois de mars 2006 de tester un système (dénommé « BlueEyes) pour les guider avec leurs téléphones portables dans les couloirs de la station Franklin-Roosevelt, située sur les Champs-Élysées à Paris. Les informations de navigation étaient alors transmises soit par oreillette, soit directement sur le téléphone portable, de grosses flèches s'affichant sur l'écran. « Au-delà de la population des déficients visuels, ce système pourrait également s'appliquer aux touristes non francophones séjournant dans la capitale. » déclarait alors Thierry Ancelot du service information voyageur de la RATP. Peut être les prémices d'un réseau qui, petit à petit, prendra soin de nous guider dans la moindre parcelle de nos vies quotidiennes ?

Enfin, le dernier exemple, sûrement le plus touchant car il concerne des bébés, se déroule en France, au Havre. Dès la fin 2007 la maternité de l'hôpital sera dotée d'un système de sécurité qui permettra, en équipant chaque b »b » d'un bracelet électronique, **d'éviter les rapts.** Bien sûr, les arguments, toujours les mêmes car émotionnellement très percutants, sont pratiquement inopposables : « c'est à chaque fois un traumatisme pour les parents, mais aussi pour tout le personnel hospitalier lorsqu'un tel drame arrive » explique Joël Martinez, directeur de l'hôpital du Havre. « Il s'agit en fait de mettre un **bracelet équipé d'une puce** électronique à chaque bébé qui vient de naître, un bracelet qui permettra de localiser l'enfant dès qu'il

[24] www.zdnet.fr 17/10/2005
[25] www.tf1.fr 20/10/2005

quittera la chambre de sa mère ou la pouponnière. Et si l'enfant franchit une porte de sortie, une alarme sera immédiatement déclenchée » ajoute-t-il[26]. Nos chers bambins vont donc faire l'expérience de commencer le tout début de leur vie dans un monde aux tendances plutôt sécuritaires. Ou comment habituer une génération à être contrôlée en permanence.

Ainsi, la population, très nettement depuis les attentats du 11 septembre, est comme « menée par le bout du nez », car on sait très précisément comment la blesser, la choquer, l'émouvoir et lui faire prendre conscience que les mesures ainsi prises par les états et certaines sphères économiques privées pour « **lutter contre** » tel ou tel fléau sont justifiées et doivent être encouragées. Vladimir Volkoff[27] qui a beaucoup travaillé sur la notion de « désinformation » avoue que « quoi qu'on en pense l'objectivité n'existe pas en matière d'information, mais toute prétention à l'objectivité doit être traitée avec soupçon. ». Concernant l'opinion publique, « les divers critères d'objectivité que nous proposent les médias – « Untel le dit et il est honnête », « Voyez vous-même l'image télévisée », «C'est l'avis de la majorité » - ne sont pas faits pour nous rassurer. »

Cependant la population, avec le temps et le développement d'un certain esprit critique vis-à-vis des pouvoirs, se fait de moins en moins aveugler. Selon l'étude « The State of News Media 2004[28] », seulement 59% des personnes interrogées font confiance aux informations publiées dans les journaux, contre 80% vingt ans plus tôt. Selon une étude de TNS Sofres de Janvier 2005 en France, 45% des interviewés ne pensent pas que les choses se passent réellement comme elles sont montrées à la télé, contre 35% en 1988. D'autant plus que le mouvement des médias est toujours vers davantage de concentration (citons le groupe Socpress qui édite en France quelque 70 titres, dont le Figaro, l'Express, L'Expansion…) et menacent donc très concrètement le pluralisme. « L'influence des grands groupes de communication propriétaires des principaux médias, souvent en connivence avec le pouvoir politique, conduit à un manque d'objectivité, parfois même à des mensonges, à des manipulations ou à passer sous silence des informations capitales, comme on l'a vu dans le cas des véritables raisons de la guerre en Irak ou de certains scandales politiques et financiers récents. L'entretien permanent de la peur de la rareté et la mise en scène de la terreur quotidienne par les grands médias contribue à maintenir « dans le rang » des foules de plus en plus difficilement « contrôlables » par les pouvoirs en place. »[29] Le phénomène « blogs » est donc peut-être aujourd'hui, pour qui désire s'informer, une vraie alternative à certains journaux que beaucoup qualifieront d' « orientés ». L'information dispensée ne passe en général que par un seul intermédiaire, le blogger, ce qui en fait toute sa force.

[26] www.canoe.com 07/11/2005
[27] Auteur de « Petite histoire de la désinformation », Edition du Rocher, 1999
[28] Mené par l'institut Project for Excellence in Journalism aux Etats Unis
[29] La révolte du pron@tariat, Joël de Rosnay, Fayard 2006

2-2 Quelques éléments de prospective : qui peut refuser la modernité ?

« Alors, cessez de tout absorber comme une éponge ou un buvard,
Et redevenez le maître exigeant de tout ce qui cherchera à entrer».
Anonyme

Une sorte de consensus existe à l'heure actuelle sur l'utilisation d'Internet. Hormis les quelques dangers réels, notamment pour les plus jeunes (pornographie, pédophilie…), la révolution Internet est ressentie comme un progrès indiscutable pour nos sociétés, et ce à tous les niveaux, social, politique et surtout économique. Il est vrai que jusqu'à aujourd'hui, hormis dans certains pays comme la Chine, Internet est devenu un espace de liberté proprement extraordinaire, sans commune mesure dans l'histoire. Mais, et c'est bien la question que soulève cet ouvrage, est-ce que cette belle ambition va pouvoir perdurer dans un futur proche où le contrôle systématique semble gagner irrémédiablement du terrain ? Qui voudra demain remettre Internet en question, à mesure qu'il s'immisce dans nos vies quotidiennes ? Pas plus qu'on ne remettrait en question l'imprimerie et les livres. Ou plutôt avons-nous réellement le temps de le remettre en question, au fil des innovations quotidienne dont la « toile » fait preuve, et que le marché sait au demeurant parfaitement organiser ? En réalité nous nous faisons porter par l'éclosion et la rapidité des technologies, sans qu'un débat éthique ne puisse prendre place. Il n'est pas trop tard. Seules quelques associations, très peu médiatisées, en France [30] ou à l'étranger, essaient de faire leur devoir d'information. Or vu l'ampleur que prennent les TIC dans tous les pans de la société et leur rapidité de propagation, la moindre des choses serait de discuter et de décider dans quelle direction nous voulons mener nos démocraties. A une telle allure, nous sommes peut être en train de foncer vers un modèle totalitaire dans lequel personne ne pourra plus sortir de la norme.

742 experts de tous domaines ont été interrogés pour une étude en 2006 de l'institut Pew et d'Elon University[31] à propos de ce que pourrait être l'Internet de 2020. Une majorité de spécialistes (56%) pense que l'Internet saura se diffuser partout, mais 49% (contre 46%) estime que le bilan de cette **transparence** sur la vie des citoyens sera globalement négatif, à cause notamment de la pénétration de leurs données privées.

En fait nous entrons dans l'ère de l'Atawad : « Anytime, Anywhere, Any Device » (N'importe quand, n'importe où, et quel que soit l'outil). Tout devient apparemment possible, et des pouvoirs de toute puissance (par exemple le don d'ubiquité), toujours rêvés par l'être humain sur son environnement sont maintenant quasiment à sa portée, au niveau matériel.
Certains ressentent le monde technologique et les possibilités quasi infinies qui s'ouvrent à nous comme très excitant et épanouissant pour l'homme. Le Communisme au début du siècle dernier était, faut-il le rappeler, parti aussi sur une utopie où l'homme devait pleinement se réaliser. Qui pourrait aujourd'hui s'élever contre la construction d'une société technologique idéale ? A l'heure des économies, qui pourrait contester les gains procurés par les TIC, au niveau personnel comme au niveau des entreprises et des administrations ? Qui pourrait contester le « pratique »

[30] Voir leurs coordonnées à la fin de l'ouvrage
[31] www.elon.edu/predictions

d'un téléphone portable ou d'une connexion Internet ? Qui, en un mot, peut refuser la modernité ?

2-2-1 Toujours plus de gratuité

« Rien n'appartient à rien, tout appartient à tous »
Alfred de Mussey

Au fur et à mesure de leur développement, les TIC sont de plus en plus abordables. Au départ réservédx à une certaine élite (on se souvient il y a une dizaine d'années des premiers téléphones portables et de leurs utilisateurs aux terrasses de cafés sur qui l'on ironisait volontiers), leur progression, dans presque toutes les couches et les âges de la société en dix ans est proprement effarante. En décembre 2005, on comptait en France quelque 27,2 millions d'Internautes[32], ce qui la place au 7ème rang mondial. Et plus de 45 millions d'abonnés de téléphone portable au 2ème trimestre 2005[33]. Début 2006, selon une étude de Comscore Networks, on dénombrait 694 millions d'Internautes dans le monde, chiffre largement entraîné par les Etats-Unis (152 millions), suivis par la Chine (72 millions) et le Japon (52 millions). D'après la GSM association il y aurait désormais en 2006 2 milliards d'abonnés GSM sur la planète. Ce chiffre traduit une moyenne de 18 souscriptions par secondes ! Alors qu'il aura fallu 12 ans pour que cette industrie atteigne le milliard d'abonnées, le second milliard a été atteint en seulement 2 ans. L'adoption des TIC se fait donc à un rythme exponentiel en agissant, phénomène de la mondialisation aidant, comme un véritable rouleau compresseur technologique.

Le monde Occidental et les pays riches prennent la grosse part du gâteau, mais les pays en développement, souvent parce qu'ils n'avaient pas d'infrastructures préalables, peuvent passer sans difficultés aux dernières nouveautés technologiques, et ce à moindre coût. La mondialisation technologique est en marche. Annoncée pour la première fois par Nicholas Negroponte, président de l'OLPC, au Forum économique Mondial de Davos, en janvier 2005, l'association « One Laptop per child »[34] propose de fournir bientôt aux écoles via de grandes initiatives gouvernementales des ordinateurs portables à moins de 100$. Ces portables sont faits sur mesure pour des enfants dans le besoin : machine suffisamment solide pour résister à la chaleur, au froid, à l'humidité, aux tempêtes de sable, et qui permettra aux enfants de pouvoir la recharger manuellement grâce à une manivelle et de se connecter au réseau en Wi-fi.

Pour permettre toujours au plus grand nombre d' « accéder » à l'information, le supplément technologique du journal anglais « The Guardian » a lancé outre manche la campagne « Free our data »[35] (libérez nos données). Leur argument est simple : étant donné que des ministères et des agences gouvernementales (comme l'Ordnance Survey, l'équivalent de l'IGN en France) collectent de nombreuses

[32] D'après une étude du www.journaldunet.fr du 26/01/2006 recensant les individus de 11 ans et plus s'étant connectés au cours du dernier mois, quelque soit le lieu de connexions
[33] www.journaldunet.fr
[34] http://laptop.org/
[35] www.freeourdata.org.uk

données utilisant les fonds publics, il n'est pas normal qu'on refasse payer les utilisateurs et les entreprises pour y avoir accès. D'autant plus que des multinationales du web, comme Google avec par exemple son Google Earth rend paradoxalement plus de services gratuitement aux internautes. Pour les partisans du système, il n'est pas acceptable de limiter les accès puisque beaucoup, et les entreprises en particulier, pourraient tirer profit de cette libéralisation. Mais est-ce là, derrière cet argument libertaire, un véritable progrès qui se dessine ? Sommes-nous réellement aptes à supporter la « liberté » de tout savoir sur tout et sur tout le monde ?

Par ailleurs, qui ne s'enthousiasme pas aussi aujourd'hui de la « téléphonie illimitée » que propose la plupart des FAI ? Pour un prix relativement dérisoire vu le service proposé, et qui devrait tendre au fur et à mesure des évolutions vers 0, vous pouvez téléphoner depuis un fixe gratuitement et « en toute liberté ». Même son de cloche avec les téléphones portables : 9 Telecom a lancé en Avril 2006 une offre de téléphonie portable illimitée (Neuf Talk Mobile) vers les fixes et 30 pays étrangers, qui marche tant que l'utilisateur se situe sur une zone couverte par des bornes Neuf Wifi (il existe plus de 32.000 hot spots compatibles aujourd'hui).

Outre l'overdose publicitaire et le côté « pratique », l'actualité, dans un sens, nous pousse aussi à utiliser de plus en plus ces nouveaux moyens de télécommunications. Simple hasard ? Rappelons-nous, les attentats terroristes avaient semé la conviction chez certains que prendre des moyens de locomotion pour rencontrer un interlocuteur était dangereux, la conséquence étant que les rencontres devenaient de plus en plus virtuelles et que les relations à venir passeraient de plus en plus par les nouvelles autoroutes de l'information. Or, sans tomber dans la parano, il faut voir qu'à terme avec la « convergence » probablement toutes les communications quelles qu'elles soient passeront par le réseau Internet. Et, alors qu'il était difficile par exemple en France d'intercepter la voix du temps de l'opérateur national (France telecom), la VoIP, fusion entre l'informatique et les télécoms, permet déjà et permettra encore davantage à quasiment n'importe qui de le faire. En effet **toutes nos télécommunications sont ainsi réduites à de simples fichiers informatiques** qu'il faut pouvoir récupérer et lire. Sans simplifier à outrance, on peut quand même dire que **plus la technologie et le moyen de communication sont récents, plus ils sont facilement interceptables.** La procédure est ainsi simplifiée pour les agences de renseignements qui désirent écouter. Ce qui est peut-être plus inquiétant, c'est que **ce pouvoir absolu d'écouter pourrait**, si la tendance s'affirme, **être accordé à n'importe quel citoyen**. De là à penser que certains d'entre-nous choisirons d'être les oreilles complices d'un système où la délation serait la norme…

Pour soutenir cette croissance des TIC, l'argument d'avoir du « gratuit » (musique, jeux vidéo, films téléchargés illégalement) commence aussi à produire ses effets. Ouvrons ici une parenthèse : le « fond » de l'affaire est pourtant une piste intéressante à étudier, s'il n'y avait malheureusement pas ce système de traçage propre aux TIC, pour l'établissement d'un nouveau paradigme (que nous aborderons en conclusion). En effet, les jeunes notamment ne trouvent pas amoral le fait de s'échanger par l'intermédiaire du réseau des fichiers en tout genre. Ceci rentre évidemment frontalement en contradiction avec la logique purement capitaliste. Ce qui semble être une nouvelle « ère » de l'abondance permet d'ouvrir un formidable

espace à la gratuité dans tout ce qui concerne la création humaine. Désormais on peut donner une information sans pour autant la perdre. Par exemple faire entendre de la musique, partager et créer des logiciels, des livres sans en perdre la propriété. On peut donc avoir le plaisir de donner sans avoir le déplaisir de perdre ce que l'on donne. Par conséquent, à l'inverse de l'économie de l'énergie où la valeur dépend de la rareté, dans celle de l'information la valeur résulte de l'abondance qui permet d'entretenir une spirale évolutive où l'on donne et l'on reçoit plus. Plus il y a de gens branchés sur un réseau, plus chacun peut y trouver de l'intérêt, et plus le réseau à de la valeur. Les forums de discussions très actifs sur Internet participent bien de cette idée. Chacun à intérêt à ce que l'autre possède ce qu'il a. Il en sera fini ou presque des réseaux pyramidaux ou chacun lutte contre l'autre pour accéder à un niveau « supérieur », mais on pourra fonctionner en réseau, en intelligence collective avec d'autres. **On fera « avec » plutôt que « contre ».** C'est un peu comme dans l'art martial japonais de l'aïkido on l'on se sert de la force de l'adversaire pour le mettre à terre. En fait, ceci se fera non pas dans le sens d'une résistance à ce qui est là, mais plutôt dans le sens d'une satisfaction de nos besoins réels
Des solutions alternatives apparaîtront probablement pour permettre aux artistes de créer et de vivre en même temps de leur travail sans passer obligatoirement par le business des « majors » qui essaient par tous les moyens de colmater le barrage.

Dans le même esprit, on entend de plus en plus parler des « logiciels libres » (et du célèbre système d'exploitation Linux) qui sont librement accessibles, copiables, modifiables et diffusables. L'utilisation de tels logiciels n'engendre pas de discrimination par l'argent dans la mesure où tout le monde peut se les procurer. Il faut voir qu'actuellement pour les artistes, avec la façon dont les droits d'auteurs sont utilisés, leur champ d'action est limité : l'artiste en effet n'a pas le droit d'utiliser la voie montrée par un autre artiste. Il est interdit de réutiliser des éléments appartenant au patrimoine artistique pour chercher à composer une nouvelle œuvre. Or en réalité, il est évident qu'une œuvre d'art est le résultat d'influences, d'idées, de cultures, mélangées et aménagées par l'artiste. L'œuvre d'art n'est pas l'expression unique et originale d'un artiste. Le monde du « libre » (ou copyleft) est une manière de reconnaître cette réalité (notamment sous l'angle de la modification et de l'adaptation de l'œuvre initiale), de reconnaître qu'il existe une certaine généalogie entre les œuvres. Dans un monde où tous les contenus seraient libres, vous pourriez alors posséder plusieurs œuvres, soit achetées, soit copiées chez vos amis. Vous pourriez remercier les auteurs soit en leur envoyant une donation sans passer par les intermédiaires, soit en leur achetant une de leurs œuvres. Vous pourriez également apporter vos modifications aux œuvres pour adapter le contenu à votre vision, et la partager avec d'autres.

Les grandes multinationales du Web (Google, Yahoo, Skype…) ont bien compris cette tendance au « tout gratuit » et ont, paradoxalement pourrait-on croire, construit leur modèle économique dessus. Et apparemment ce modèle devrait fonctionner puisque leur capitalisation boursière dépasse bien souvent celles des grandes multinationales du Dow Jones. D'après ces firmes, il vaut mieux facturer un service à 10 centimes à des millions de personnes et sans renfort de publicité (puisque le bouche à oreille fonctionne dans ces cas là à plein lorsqu'un internaute connaît un « bon plan » à partager) plutôt que de « ramer » avec des budgets de publicité gigantesques pour trouver 10.000 clients acceptant de payer 100 Euros pour le service. Il faut cependant être conscient que ces firmes n'ont jamais eu des buts

philanthropiques. En effet, elles proposent du gratuit pour attirer et capturer des usagers et les vendre ensuite à des annonceurs ou les valoriser en bourse. L'émergence du marché de la vie privée, que l'on détaillera dans un chapitre suivant, est le scénario logique à ce « néo-capitalisme ».

Il est évident que ces nouvelles donnes sur la gratuité d'accès à certaines données qu'offre le réseau paraissent (presque trop) idylliques, qu'il faut peut-être faire preuve de discernement, et que les scénarios tout tracés d'avance sont toujours à envisager avec prudence. Il serait donc judicieux de suivre l'actualité pour vérifier que toutes ces bonnes intentions, à l'heure du renversement des symboles, nous conduisent bien vers un épanouissement de l'être humain et non vers son asservissement.

Logiciels libres : L'expression « logiciels libres », donnée par Richard M. Stallman, fait référence à la liberté pour tous (simples utilisateurs ou développeurs) d'exécuter, de copier, de distribuer, d'étudier, de modifier et d'améliorer le logiciel. Plus précisément, elle fait référence à quatre libertés pour un individu ayant acquis une version du logiciel, définies par la licence de ce logiciel :

- la liberté d'exécuter le programme, pour tous les usages (liberté 0) ;
- la liberté d'étudier le fonctionnement du programme, et de l'adapter à ses besoins (liberté 1) ; pour cela, l'accès au code source est nécessaire ;
- la liberté de redistribuer des copies, donc d'aider son voisin (liberté 2) ;
- la liberté d'améliorer le programme et de publier ses améliorations, pour en faire profiter toute la communauté (liberté 3) ; pour cela, l'accès au code source est nécessaire.

Un logiciel ne respectant pas totalement une de ces libertés est appelé logiciel propriétaire par les partisans du logiciel libre. Ceci est ainsi par exemple le cas des logiciels Microsoft.

Pour illustrer le principe du logiciel libre face au logiciel non libre, on peut comparer cela à la recette de cuisine d'un gâteau, conformément à une analogie fréquemment utilisée par Richard Stallman :

- selon le principe du libre : vous avez obtenu légalement cette recette par n'importe quel moyen (revue, bouche à oreille...). Vous avez le droit de redistribuer cette recette à qui vous voulez et vous pouvez la modifier puis la redistribuer comme il vous plaît.
- selon le principe du logiciel non libre : vous n'avez pas accès à la recette mais uniquement au gâteau déjà fait. Vous ne pouvez manger le gâteau que dans une seule cuisine, et personne d'autre que vous ne peut le manger. Quand bien même la recette serait fournie avec le gâteau, toute copie ou modification serait interdite.

(Source : wikipedia)

Les logiciels libres ont deux caractéristiques principales qui font penser qu'ils sont aujourd'hui **une alternative, au moins pour un temps**, aux produits dit propriétaires :

- ils permettent une utilisation de l'informatique en toute légalité. Qui en effet, n'utilise pas sur son micro personnel des copies de logiciels propriétaires comme Microsoft Office ou bien d'autres. L'alternative « libre » permet donc de ne pas franchir la ligne jaune.
- Ils offrent beaucoup moins de failles de sécurité que leurs homologues propriétaires. En effet il faut voir que le « libre » fonctionne sur le principe d'une communauté mondiale de programmeurs passionnés et indépendants qui améliorent sans cesse les logiciels. Ainsi, normalement, si l'un d'eux avait par exemple la mauvaise intention d'installer une « backdoor » sur l'un des logiciels en co-développement, celle-ci serait repérée rapidement par les autres programmeurs, et ainsi supprimée.

2-2-2 Toujours plus de « portabilité »

« Let's disconnect all communications »
Kubb

La miniaturisation est effectivement en marche dans le secteur des TIC. Tout y passe : téléphone portable, ordinateurs portable, mémoire de masse, lecteurs multimédia, etc.
Sans trop se tromper, on peut penser qu'à l'avenir ces concentrés de technologie seront regroupés dans un appareil unique, après miniaturisation à l'extrême. En quelque sorte **le couteau Suisse du 21ème siècle**. Déjà les derniers téléphones portables, notamment vendus au japon ont une mémoire interne, un système GPS, font office de lecteur multimédia et servent à l'occasion de carte bancaire.
Par exemple, grâce au MPS (le GPS adapté au monde des téléphones portables, pour Mobile Positionning System) on peut localiser, encore plus précisément qu'avec le système des relais actuels (appelé aussi BTS ou station de base), l'utilisateur d'un téléphone portable. Au départ réservé au cadre exclusif d'enquêtes judiciaires (comme après l'assassinat du préfet de Corse Claude Erignac), ces pratiques sont déjà passées dans le secteur privé. Le site « Ootay »[36] permet ainsi à n'importe quel Français de visualiser où l'un de ses proches se trouve en offrant un service de géolocalisation relativement précis, c'est-à-dire en zone urbaine entre 100 et 300 mètres près. Dans la même veine, Disney[37] à lancé dans l'été 2006 aux Etats-Unis une offre permettant aux parents de savoir où se trouve précisément leur progéniture, de définir les heures auxquelles ils peuvent être appelés, de limiter leur consommation, etc.
Mais l'eldorado marketing qui s'offre au monde de la « portabilité » n'en est qu'à ses prémices. Ainsi, une salle de cinéma qui se retrouverait pour la projection d'un film avec des places invendues pourrait cibler les promeneurs alentours et leur proposer une offre promotionnelle pour venir voir le film. Cette offre, ainsi qu'un plan du quartier s'afficheront directement sur l'écran du portable. Bien sur la localisation se fait à l'insu de la personne visée : dès que celle-ci pénètre dans une « cellule » de la zone de couverture par les antennes réceptrices, un signal imperceptible rebondit sur l'appareil et retourne ensuite vers l'antenne. Le temps écoulé indique au cinéma la

[36] www.ootay.fr
[37] www.vnunet.fr 07/04/2006

distance qui la sépare de l'antenne et permet de savoir, à quelques mètres près, où se trouve exactement le client.
Au Royaume-Uni, les usagers du service Zagme ayant au préalable indiqué leurs centres d'intérêts sont automatiquement et personnellement alertés, via leur téléphone, au moment où ils passent devant un magasin lorsqu'une offre publicitaire est supposée les concerner… Fini le temps de la flânerie et du hasard : **la machine s'occupe de votre temps libre**. Elle décide à votre place en vous alléchant sur le prix et en vous adressant un discours promotionnel adapté à vos goûts personnels[38].
En fait la question est de savoir si la personne a donné son accord pour être localisée et dans le cas contraire si elle peut réellement s'y opposer. Or la réponse n'est pas tout à fait claire, ni du côté des opérateurs, ni des forces de l'ordre qui ont tout intérêt à pouvoir pister les gens à leur insu. Ainsi on sait que lors des manifestations anti-mondialisation (Prague, Milan, Nice…), la police a utilisé un système comparable pour localiser les leaders de la manifestation et tenter de limiter leurs champs d'action.
La portabilité est aussi au cœur des stratégies du groupe Suédois Ericsson qui associe vidéo et géolocalisation. Ainsi l'automobiliste peut à l'aide de son portable et des caméras de surveillance du réseau autoroutier le plus proche, en fonction de l'intensité du trafic, choisir l'itinéraire le moins encombré.
A terme, même les plus modestes acteurs économiques tels que les petits commerçants prennent la voie ainsi tracée par les plus grands. Les clients d'une épicerie de quartier pourront bientôt payer leurs achats en passant leur téléphone cellulaire devant un capteur, rendant obsolètes porte-monnaie, carte de fidélité et même les caissières de chair et d'os. Déjà l'épicerie familiale Chevy Chase vieille de 50 ans est l'un des premiers commerces de la région de Washington aux Etats-Unis à vouloir implémenter ce type de paiement, et proposer aux clients des coupons de réductions électroniques, des bonis et des informations sur le magasin par le biais de messages textes[39] …
Le temps se rapproche où cet outil nomade pourrait devenir **la prothèse principale** des individus, sorte d'organe artificiel aux multiples fonctions.

2-2-3 Toujours plus de connexion

« Le seul ordinateur réellement sécurisé est un ordinateur éteint… Et encore… je ne suis pas sûr. »

www.assiste.com

La tendance de fond, que beaucoup auront repéré, est aujourd'hui la **« mise en réseau » systématique** par les TIC des produits et des individus. Tout à commencé avec les réseaux des téléphones portables et Internet. Et cela s'affirme de manière exponentielle. La VoIP est de plus en plus populaire (on prévoit rien qu'en France 180 millions de lignes VoIP en entreprise en 2009 soit 40% du marché[40]). Aujourd'hui et l'on y reviendra aussi plus tard, ce sont les biens de consommation (appelé « **l'internet des objets** »), et les hommes qui sont en passe d'être « connectés », et

[38] Manière de voir n°71 / Le monde diplomatique / Obsessions sécuritaires / Octobre Novembre 2003.
[39] www.canoe.com 25/09/2006
[40] Etude réalisée en 2004 par l'Idate

donc corollairement « tracés », l'un n'allant pas sans l'autre sur les infrastructures actuelles du réseau Internet.
Le vrai problème arrive - ce qui n'avait jamais été le cas dans l'histoire jusqu'à aujourd'hui - lorsque 2 paramètres sont mis en relation : la **connexion** (donc des flux sortants et flux entrants d'informations) d'une part et **les donnés personnelles** d'autre part.
Sans probablement vous en rendre compte, la première fois que vous avez joué ce scénario fut au moment où vous avez rentré sur votre téléphone portable et/ou sa carte Sim les noms, prénoms et numéros de téléphones de tous vos « contacts ». Alors qu'avant, avec le carnet de téléphone papier, il y avait une sorte d' « étanchéité » entre votre vie privée (vos amis, familles) et l'extérieur, aujourd'hui le sas est ouvert. Bien sur on nous conforte chaque jour dans l'idée que des « filets » de sécurité sont là pour tout protéger (ex : le code Pin pour un portable). Mais si des hackers et des agences de renseignements sont déjà capables aujourd'hui d'accéder via le réseau à notre vie privée, demain les ouvertures seront encore plus béantes.
La 2nd fois, et l'exemple est peut-être plus évident, où vous avez mis les 2 paramètres (connexion et données personnelles) en relation, est lors du branchement de votre PC au réseau Internet. Sur votre PC se trouvent peut être vos comptes, des photos de familles, vos passions…. Bien sûr aujourd'hui, et malgré les spywares et autres animaux de compagnie, les intrusions menaçant votre vie privée sont probablement limitées : répétons-le, la **paranoïa n'est pas du tout de mise aujourd'hui**, et vous pouvez encore consulter tranquillement votre ordinateur ! Néanmoins, au rythme où s'accélèrent les choses, c'est le futur proche qui s'avère plus menaçant. On apprend par exemple que Microsoft avait déclaré qu'à partir de mi-2006, les utilisateurs de son système d'exploitation étaient obligés de le mettre à jour, en ligne, au fil des « updates » (mises à jour) disponibles. Une manière un peu cavalière de ne pas laisser l'utilisateur maître de son PC, et qui sait, de le surveiller d'un peu plus près. D'autant plus lorsqu'on connaît les rachats par le géant de Redmont de sociétés privées spécialisées dans le renseignement. Récemment, des utilisateurs du système d'exploitation se sont aperçus[41] que la nouvelle version du système anti-piratage WGA (Windows Genuine Advantage, qui permet d'authentifier à distance sa copie du logiciel) de Microsoft envoie des données à l'éditeur à chaque démarrage de l'ordinateur et non uniquement lors de la première installation. Microsoft, de son côté, assure que WGA lui transmet des informations quotidiennes uniquement à des fins de maintenance… Selon le blog de Lauren Weinstein, activiste renommé, l'éditeur reçoit au moins quotidiennement lors de chaque connexion l'adresse IP et l'heure de connexion de chaque utilisateur dans le monde.

Dans le même ordre d'idée, il est aussi intéressant d'observer, lors d'une connexion Internet, comment fonctionne son modem (haut ou bas débit). Au fur et à mesure du surf de l'internaute, le modem permet de « télécharger » les pages pour les afficher. On appelle aussi cela le « download », et on comprend bien pourquoi sa mesure (en octets) grimpe au fur et à mesure de la connexion : ceci est dû au « rapatriement » des pages et des images (qui pèsent un certain « poids », mesuré en octets) du web sur l'ordinateur. Mais il est tout à fait remarquable de noter aussi que l' « upload », c'est-à-dire les données qui partent de votre ordinateur pour aller sur le réseau, le contraire du « download », est souvent aussi, en terme de mesure, très significatif. Et l'ennui c'est qu'en fait l'on ne sait pas très bien où vont ces données : ce qui est sur c'est qu'elles vont bien quelque part. Bien sur l'upload peut être volontaire, et c'est

[41] www.ZDnet.fr 8/06/2006

souvent le cas par exemple lorsqu'on partage des fichiers avec des logiciels de peer-to-peer, lorsque d'autres internautes viennent se « servir » sur votre ordinateur. Mais l'upload « non consenti » est bien réel, malgré toutes les protections en firewall que vous pourrez instaurer, et peut-être faudra-t-il commencer à s'en inquiéter. Actuellement, chez tous les fournisseurs d'accès, le débit théorique en upload est toujours beaucoup plus faible qu'en download. Très souvent par exemple, un débit en téléchargement de 20 Mégabits/secondes correspond à un débit en upload entre 5 et 6 Mbits/s. On peut seulement se demander, sauf cas particulier (PeerToPeer, upload de sites web entiers…) à quelles fins un tel débit peut bien servir. C'est peut être **la première étape, d'une connexion permanente au réseau** où se croiseront flux de données entrants et sortants et où il deviendra très difficile de se protéger. A moins que, comme nous le verrons plus tard[42]**, la tendance s'affirme à la délocalisation du disque dur de son ordinateur vers des espaces de stockage mutualisés** accessibles via le réseau, proposés d'ores et déjà par des multinationales du web. Paradoxalement, il faudra donc se connecter à d'autres ordinateurs (les serveurs de ces grandes firmes) pour accéder à ses données personnelles ! **Ou comment privé et public en viennent à s'inverser.**

Progressivement, ce qu'on appelle les appareils « nomades » vont eux aussi se connecter au réseau sans avoir à passer par un ordinateur. Ils vont devenir « autonome », grâce à (ou à cause de) la généralisation du Wi-fi sur la planète (la ville de San Francisco, grâce notamment au lobbying de Google, a annoncé fin 2005 qu'elle allait devenir un gigantesque lieu (Hot Spot) Wi-fi quasi gratuit. Bien d'autres villes devraient aussi suivre le mouvement). Bien sur on connaît les PDA et autres téléphones portables. Plus insolites, les premiers appareils photos Wi-fi commencent à apparaître. Le système est simple : vous prenez des photos lorsque par exemple vous êtes en voyage à l'autre bout de la planète, et l'envie vous prend de partager immédiatement ce moment unique avec la terre entière. En quelques clics, sans fil et par Internet vous pouvez les envoyer à quiconque dispose d'une adresse e-mail. En publiant ainsi sur le web, malgré les discours sur les sécurités du réseau, qui sont souvent un leurre, vous offrirez votre intimité à l'apparente bienveillance du réseau. A terme on pourra tout à fait à partir de ce simple cliché trouver des **relations** entre le propriétaire de l'appareil (IPv6) et les personnes auxquelles l'image à été envoyée (adresses emails) qui seront probablement pour partie ceux qui sont sur la photo.
On voit tout l'avantage d'un tel système pour des pays aux libertés surveillées (comme la Chine). Le travail des forces de répression serait ainsi grandement facilité, Internet apportant des preuves tangibles pour remonter un réseau d'opposants au système. L'organisation Humanitaire Human Rights Watch (HRW) accusait d'ailleurs dans un rapport présenté en Aout 2006 les géants du web de complicité passive envers le régime de censure Chinois[43].
Sans parler du Wi-fi, il est un fait que les photos circulent aujourd'hui énormément sur le réseau, de la simple pièce jointe envoyée à un ami, aux sites de développement de clichés papier qui téléchargent vos photos numériques par dizaines, en passant par les sites d'albums photos on-line qui permettent le partage entre amis et proches de clichés personnels. Le rachat récent, par Google et son

[42] Cf chapitre « Un disque dur et une connaissance planétaire »
[43] www.vnunet.fr 10/08/2006
La Chine est l'un des pays où la surveillance de l'Internet par les autorités locales est la plus élevée au monde à tel point que le réseau national est surnommé le *"Great Firewall" (le Grand Pare-feu)*. Il est par exemple reproché à Yahoo d'avoir livré à plusieurs reprises les identités d'internautes critiques envers le régime en place et qui ont conduit à l'emprisonnement de quatre d'entre eux.

activité de gestion de photos (Picasa), de Neven Vision, une société spécialisée dans les logiciels de reconnaissance photo peut faire froid dans le dos. Même si la firme de Montain View n'a pas indiqué ce qu'elle comptait exactement en faire, Adrian Graham, responsable de Picasa indique dans son blog qu'il « pourrait simplement servir à repérer s'il y a une personne sur une photo mais qu'il pourrait aussi permettre un jour de reconnaître les individus, les lieux, et les objets »[44]. Etendu au monde Internet, on peut déjà en imaginer toutes les implications… Dans le même esprit, une société suédoise[45] dénommée Polar Rose entend permettre de rechercher des visages à partir de photos en se servant d'une technique alliant les mathématiques et l'intelligence des utilisateurs. Leur logiciel construit un modèle 3D des visages de sorte que les Internautes puissent facilement identifier des personnes. En fournissant une partie du « code » du logiciel, la société espère inciter d'autres entreprises à créer des applications semblables !

Le **Wi-fi** est une technologie de réseau informatique **sans fil**. Mis en place au départ pour relier et faire communiquer les ordinateurs (les mettre en réseau) entre eux sur un même lieu (par exemple dans une entreprise), le Wifi est en train de s'imposer comme moyen principal d'accès à l'Internet haut débit. On peut conjecturer que dans un futur proche, l'on pourra, dans de nombreuses villes, se connecter via son ordinateur (portable) depuis n'importe quel endroit, sans fil et gratuitement.

La **VoIP**, dite voix sur IP n'est rien d'autre que la fusion des télécoms et de l'informatique en réseau. C'est la possibilité de téléphoner à moindre coût, et même a priori gratuitement (c'est ce que font les utilisateurs du logiciel Skype) en utilisant le réseau Internet mondial. Amélioration sensible de la qualité et du confort de la communication, réduction importante des coûts, et services novateurs (convergence IP : outils collaboratifs, visio…) font de la VoIP une solution qui va probablement tendre à s'imposer pour les particuliers comme pour les entreprises dans les prochaines années. Rien qu'en France sur l'année 2005, la téléphonie sur IP à progressé de 252% et compte 3,3 millions d'abonnées. En 2011, elle devrait concerner au moins 80% des lignes téléphoniques mondiales (Chiffres Idate). On a remarqué que la popularité de la VoIP croît très significativement quand elle est couplée à un réseau sans fil. Aux Etats-Unis, c'est même la Voix sur Wi-fi qui devient l'argument principal pour déployer un réseau sans fil en entreprise. La **VoWi-fi est une tendance forte à court terme.** Elle combine les avantages de la VoIP avec ceux du Wi-fi (standard universel, apport d'une large bande passante, liberté du sans fil, tendance du nomadisme, souplesse due à l'absence de cablage…). Les experts indiquent que le nombre de mobiles Wi-fi atteindra 13,5 millions en 2007 pour exploser à 136 millions en 2010.
Derrière toutes ces dénominations techniques un peu barbares, on retrouve le problème de **la convergence** : à terme les technologies permettront une interopérabilité automatique et sans couture de tous les réseaux apparemment hétérogènes (VoIP, Voix sur Wi-Fi, VoIP sur UMTS ou GPRS, voire Voix sur WiMax depuis tous les types de terminaux (mobiles) et système d'exploitation (comme Windows Mobile)[46]. Ainsi dans moins de 5 ans, la majorité des appels dans le monde transiteront par Internet. La VoIP doit débarquer par exemple sur les téléphones mobiles japonais dès 2007 et indique que, comme pour la téléphonie

[44] www.lemondeinformatique.fr 16/08/2006
[45] www.fr.computermagazine.be 22/12/2006
[46] www.conventionvoip.com

fixe, la généralisation est en route[47]. Grâce à des logiciels de type Skype et sans avoir à passer par un service payant (type GSM), il sera possible de téléphoner gratuitement, de s'échanger des SMS, de télécharger de la musique et même de recevoir la télévision assis dans un parc public ou dans un aéroport, son téléphone portable à la main. Nous n'aurions en fait plus grand-chose à envier aux Dieux.
Un nouvel espace de liberté ? En apparence tout du moins.

2-2-4 Etude de cas : toujours plus de pouvoir

« De grands pouvoirs impliquent de grandes responsabilités »
Spiderman[48]

Les exemples commencent en effet à affluer concernant les TIC sur un discours du « toujours plus » de gratuité, de portabilité et de connexion. Vous en trouverez probablement de plus en plus dans l'actualité.
Le cas suivant est celui qui nous à semblé le plus révélateur : depuis fin 2005 et ce pendant 6 mois dans un test grandeur nature mené par France Telecom, 200 habitants de Caen ont été équipés de téléphones portables dotés d'une puce NFC[49] (pour Near Field Communication), une norme initiée par Sony et Philips et qui augure de ce futur couteau suisse technologique dont nous avons parlé dans les précédents chapitres. Le concept est assez simple : faire du téléphone mobile un appareil capable de remplacer les cartes de paiement et de recevoir des informations – audio, vidéo, texte – en étant placé devant des bornes ou des étiquettes de type RFID[50] par exemple. Le tout grâce à une puce intégrée capable de recevoir et d'émettre des ondes de courte portée (moins de 10 cm).
Pour cette première mondiale, particulièrement sous médiatisée, les clients ont pu ainsi payer directement avec leur portable en passant le dos du téléphone devant un lecteur estampillé du logo « Fly Card », ouvrir des barrières de parkings, le débit se faisant directement sur le compte bancaire, ou aussi recevoir de l'information en le passant devant une étiquette particulière. Dans un abribus, ils ont pu ainsi obtenir un message audio leur indiquant l'heure du prochain transport. Devant un cinéma ou une affiche, ils ont pu visionner la bande-annonce du film. Même chose devant un monument historique où un court texte de présentation leur a été fourni[51]. Et bien d'autres projets avec les Universités et les municipalités qui pourront s'en servir comme carte de fidélité, contrôle d'accès, accès aux transports en commun…

Revenons quelques instants au mode de paiement. Le porte monnaie électronique Monéo a peine à séduire les Français. Or cette version sans contact, adaptée aux petits paiements de moins de 20 euros qui ne nécessite aucune autorisation, a été un vrai succès sur le plan de cette expérimentation sur Caen. Cette décision de passer au paiement sans contact n'est pas une affaire française. Il s'agit d'une tendance internationale venue des grands émetteurs de carte bancaire : American

[47] www.atelier.fr 14/10/2005
[48] Film de Sam Raimi, 2002
[49] www.vnunet.fr 19/10/2005
[50] Voir chapitre suivant
[51] www.01net.com 20/10/2005

Express (ExpressWay), MasterCard (PayPass), et Visa (Visa Walver). Bruno Carpreau, vice-président de MasterCard Europe explique : « Nous voulons rendre les paiements par carte plus conviviaux et plus rapides pour s'attaquer à des circonstances où le paiement en espèces reste privilégié : restauration rapide, péages, cinéma, parking, stade, épiceries. » **Les paiements en espèces, qui pourtant symbolisaient jusqu'à maintenant un acte d'achat anonyme**, sont, on le voit, en train d'être progressivement supprimés, ce qui est grave pour la démocratie.

Les banques du groupe Crédit Mutuel ont annoncé le lancement en partenariat avec NRJ Mobile, d'un service permettant de payer ses achats avec son téléphone portable. Une version pilote du projet à été lancée dès la fin novembre 2006 dans la ville de Strasbourg auprès de 50 commerçant durant 6 mois. La carte bancaire est directement intégrée dans la carte SIM du téléphone, et le paiement se fait « sans contact ». Bien sûr ; des chaînes telles que les cinémas UGC sont très intéressées par l'expérience. "Notre solution transmet le paiement en quelques dixièmes de secondes, ce qui permet de réduire considérablement les files d'attente traditionnellement longues dans les cinémas de l'enseigne", déclare Nicolas Guilbert, directeur Marketing chez NRJ Mobile. En arrivera-t-on comme au Japon où, comme l'explique ce dernier, "J'ai vu il y a un an, lors d'un voyage d'étude, des gens payer une salade dans une superette avec leur téléphone portable."[52]
La Caisse d'Epargne présentait quant à elle Movo, un service qui permet de transférer de l'argent de particulier à particulier depuis son portable, via un SMS ou un serveur vocal[53].

Les paiements électroniques devraient en effet avoir doublé en 2009 par rapport à 2004[54]. L'étau se resserre autour des consommateurs. Guido Mangiogalli, de Visa Europe, confirme : « Nous sommes en train de travailler sur une offre commerciale adéquate pour que les commerçants préfèrent les achats sans contact à la manipulation de monnaie et pour que les banquiers aient un intérêt financier à le proposer à leurs clients. » La généralisation du système devrait être pour… fin 2007[55].

Autre exemple de ce « toujours plus », le développement du numérique hertzien. On peut imaginer, dans un avenir pas si éloigné, comme possible la liberté de connexion à tous les systèmes de vidéosurveillance en circuit fermé d'une ville. Il serait alors possible de se brancher sur le système vidéo de sa banque ou celui d'un musée ou d'un cinéma pour estimer l'importance de la file d'attente. Par une simple touche, on pourrait ainsi se retrouver en quelques instants aux quatre coins de la ville, et assouvir un pouvoir jusqu'alors réservé au divin, une pulsion scopique de vision à distance.

[52] www.journaldunet.com 23/10/2006
[53] www.01net.com 12/10/2006
[54] Reuters, 4/05/2006
[55] www.01net.com 18/11/2005

2-3 Focus : qu'est ce que la technologie RFID[56] ?

L'étiquette RFID (ou tag) vient de l'anglais Radio Frequency Identification pour identification par radio-fréquence. Cette technologie **devraient rapidement remplacer les codes barres** dans leur marquage des marchandises et produits de consommation du fait de leurs nombreux avantages : **lecture sans contact**, omnidirectionnelle, au travers des emballages, à grande distance et avec une capacité à **mettre à jour l'information embarquée dans l'étiquette**. Elle se compose d'une puce d'une taille minimale d'un millimètre carré, et d'une antenne, toutes deux placées sur un support de quelques dizaines à plusieurs centaines de millimètres carrés. La majorité des étiquettes, dites « passives » ne sont pas alimentées en énergie. Cette dernière leur est fournie par le lecteur au moment de l'interrogation, grâce à une induction électromagnétique. Les étiquettes sont ainsi des matériels extrêmement robustes, dotés d'une durée de vie très longue. Bien que cette technologie date de plusieurs dizaines d'année (le principe de la radio fréquence à été utilisé pour la première fois en 1950 pour identifier les appareils de la Royal Air Force en vol), sa miniaturisation (les puces ne sont guère plus épaisses qu'une étiquette classique), l'émergence de standard et la baisse drastique du coût d'acquisition (selon une récente étude de LogicaCMG, les étiquettes RFID ultra haute fréquence devraient connaître une baisse de coût de 70% d'ici 3 à 5 ans.) en font un marché prometteur (la puce pouvant contenir beaucoup plus d'information que le code barre classique, soit aujourd'hui entre 96 bits et 2 Mbits)**.** Selon une étude IDtechEx, le marché mondial de la RFID devrait décupler en dix ans. De 2,7 Milliards de Dollars en 2006, la RFID générerait ainsi un revenu de 12,3 Md$ en 2010 et 26,2 Md$ en 2016. Selon l'étude, 1,3 Milliards d'étiquettes ont été vendues en 2006. Le marché n'en est qu'à ses balbutiements et est en train d'exploser. Pour preuve, le nombre d'étiquettes vendues annuellement devrait être multiplié par 450 d'ici 2016.

Les étiquettes « intelligentes » RFID, on le voit, ont de grandes chances de **rentrer sous peu dans notre intimité**. D'autant plus qu'elles vont pénétrer dans l'ère de l'infiniment petit. Déjà, Hitachi a déclaré récemment avoir mis au point la plus petite puce électronique sans contact du monde. Ce composant de 0,15 millimètres de côté est capable de transmettre des données par une liaison sans fil grâce à une antenne ultra fine qui l'entoure[57].

Plus généralement, les promoteurs des RFID envisagent en fait de multiples implantations sur de nombreux supports :

- Dans la gestion de la chaîne logistique, tous les niveaux d'emballages étant concernés : containers, palettes, cartons et articles eux-mêmes.
- Les billets de banques, cartes de crédit, téléphones portables pourront utiliser des puces pour un paiement sans contact.
- Tous types de petits appareils pourront communiquer via ces puces.

Mais le plus angoissants c'est qu'ils prévoient aussi d'en équiper :

- Les animaux domestiques,
- Les êtres humains qui pourront porter une étiquette par exemple dans le cadre de leur suivi hospitalier ou pour accéder à des locaux sensibles. Fin

[56] Ce chapitre est inspiré d'un article de http://solutions.journaldunet.com/ paru le 30/11/2005
[57] www.lexpansion.com 06/02/2006

2006, Hitachi à présenté une balise RFID à fonctionnalité Wi-fi pour pouvoir parfaitement localiser les personnes dans un bâtiment et savoir quand elles y entrent et en sortent[58]. Quitte à en équiper les vêtements.

En fait énormément de métiers sont concernés par cette technologie. On pourrait citer :

- Les compagnies aériennes pour la gestion des bagages,
- Les transporteurs pour le marquage des colis,
- Les bibliothèques pour l'étiquetage des livres,
- Les constructeurs automobiles ou de matériel électronique pour l'étiquetage et le suivi de pièces entrant dans la chaîne de production,
- Les laboratoires pharmaceutiques pour la traçabilité des médicaments.

De nombreuses applications ont déjà débuté : en France par exemple, le duo d'entreprises Tagsys-Ident a remporté un appel d'offre émis par le Sénat pour protéger et identifier les 450 000 volumes de sa vaste bibliothèque en ayant recours à des technologies RFID[59]. Et en déployant un véritable arsenal, avec plusieurs centaines de milliers d'étiquettes à puce, de stations de lecture, de portiques antivol, d'automates de prêt et des lecteurs RFID portables Wi-Fi. En quelques mois, Tagsys et Ident ont remporté plus de 20 projets RFID pour des bibliothèques publiques (communauté d'agglomération d'Aurillac, villes de La Seyne-sur-Mer et Douarnemez) et universitaires (Paris X à Nanterre). Rappelons que Tagsys avait aussi en 2002 remporté l'appel d'offres de la bibliothèque de Seattle pour équiper ses quatre millions d'ouvrages. L'objectif premier est de faciliter les inventaires au moyen de lecteurs RFID portables. Le système permet également d'automatiser la gestion des prêts. L'emprunteur dépose ses livres près d'une borne RFID qui va identifier les ouvrages, alimenter la base de données centrale et désactiver la fonction antivol. L'opération automatisée est identique pour les retours.
Toujours autour des livres, c'est la plus grande chaîne de librairies hollandaises, BGN (avec 42 magasins et jusqu'à 40.000 livres vendus chaque jour), qui investit dans la radio fréquence en lançant une expérience pilote[60].

Aux Etats-Unis, les grands détaillants, dont Wal-Mart (chaîne américaine de grands magasins), s'intéressent fortement à ces avancées. Un demi-millier de magasins de la chaîne s'est doté de cette technologie fin 2005[61]. Grâce à l'identification par radio fréquence, il est entre autre possible d'installer des **caisses libre service** ou de **faire l'inventaire en un tour de main**. Cette solution de traçabilité a vocation à optimiser la gestion des flux, des stocks et la mise à disposition des produits en magasins. La chaîne Britannique Marks & Spencer (M&S) équipera ainsi par exemple d'ici le printemps 2007, 122 boutiques pour améliorer la gestion des stocks de vêtements (confection masculine et féminine) et bénéficier d'un suivi précis en temps réel des achats[62].
Les besoins mis en avant par les entreprises sont donc là une réduction des erreurs d'inventaires, la limitation des contrefaçons, ainsi que l'optimisation de la sécurité des biens et des produits. Par exemple, les pertes financières liées à des inventaires

[58] www.fr.computermagazine.be 3/10/2006
[59] www.VNUnet.fr 09/06/2006
[60] www.zdnet.fr 11/10/2006
[61] www.canoe.com 14/10/2005
[62] www.zdnet.fr 14/11/2006

mal organisés et aux vols sont estimées à plus de 40 milliards de dollars par an[63]. Bref, **toujours ce même argument économique** pour nous faire avaler la pilule !

En fait, comme ce qui a pu se passer avec l'informatique qui au départ n'équipait que quelques secteurs (banques, recherche…) et qui s'est ensuite répandue, les « tags » pourraient se généraliser à bien d'autres domaines que ceux cités ici. Par exemple, les Etats-Unis, depuis 2005 imposent des passeports RFID, soutenus par le département d'Etat américain avec sa loi sur la sécurité aux frontières de 2002. Pour les ressortissants, ils ont du tous adopter cette technologie avant la fin octobre 2006.
Autre exemple, l'administration américaine a récemment imposé à l'industrie pharmaceutique, pour les médicaments les plus chers qui sont très souvent copiés, le recours aux possibilités de traçabilité de la RFID : en effet selon les chiffres, les E.U. seraient passés de 4 faux médicaments sur 10 en vente avant l'an 2000, à 22 faux pour 10 vrais actuellement[64].
Plus anecdotique mais tout aussi inquiétant, ce sont désormais les 95.000 arbres d'alignement (c'est-à-dire plantés sur des trottoirs) de Paris qui se sont vu implantés des puces RFID à 2cm de profondeur dans leur tronc. «Chaque arbre des rues parisiennes dispose de sa "carte d'identité informatique"» désormais, explique Oracle. Les agents municipaux sont équipés d'un terminal nomade permettant de lire les puces : ils mettent ainsi à jour des informations sur chaque arbre concernant sa date de plantation, ses arrosages, les maladies éventuellement diagnostiquées et les événements particuliers tels qu'un choc avec un voiture. On retrouve bien là certaines des conclusions déjà formulées (à Autrans) comme quoi l'Internet et la réduction nanométrique des capteurs sont en train de créer un environnement quotidien fortement technologique et surtout totalement invisible pour le citoyen.

Pour parler des peurs liées aux technologies RFID, elles peuvent être classées en 3 catégories :

- **risques liés au traçage des objets que nous utilisons**
    - Les RFID permettent d'envisager par exemple des achats sans présentation des articles à la caisse grâce à des sas de comptage automatisés. Bien sûr, cette fonctionnalité permet de fluidifier l'acte d'achat en supprimant les queues aux caisses. Mais reste toute la question du traçage des marchandises dans le panier du consommateur. En effet, les marqueurs permettent le profiling des consommateurs à leur insu. On peut imaginer de corréler leurs achats avec une fiche d'identité, comme par exemple une carte de fidélité, pour établir des profils de consommateurs.

- **risques liés à notre traçage individuel**
    - Les marqueurs RFID peuvent permettre le suivi des patients souffrant de la maladie d'Alzheimer ou des personnes âgées. Un projet américain va même beaucoup plus loin en proposant d'injecter un identifiant de dossier médical à tous les citoyens américains. Son soi-disant objectif : ne pas donner des traitements contre indiqués ou incompatibles aux accidentés de la route inconscients. Cette mesure extrêmement intrusive semble intéresser les producteurs de RFID qui

[63] http://solutions.journaldunet.com 14/10/2005
[64] www.lemondeinformatique.fr 20/06/2006

développent une offre d'étiquettes « implantables ». Effrayant… Le traçage individuel n'est plus un concept vidé de sens puisque, au départ, les pays Occidentaux, tirés par les Etats-Unis imposent déjà passeports ou cartes d'identité biométrique. Ainsi comme on l'a vu, la puce, lisible par onde radio et donc sans contact, permet un contrôle d'identité en tout milieu et au travers de tout support (autre que métallique) à l'insu de son titulaire. Alors qu'actuellement les contrôles d'identité ne peuvent être effectués que moyennant le respect de certaines conditions, on aboutit avec la puce RFID à une banalisation complète de ce genre de contrôle ! Par ailleurs, puisqu'il y a émission d'ondes radio, il existe des risques de lecture indue et d'interception des données, au détriment du droit au respect de la vie privée et à la protection des données à caractère personnel.

- **risques liés aux échanges invisibles entre machines**
    - On se rappelle les « Terminator » joués par Arnold Schwarzenegger où les machines prennent le contrôle de la planète et sont sur le point d'anéantir la race humaine. Dans la réalité, le champ de bataille des militaires du 21ème siècle, avec satellites électromagnétiques ou autres de renseignement et de télécommunication, est quasiment déjà numérisé. Les militaires sont et seront de plus en plus derrière les écrans, confiant à des « robots guerriers » le soin d'appliquer leurs décisions au point que « l'intervention humaine » dans la décision de faire feu sera peut être considérée comme une perte de temps[65]…

Voici un lien Internet sur « You Tube » (la vidéo est appelé « The Catalogue »), à voir absolument pour se donner une idée de ces « anticipations » qui n'en sont déjà presque plus :
http://www.youtube.com/watch?v=zLztxjz4cWk

Autre exemple typique de cette ère du « tout technologique », Nike et Machintosh ont récemment sorti le Nike+iPod Sport Kit qui consiste en un capteur sans fil s'installant dans les chaussures de course Nike et d'un petit récepteur qui se connecte à un iPod Nano. Ce systême permet de suivre la vitesse, la distance et les calories brûlées. Mais ce n'est pas tout : la puce RFID du soulier émet jusqu'à une distance de 20 mètres. Du coup une équipe de l'Université de Washington a tenté empiriquement de réaliser un appareil de surveillance, pour un coût de 250$, en intégrant leur système d'espionnage à Google Maps. Et ça marche. Le transmetteur RFID diffusant un signal identificateur unique, les utilisateurs peuvent ainsi être surveillés. «La vraie signification de ce travail réside dans la facilité avec laquelle il a été accompli», a révélé Schneier, expert en sécurité. «À moins de faire passer une loi qui exigerait des compagnies qu'elles intègrent une forme de sécurité à ce genre de système, les compagnies continueront de produire des appareils qui érodent sans cesse notre vie privée par l'application de nouvelles technologies. Pas

[65] http://rewriting.net « Après la course au nucléaire, la guerre de l'information », novembre 2005

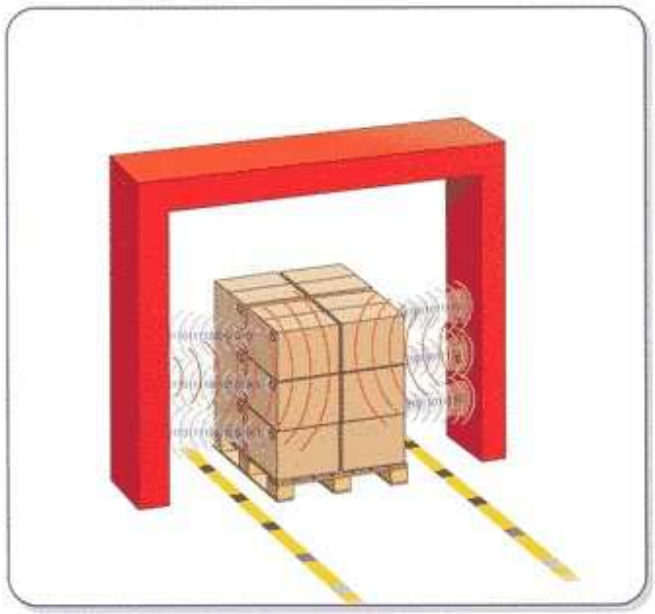
nécessairement à dessein ou par intention malveillante, mais juste parce qu'il est plus simple d'ignorer les facteurs externes que de s'en préoccuper.»[66]

D'une étude effectuée par la Commission européenne, il apparaît effectivement que la peur du non-respect de la vie privée constitue un véritable obstacle à l'introduction de la technologie RFID. Selon la commissaire européenne Viviane Reding, les citoyens doivent recevoir la garantie que le balisage d'éléments comme les cartes d'identité ne débouchera pas sur une surveillance automatique à grande échelle. Il suffit de penser à un scénario prévoyant que les cartes d'identité soient munies d'une puce RFID. Si un jour, les autorités décident d'équiper l'éclairage public de scanners RFID, il leur serait possible de savoir assez précisément où se trouvent les citoyens et à quel moment… Les participants à l'étude ont répondu en majorité qu'ils voulaient eux-mêmes exercer un contrôle final sur l'utilisation de la RFID : selon eux, les citoyens doivent avoir la possibilité de détruire les balises RFID s'ils le veulent. Mais dans ce cas, pourquoi vouloir alors les diffuser si largement. Viviane Reding s'attend à des propositions de loi en 2007[67]…
En Belgique, deux universitaires de référence en matière de sécurité (dont l'un se classe sans fausse modestie parmi les inventeurs de la carte à puce) se sont élevés pour **proposer un moratoire sur l'utilisation de la nouvelle génération de passeports électroniques** équipés de RFID. Ils affirment eux aussi que ces passeports dotés d'une puce, au lieu d'améliorer la protection des personnes, introduisent de nouveaux risques sécuritaires car, bien que les données soient cryptées, le cryptage reste fixe aux différents postes de contrôle et permet ainsi facilement de suivre à la trace un individu, même sans avoir à déchiffrer les données de la puce[68].

Et pour faire accepter la technologie RFID dans l'usage quotidien, il n'y a pas de doutes sur le fait que les entreprises essaieront par tous les moyens de la faire adopter en employant une rhétorique qu'elles sont en train de roder. Déjà, IBM fait la démonstration d'un « Clipped Tag », étiquette RFID pouvant être partiellement désactivé par le consommateur. Le principe : réduire la portée des transmissions émises par la puce en ôtant une partie de l'antenne. Le « tag » ne reste ainsi

[66] www.canoe.com 14/12/2006
[67] www.fr.datanews.be 17/10/2006
[68] www.fr.datanews.be 24/11/2006

exploitable qu'à condition d'être présenté directement devant un proche lecteur[69]. Pourtant ne nous y trompons pas : une fois le processus engagé et « toléré » par la population, **il sera très difficile de revenir en arrière**. Or, **aucun argument ne devrait justifier cette technologie** qui, vous l'avez compris, mettrait très rapidement à mal nos libertés individuelles.



Source : GS1 France

[69] www.lemondeinformatique.fr 02/05/2006

3 – Une « toile » sans fin

«Oh simple things, where have you gone? »

Keane, «Somewhere only we know»

3-1 Comment les citoyens tissent eux même leur propre enfer

« Il y a un monde ailleurs »
Jean Louis Aubert

Au nom de la productivité, crise aidant, plus rien n'est laissé au hasard. Il faut optimiser tous les processus, quels qu'ils soient. Là encore l'économie est le fer de lance pour cette nouvelle quête. Or, les plus gros gains de productivité se font aujourd'hui par les TIC, à la fois dans les entreprises et les administrations.
Lancée en 2004 par le gouvernement Raffarin en France, l'administration électronique, dénommée « Adèle » vise à simplifier « les échanges électroniques entre usagers et autorités administratives et entre les autorités administratives » résume Jean François Copé, Ministre délégué au Budget et à la Réforme de l'Etat du gouvernement De Villepin. Par exemple saisine d'une administration, accusé de réception, confirmation que la demande de l'usager est bien prise en compte : toutes ces procédures, effectuées par courrier jusque là, pourront désormais être réalisées en ligne[70] et par email. De la même manière les administrations pourront utiliser la signature électronique pour les documents transmis en ligne.
Une des idées derrière tout cela est d'alléger considérablement les effectifs, notamment du personnel chargé de la saisie, puisque maintenant tout se fait en ligne et que ce sont les personnes concernées elles-mêmes qui rentrent leurs informations. Ainsi le changement d'adresse d'un particulier se fait désormais on-line, ainsi que la demande d'acte de naissance ou les demandes de subvention pour les associations. Là encore, bases de données et connexion généralisée font craindre des dérives.
Mais le ministre délégué va plus loin en proposant la création « d'un espace de stockage personnalisé accessible en ligne » à partir duquel l'usager pourra communiquer avec les administrations et conserver les informations et documents nécessaires à ses démarches. Autrement dit, à partir d'un identifiant unique, on va pouvoir accéder à tous les dossiers administratifs d'une personne, là où avant chaque information était disséminée. Cette « innovation » est expérimentée depuis début 2006 auprès d'un panel de 500 personnes et ce pendant un an avant que les autorités en tirent un bilan.
Le travail des services de renseignement du pays sera donc extrêmement facilité (rappelons cependant qu'en France, contrairement au monde Anglo-Saxon, leurs effectifs sont encore très réduits). S'ils désirent tout connaître de quelqu'un, plus qu'ils n'en savaient déjà, rien de plus facile... et en prime, ô comble de l'ironie, **c'est la personne ainsi suspectée qui aura fait en grande partie le travail de saisie de ses antécédents** (administratifs). Quant à autoriser un jour le particulier de fouiner dans la vie de son voisin pour vérifier qu'il rentre bien « dans les normes »…

[70] www.01net.com 08/12/2005

Mais si on a vu que la productivité et le côté « pratique », érigés en fondement de nos sociétés, incitaient la population à émettre des informations à caractère personnel sur le réseau, c'était sans compter toutes les innovations technologiques qui l'incitent ainsi à se dévoiler jusque dans son intimité. Intimité dès lors gérée par des firmes du privé. Par exemple, fin 2005 le lancement de Google Base, procède ainsi de cette logique : inciter les internautes à lui **apporter du contenu** et de le gérer – comme avec Google Vidéo. Ce service est en effet conçu pour héberger et ouvrir à la recherche « tous types de contenus on-line et off line ». Les internautes peuvent publier leur contenu sur Google Base, gratuitement, et charge pour eux de les classifier et de les décrire à l'aide de mots clés.
Plus généralement, c'est le phénomène **«** Internet 2.0 **»** ou « **Web 2.0** » qui est en jeu. De quoi s'agit-il ? C'est une petite révolution du monde Internet qui permet déjà **à n'importe quel Internaute de facilement publier, partager ou diffuser ce qu'il veut sur la toile, et ce sans aucune compétence technique**. Dans cet état d'esprit, certains, comme Edward Bilodeau[71] n'hésite pas à revisiter ce concept de web 2.0 avec une certaine ironie. En effet, dans cette nouvelle utilisation des technologies :
« - Les utilisateurs fournissent les données (qui deviennent la propriété du prestataire de service) ;
- Les utilisateurs fournissent les métadonnées (qui deviennent la propriété du prestataire de service) ;
- Les utilisateurs créent la valeur ajoutée (qui devient la propriété du prestataire de service) ;
- Les utilisateurs paient le prestataire de service pour avoir le droit d'utiliser et de manipuler la valeur ajoutée qu'ils ont contribué à créer. »

Les blogs, par exemple, participent de cette tendance, mais aussi les wikis, les média citoyens, les services de partages de photos, etc. Ainsi, là où il y avait encore un jeu de pouvoir entre des « techniciens » du web qui faisait payer leurs services pour créer un site web pour un client lambda, il faut bien voir que **demain tout le monde sera en capacité de diffuser toutes les informations qu'il souhaite sur le web, sans compétences particulières…** Dans un billet intitulé « Esclavage 2.0 : eux, nous et moi » [72] Karl Dubost fait part de son énervement : « Toutes les entreprises du Web 2.0 sont là pour faire du commerce, pour exploiter vos données personnelles afin de les faire fructifier, parfois même en vous faisant payer. Google se sert de votre contenu pour faire des revenus publicitaires, même si votre contenu est sous une licence d'utilisation non commerciale, etc. Il faut arrêter de prendre les gens pour des imbéciles. Utiliser les concepts de liberté, de créativité, de beaux sentiments, de communautés pour mieux vous abuser, pour mieux pomper tout ce qui fait de vous un consommateur bien identifié est une arnaque. »
En effet, les multinationales du web mettent tout en œuvre **pour que les internautes partagent un maximum de contenu sur la toile.** Bien sûr, leurs politiques marketing masquent leurs vrais intérêts commerciaux en déployant sans fin leurs arguments sur la soi-disant « liberté totale de communication » du web. Et ça marche : aux Etats-Unis, le web communautaire ou web 2.0 est devenu une réalité pour la moitié des Internautes américains, avec un trafic en hausse de 367% sur un an.

[71] http://www.coolweblog.com/bilodeau/archives/001641.html
[72] www.la-grange.net/2006/03/29.html

Tout le scénario de notre époque était fait comme si, en apparence, on pouvait tout étaler sur soi au grand jour et le partager avec les autres, en étant totalement libre de se dévoiler. Cette tendance a pris ses galons depuis une dizaine d'années avec les « psys » en tout genre qui nous ont conditionnés à tout leur raconter étant donné que la parole libère, ce qui est au demeurant probablement exact. Mais bien vite les magazines people et la télé réalité aidant, on s'est rendu compte qu'il fallait tout dire sur soi et à tout le monde, les TIC et autres blogs prenant ensuite le relais pour « mondialiser » son petit « soi ». La « personnalisation » en tout genre est la suite logique de cette auto-contemplation. Et le marché des TIC en tire son épingle du jeu. Par exemple mettre sa photo en signature dans les Mms que l'on envoie. Et les « machines » peuvent aider à aller encore plus loin : la société Dodgeball vous envoie automatiquement un SMS quand un ami, un ami d'ami, ou un béguin est dans un périmètre rapproché de votre localisation[73]. On dérive donc logiquement vers une personnalisation faite paradoxalement à l'insu de l'individu, car presque entièrement gérée par les ordinateurs.

Rien ne serait inquiétant jusque là si ce qu'on racontait sur sa petite vie n'était pas « enregistré » définitivement quelque part. **Ce système de « traces » est bien la plus grosse faiblesse d'Internet**, ce qui pourrait un jour le faire basculer « du côté obscur » si les défenseurs des libertés individuelles, nous, citoyens, n'y prenons garde. Le réseau conserve en effet une **mémoire quasi-parfaite** (contrairement aux psy) de tout ce qui s'y passe. Pour prendre un exemple sur le réseau Internet, et pour revenir à Google, imaginons qu'un webmaster quelconque (une association dont vous faites partie, dans votre entreprise...) publie sur le réseau une page web, avec quelque part dans le document votre nom qui apparaisse. Et bien lorsque vous taperez sous Google votre nom, vous serez sûr d'apparaître quelques jours plus tard dans les résultats du moteur. Mais le plus ahurissant c'est que, même si vous demandez la suppression de votre nom au webmaster en question et qu'il s'exécute, la page pourra bien ne plus exister « physiquement » sur le serveur, Google, dans ce qu'il appelle son « cache », en aura gardé une trace et pourra vous la ressortir lors de n'importe quelle interrogation du moteur !

Qu'est ce que le « cache » : Ce mot à été importé de l'anglais « cache memory ». Le mot mémoire tampon est plus approprié en français mais peu utilisé. La mémoire cache est une mémoire intermédiaire dans laquelle se trouvent stockées toutes les informations que le processeur central (d'un ordinateur) est le plus susceptible de demander. Elle sert donc à accélérer la communication entre un élément fournisseur (le disque dur par exemple) plus lent que l'élément demandeur (ex : processeur). Pour anecdote, la langue anglaise aurait emprunté au français canadien le mot « cache » (féminin) qui désigne la cachette où le trappeur entrepose des provisions ! Le cache de Google fonctionne donc sur le même principe. La version « en cache » des pages web proposée par Google correspond aux pages telles qu'elles se présentaient lors de la dernière consultation effectuée par le moteur californien. Donc même en cas de suppression de la page par un webmaster, Google gardera une mémoire de la page lors de sa dernière visite avant l'effacement.
La justice américaine a récemment donné raison à Google en estimant que les copies d'œuvres réalisées par le système de cache relevaient d'un « usage loyal » et n'enfreignait pas le copyright américain.

[73] www.atelier.fr , 30/09/2005

Pour l'instant, les grands moteurs de recherche n'offrent pas la possibilité d'effacer définitivement cette mémoire, à fortiori si elle vous concerne et peut vous porter préjudice. En viendront-ils à faire payer ce service. Ce serait un comble : payer pour que sa vie privée ne devienne pas publique !

A noter, pour les experts du web, il est possible d'exclure, a priori, c'est-à-dire dès sa conception, un site du cache de Google et des autres moteurs en utilisant des balises html appropriées.

3-2 Les avancées inquiétantes de la biométrie et le faux problème de l'identifiant unique

« Dans les villes de l'an 2000,
La vie sera bien plus facile,
On aura tous un numéro dans le dos,
Et une étoile sur la peau,
On suivra gaiement le troupeau »

Monopolis, Opéra Rock Starmania

Qu'est ce donc exactement que ce concept de **biométrie** ? Il s'agit en fait d'un moyen d'authentification, comme l'est par exemple votre mot de passe lorsque vous allumez votre ordinateur, ou encore plus simplement votre code secret pour votre carte bancaire. Mais ce n'est pas n'importe quel moyen : il s'agit ni plus ni moins que de **recourir à une partie de votre corps humain pour vous authentifier**. Sur le marché les technologies les plus répandues sont les empreintes digitales (48% du marché), la morphologie faciale (12%), la géométrie de la main (11%), l'iris (9%), la reconnaissance vocale (6%), de la rétine, des veines et des oreilles ainsi que la radiographie dentaire. Et le secteur économique de la biométrie est en pleine croissance : il pourrait atteindre les 5 milliards de dollars d'ici 2008[74]. Personne ne s'y trompe d'ailleurs : des représentants du Département américain de la sécurité intérieure, du groupe IBM et de diverses agences de sécurité se sont regroupés fin 2005 au sein de l'International Biometric Advisory Concil (IBAC). Ils comptent intervenir en coopération avec d'autres organisations comme le Forum Européen sur la biométrie pour établir des standards internationaux en la matière.

L'entreprise japonaise Oki Electric a récemment développé une technologie baptisée FSE, pour Face Sensing Engine (Moteur de reconnaissance du visage) pour téléphone portable. Celle-ci peut être utilisée pour restreindre l'accès aux données stockées sur un téléphone mobile pourvu d'un appareil photo numérique. Le système peut identifier son propriétaire en étudiant la photo courante de son visage, et en la comparant avec des caractéristiques déjà extraites et présentes en mémoire. La technologie emploierait notamment la localisation relative des yeux, des sourcils et de la bouche pour reconnaître un visage. Le système pourrait également s'adapter automatiquement aux changements d'éclairage et aux différentes expressions qui modifient le visage.

La Colombie est l'un des quelques endroits dans le monde où les banques ont adopté un système de vérification biométrique de l'identité. La personne est identifiée au moyen de ses caractéristiques physiques particulières, notamment par les

[74] http://solutions.journaldunet.com 20/05/2005

empreintes digitales ou l'iris de l'œil.[75] Même son de cloche au Japon où certaines banques ont mis en circulation une nouvelle carte de retrait équipée d'une puce sur laquelle est enregistrée sous forme cryptée une image des veines de la main de son propriétaire. « Lors d'une transaction, le client approche la main d'un lecteur lié au distributeur qui scanne, sans contact, son réseau vasculaire. La puce effectue la comparaison entre les données capturées à cet instant et celles qui ont été préenregistrées avant d'autoriser ou non l'opération », explique un porte parole de la banque[76].

« La biométrie rendra le corps humain lisible par la machine (…) et les informations biométriques pourront être utilisées en tant qu'identificateur unique universel ». La prévision est alarmante. Elle émane d'une quarantaine de commissaires à la protection des données et à la vie privée, dont la CNIL.
C'est ce même genre de protestations qui avaient, rappelons-le, en France, aboutit à la loi du 6 janvier 1978 dite loi « Informatique et Libertés » lorsqu'à l'époque le gouvernement avait annoncé l'utilisation d'un numéro unique attribué à la naissance à chaque citoyen français afin de simplifier les relations des services publics avec leurs administrés. Non seulement le projet avait été abandonné, mais les défenseurs de la vie privée et des libertés individuelles avaient en plus exigé une loi pour prévenir des risques quant à l'utilisation de données personnelles dans les systèmes informatiques. Cette loi avait aussi abouti à la création de la Commission Nationale Informatique et Libertés, instance indépendante chargée de surveiller les évolutions dans ce domaine.
Pour l'ancien secrétaire général de la CNIL, Christophe Pallez quant à la réflexion sur la biométrie, il faut « éviter la mise en place d'un identifiant unique ». Car, selon lui, les implications de fichage inhérentes à l'intégration de données biométriques sur une carte à puce « pourraient avoir un jour des aboutissements redoutables »[77].
Mais selon Jacques Henno[78], la technologie a même dépassée la fiction. **Les ordinateurs et les systèmes de gestion de bases de données sont désormais assez puissants pour se passer d'un identifiant unique.** Quelques paramètres (nom, adresse, date de naissance, numéro de carte bancaire…) leur suffisent pour s'assurer que les renseignements qu'ils ont récupérés à droite ou à gauche concernent la même personne. Plus besoin du numéro de sécurité sociale pour accumuler des informations sur chacun d'entre-nous. Malheureusement le sujet est très peu médiatisé, ou s'il l'est, ne fait montre que d'un débat technique de spécialistes ou encore fait office de véritable « progrès ».

En outre, on pourrait penser que le fait que les bases de données soient encore aujourd'hui éparpillées au 4 coins du monde et sans encore trop de relations entre elles nous offre une tranquillité totale. Cependant, c'était sans compter la toute puissance des innovations informatique puisque, déjà, des *data mediations systems*

[75] www.canoe.com du 13/10/2005
[76] www.laviedunet.be 17/05/2005
[77] Pourtant, la CNIL facilite l'adoption de la biométrie en France. En effet, depuis le 27 avril 2006, elle a opté pour trois autorisations pour simplifier les formalités de certains dispositifs biométrique : tout d'abord l'identification par le contour de la main pour le contrôle d'accès, la gestion des horaires et l'entrée à un restaurant d'entreprise ; l'empreinte digitale réservée exclusivement au contrôle d'accès au lieu de travail et enregistrée sur un support individuel ; et enfin, le cas particulier, qui implique des mineurs, du contour de la main pour l'accès au restaurant scolaire. Dans ces trois cas de figure, il est possible de faire une simple déclaration en ligne à la Cnil. (source : www.01net.com du 22/05/2006)
[78] Tous fichés (Jacques Henno)

(systèmes de médiation de données) commencent à voir le jour : en clair, à partir d'un seul ordinateur on pourra interroger des bases de données hétérogènes et dispersées géographiquement, en ayant l'impression de n'en interroger qu'une seule, le système étant totalement transparent pour l'utilisateur. C'était pourtant ce qui garantissait jusqu'alors un quasi-anonymat à chacun.

Alain Weber, de la LDH, reste lui aussi très critique sur la biométrie qui ne permettra pas selon lui d'enrayer les causes auxquelles elle s'attaque : « Les prétextes sont divers. Combattre le terrorisme ? La biométrie n'aura aucune influence directe sur la lutte contre ce fléau. Traquer les faux papiers. Celui qui se présentera à la frontière avec un visa biométrique associé à un faux état civil passera aisément tout contrôle. Les arguments en faveur de la biométrie ne tiennent pas la route… Empêchons nos ministres d'être des apprentis sorciers ! »[79]
Jean-René Lecerf, Sénateur UMP du Nord et auteur du rapport de la mission d'information sur la fraude documentaire, dans le même article, expose clairement son point de vue « pour » face à cette technologie : en effet, « le système actuel est une passoire » et « à l'heure actuelle, la biométrie est la seule technologie permettant l'identification de millions de personnes, dissuadant les velléités d'usurpation. » Et les arguments économiques sont toujours parmi les plus présents « La France a accumulé un retard significatif en matière de biométrie… Triste constat qui fait aujourd'hui de l'hexagone un élève moyen de la classe européenne alors que les entreprises françaises spécialisées dans les applications biométriques comptent parmi les plus compétentes… ».
Quand l'économie devient une fin, et l'homme son moyen…

3.3 La signature électronique et la traçabilité parfaite : la fin du « hasard »

« Les hommes n'ont jamais l'air si heureux que le jour où ils abdiquent leur liberté »

Charles Nodier

Voici une petite anecdote qui s'est déroulée il y a peu de temps lors d'un déjeuner au restaurant. Nous observions depuis nos places respectives les serveurs naviguer d'une table à l'autre, et aller à la caisse enregistreuse, dans une ronde permanente. En essayant de comprendre un peu plus leurs faits et gestes, nous avons remarqué qu'ils disposaient chacun d'une sorte de « clé » qu'ils utilisaient chaque fois qu'ils faisaient une opération à la caisse. A chaque moment qu'ils encaissaient une commande, ils inséraient leur « clé » individuelle dans un endroit spécifique situé sur la caisse. Celle-ci les reconnaissait automatiquement, leur nom et prénom s'affichant sur le petit écran de contrôle, et ce n'est qu'à partir de ce moment qu'ils pouvaient « rentrer » les plats commandés par leurs clients et leur établir leur note. Cette technologie existe depuis très longtemps chez les restaurateurs et a été assez récemment améliorée par des carnets de commande électronique qui permettent au serveur lorsque les clients ont choisi leurs plats d'envoyer toutes ces informations directement en cuisine.
Bien sûr, cette technique attire de plus en plus de petits commerçants (et est

[79] www.lexpress.fr , 05/09/2005

quasiment systématique dans les grandes enseignes et franchises) qui veulent surveiller les performances de leurs vendeuses : on sait tout sur elles, depuis leur panier moyen jusqu'au chiffre journalier ou mensuel qu'elles ont généré. Ainsi elles ne peuvent plus « tricher » ou faire semblant : les chiffres sont là pour témoigner de leur résultat.

Pour étendre cette façon de travailler qui prend irrémédiablement du galon de nos jours dans beaucoup de secteurs économique, une start-up française, CertiMail commercialise aujourd'hui par exemple une clé USB pour certifier les emails[80] (et leurs pièces jointes) et pour vulgariser l'usage de la signature électronique. Cette pièce dématérialisée peut servir de preuve recevable devant la justice française en cas de litige.

Si l'obsession sécuritaire continuait de se propager sur la planète (le marché français des solutions de sécurité a crû de 17% en 2005[81]), ce système de « clé » (qui pourra selon la tendance se faire à distance, sans liaison physique, comme avec le Wifi ou Bluetooth) pourrait se généraliser. Ainsi cette clé, qui pourrait bien dans un futur proche être remplacée par la simple empreinte biométrique, permettra d'accéder à tous les espaces de nos vies quotidiennes : ouvrir une session sur son ordinateur, personnel et professionnel ou même d'un cybercafé, prendre les transports en commun, accéder à des locaux, payer, démarrer sa voiture… Les applications sont en fait infinies.
Certes, les arguments « pour » seront nombreux : les politiques pourront dire aux citoyens aveuglés : « Puisque vous n'avez rien à vous reprocher, servez-vous librement de votre clé ou de votre empreinte digitale. Elle est simplement là pour empêcher tout acte frauduleux ou terroriste». Le côté « pratique » séduira aussi énormément le public : plus besoin de clé, plus besoin de mots de passe, plus besoin de carte bancaire…c'est la liberté totale !!!

Pourtant ne soyez pas dupes de ce simulacre de liberté : votre parcours quotidien sera pisté au millimètre près et de manière totalement invisible pour vous. La signature électronique ne se bornera pas simplement aux actes importants, qui se font aujourd'hui encore par signature manuelle. Elle interviendra dans le moindre recoin de nos vies, nous empêchant de dire : « Non, là ce n'était pas moi ». **La preuve électronique, à priori infalsifiable, nous empêchera tout comportement déviant**, c'est-à-dire toute originalité et toute créativité, tout ce qui fait l'homme dans son essence.
Et même s'il était possible de réaliser une quelconque imitation (voir plus loin l'exemple des vraies fausses empreintes digitales imaginées par des chercheurs japonais), ceci pourrait avoir des conséquences catastrophiques. « Une personne pourrait se retrouver fichée par erreur et être interdite d'accès, par exemple à un aéroport ou au réseau Internet. Et à qui incombera la charge de la preuve de l'identité ? Celle-ci risque fort de reposer sur le citoyen lui-même ! Or prouver qu'on est bien la personne que l'on prétend être est une tâche difficile – voire impossible – surtout dans une société où l'identité d'un citoyen est de plus en plus définie par des paramètres émanant du gouvernement (permis de conduire, carte d'assurance maladie, acte de naissance…) »[82] .

[80] www.VNUnet.fr 02/05/2006
[81] www.lemondeinformatique.fr 29/11/2005
[82] Communiqué de l'AEDH (Association Européenne pour la défense des droits de l'Homme) du 29/11/2005

D'ailleurs, la profession de notaire, l'autorité en France pour certifier les actes subit depuis plusieurs mois une profonde restructuration dans sa manière de travailler : la signature électronique constitue une étape importante pour le métier et débouchera sur la possibilités de rédiger des actes juridiques dématérialisés. La carte Real est déjà apparue avec, en accord avec les directives du Conseil supérieur du Notariat, la possibilité de signature électronique entre notaires, garantissant leurs identités respectives et l'intégrité du contenu de leurs échanges. Tout cela pour gagner en vitesse et traiter les dossiers des clients plus rapidement.

La tendance dans un futur proche apparaît déjà : tous les fichiers (et la virtualisation du monde fait que **tout est en train de devenir fichier : email, photos, vidéos, conversations téléphoniques, mouvements bancaires…**) envoyés sur le réseau par un individu seront peut être un jour systématiquement « signés » (à terme biométriquement) par ce dernier qui deviendra le responsable du moindre détail de sa vie quotidienne. En tous les cas, les états commencent à ratifier entre eux des traités pouvant aboutir à utiliser toutes ces preuves « virtuelles » au nom de la lutte contre les délits sur le web. Fin 2006, les Etats-Unis ont été le 16ème pays à adopter la convention internationale sur la cyber criminalité. Le texte appelle ses membres à partager et échanger leurs données électroniques. Tous ceux qui l'ont ratifié et définitivement adopté, dont la France en début d'année, s'engagent à collaborer lors des enquêtes afin de poursuivre les auteurs des crimes. «La convention sur le cybercrime du Conseil de l'Europe est une approche de solution mondiale au problème également mondial de la criminalité informatique » a déclaré Sean McCormack, porte-parole du département d'État américain[83]…
Toujours aux Etats-Unis et dans le même esprit, pour se conformer à de nouvelles règles fédérales, les entreprises américaines devront faire le suivi de tous les courriels, messages instantanés et documents électroniques générés par leurs employés. Autrement dit, faire un **archivage numérique systématique** de tous les documents et communications produits **par chaque salarié** ! Approuvé par la Cour Suprême en avril 2006, ce changement souligne plus que jamais l'importance pour les compagnies de connaître la nature de leurs renseignements électroniques et d'en connaître la localisation. Ainsi avec la nouvelle réglementation, un employé des technologies de l'information qui, comme d'habitude, écrase avec des données fraîches les données présentes sur une copie de sauvegarde, pourrait être en train de commettre l'équivalent d'un **«déchiquetage virtuel»,** a expliqué Alvin F. Lindsay, associé au cabinet Hogan & Hartson LLP et spécialiste des litiges dans le domaine technologique[84].

[83] www.zdnet.fr 4/10/2006
[84] www.canoe.com 01/12/2006

Sélection PME express

Offres spéciales Petites et Moyennes Entreprises

IBM

Vous avez sous les yeux l'ordinateur le plus sécurisé du monde.

ibm.com

Et le moyen le plus simple de le déverrouiller.

Le portable le plus sécurisé.
Uniquement sur ThinkPad

Contactez votre revendeur IBM dès maintenant.

Pour connaître votre revendeur le plus proche, rendez-vous sur **bm.com**/pc/fr/promo ou appelez le 0810 333 810*

intel inside
centrino
MOBILE TECHNOLOGY

3-4 Toujours plus de sécurité pour moins de libertés : la fin de l'innocence

« Une société dans laquelle nous devrions tout savoir pour être en sécurité serait une société dans laquelle tout le monde serait potentiellement terroriste et où chacun devrait se méfier de son voisin. » [85]

> Jean Pierre Dubois, Président de la ligue des droits de l'homme (LDH) et professeur de droit constitutionnel à l'Université Paris XI

Avec la virtualisation de la vie quotidienne des citoyens de la planète, les délits, il ne faut pas le nier, se passeront de plus en plus sur la « toile ». D'après une étude auprès de 2000 sociétés américaines, rendu publique par le FBI début 2006, la cybercriminalité coûte déjà aujourd'hui en moyenne 24.000 dollars à une entreprise américaine, soit 67 milliards de dollars à l'échelle du pays.
Le gros problème avec Internet, c'est que si l'on commence à vouloir mettre en place des contrôles, la technique aidant, **la population suspecte de référence ne va pas être de quelques individus, mais de la totalité des Internautes.** Dans une déclaration récente, les responsables régionaux chargés de contrôler l'utilisation des données personnelles en Allemagne, se sont inquiétés du fait que le développement des aspects préventifs des politiques de sécurité «*conduit de plus en plus les autorités à traiter sans raison des citoyens intègres comme des suspects »*[86]*.*
Ne l'oublions pas, l'Internet utopique (dans sa perspective de matérialiser sur le réseau chaque individu et produit de la planète) marche aussi, comme l'informatique, en binaire. Les technologies de surveillance, si elles sont déployées à grande échelle sur le réseau, feront que soit on contrôle tout le monde, soit on ne contrôle personne. Il n'y a pas de nuance. Lorsque Internet deviendra « transparent » pour tous, c'est-à-dire en d'autres termes que chaque citoyen sera un Internaute de fait (peut être faudra t'il alors inventer un autre mot, car « internaute » est encore trop teinté de « web ») puisque l'ensemble de ses appareils communicants le traceront dans ses moindres faits et gestes, alors les enquêtes policières seront facilitées, voire même résolues de fait. En effet, la convergence des systèmes GPS, Web, et autres communications en tout genre rendront quasi-impossible tout dépassement de la norme et du cadre légal. Faut-il s'en réjouir ? Probablement pas en ce sens où l'on dériverait rapidement vers une parodie de la justice et vers un extrême ultra sécuritaire, où tout ce qui fait la richesse de l'homme dans toutes ses dimensions autres que purement matérielles et physiques, serait tout simplement nié.

Il faut bien voir que ce qui se profile déjà, c'est **que la majorité des délits** ne sera plus de faire un crime, mais **d'être susceptible de commettre une infraction**. Les systèmes informatiques vont essayer de plus en plus de prévoir, d'anticiper les méfaits. A vouloir tout quantifier, on donnera probablement des notes de dangerosité au individus, pouvant changer au fil du temps, suivant l'évolution de leur « vie privée ». En fait, **la présomption d'innocence est belle et bien en train de**

[85] www.nouvelobs.com 26/10/2005
[86] www.01net.com 17/11/06

disparaître, au profit de la présomption de culpabilité. Les terroristes, puisque c'est l'argument presque toujours avancé, sont tellement bien fondus dans la population, qu'il faut désormais à l'Etat des moyens plus subtils de recherche et d'intervention : il est **plus facile de présumer tout le monde coupable et de faire ouvertement des recherches dans nos vies privées** (et l'outil Internet rendra cela très facile), **plutôt que d'utiliser la présomption d'innocence et s'empêcher ainsi des recherches fructueuses.** Nous sommes dans une ère de pragmatisme : tous les moyens, **quels qu'ils soient,** sont bons pour arriver au but.

C'est dans cet esprit là que Norwich Union (une société d'assurance) propose à ses clients anglais d'installer une boite noire dans leur véhicule afin de relever leurs habitudes de conduite. En échange, ils peuvent espérer des baisses de prix sur leur assurance auto. Ce contrat est baptisé « pay as you drive » (payer comme vous conduisez). Le « mouchard », relié à divers capteur de l'automobile et doté d'un module GPS, enregistre les informations liées aux déplacements effectués (plages horaires, distance, positionnement), ainsi que certaines données sur les comportements de conduite (comme la vitesse). Ces données sont ensuite régulièrement transmises à l'assureur via une communication par réseau cellulaire. Celui-ci peut alors moduler chaque mois le montant de l'abonnement de l'assuré en fonction du kilométrage, du type de parcours (ville, autoroute, zone statistiquement dangereuse ou non…) ou du respect des limitations de vitesse par exemple[87]. Le business des assurances est donc en train de changer de modèle : d'un contrat supposant la bonne conduite de l'assuré sur le long terme, on passe à une convention le jugeant en permanence susceptible de commettre une infraction. Ce qui pourrait apparaître au premier abord comme une « nuance » entre les 2 modèles, est, en y regardant de plus près, un véritable fossé puisque la notion de **confiance est en train de disparaître**. D'ailleurs, même s'ils ne passent pas par Norwich Union, les automobilistes anglais sont aussi depuis peu sous surveillance resserrée[88]. Grâce à l'informatique, les voitures de polices dûment équipées alertent les officiers dès qu'ils croisent un automobiliste sans permis, sans assurance ou sans vignette. Ce qui trahit le suspect : sa plaque d'immatriculation scannée et identifiée en quelques instants par base de données interposée recensant 28 millions de véhicules « fichés » (dont 1,1 millions sont susceptibles de déclencher une alerte) et grâce à une caméra embarquée dans la voiture de Police. Lorsqu'une plaque est photographiée, l'ordinateur enregistre également la date, l'heure, la géolocalisation (par GPS) du véhicule, ainsi qu'une petite photo du conducteur et tout cela conservé pour une durée de 2 ans. Certes la fraude à diminué , mais quelle régression pour les libertés individuelles !
Et la France s'apprête à importer le système. La loi contre le terrorisme du 23 janvier 2006 a ouvert une brèche dans laquelle le ministère de l'Intérieur s'est engagé : les derniers obstacles juridiques devraient être levés, et les premières patrouilles équipées devraient voir le jour courant 2007. On peut par ailleurs, suite à notre développement antérieur sur la technologie RFID imaginer sans trop se tromper comment les « machines » vont à venir à gérer « naturellement », comme pour ce cas-ci, les façons de faire des humains.
Les Emirats arabes unis sont passés à une étape encore supérieure en mettant en place un système de **verbalisation automatique** en cas de dépassement de la vitesse autorisée. En cas de dépassement de la limite, le conducteur est averti par

[87] www.01net.com 31/05/2005
[88] www.01net.com 24/11/2006

un message vocal. S'il ne ralentit pas, le boîtier transmet les informations d'identité, de localisation et la vitesse du véhicule directement à la police. Le boîtier aura de bonnes raisons pour se faire adopter largement : entre autre la localisation par les services d'urgence, le calcul des contrats d'assurance (favorable aux bons conducteurs) ou encore comme moyen d'antivol. « Bonnes raisons » qui, au nom du progrès technique, laissent de plus en plus le pouvoir aux machines et sont en train de dénaturer le lien de confiance entre les hommes. D'ailleurs, le fait est que dans le monde du sport les ordinateurs commencent déjà à décider à la place des hommes. Lors de la Coupe du Monde 2006 de football et du fameux coup de tête de « zizou », un quasi-consensus a émergé quant à la mise en place systématique de caméras permettant de « juger » en quelque sorte à la place de l'arbitre du match. « Avancées » encore plus surprenantes lors du tournoi de tennis de Bercy 2006 où désormais le joueur qui soupçonne une erreur d'arbitrage en sa défaveur peut demander à l'arbitre (ou du moins ce qu'il en reste) de vérifier sur les ordinateurs, équipés de puissant logiciels, la trajectoire exact de la balle.

Dans un domaine qui touche le cœur de nos régimes politiques Occidentaux, des experts se sont en effet exprimés pour mettre en garde contre le déclin démocratique que pourrait représenter le déploiement prématuré de « machines à voter ». Quelque 1200 machines équipent déjà plus de 800 bureaux de vote dans une cinquantaine de villes françaises comme Brest ou Le Havre, et ces chiffres doubleront probablement en 2007. La fin des fameux dépouillements réalisés manuellement par des citoyens volontaires dans tous les bureaux de vote du pays, pourtant ciment de nos démocraties, aboutit là aussi à une dégénérescence des liens de confiance entre les hommes. Gain de temps oblige, la machine prend tout pouvoir. Chantal Enguehard, maître de conférences en informatique au LINA et auteur d'un rapport[89] sur le sujet note qu' «à aucun moment l'électeur ne peut vérifier que son vote a été effectivement bien noté [...] ni participer au dépouillement puisque l'ordinateur le réalise en toute opacité sans qu'il soit possible de vérifier ses résultats.» La fondation néerlandaise "Nous ne faisons pas confiance aux machines à voter" a publié aussi un rapport[90] qui détaille comment des personnes peuvent prendre, avant les élections, le contrôle à distance d'une machine à voter de la société Nepad (agréée en France) et modifier le résultat du scrutin. «Compromettre le système nécessite seulement de remplacer un simple composant de la taille d'un timbre-poste et s'avère impossible à détecter», écrivent les auteurs[91]. Et ce type de système est en fait appelé à se développer aussi pour les entreprises, les institutions et les syndicats. Vivendi, Lafarge ou France Telecom par exemple ont déjà adapté leurs statuts pour permettre le vote électronique[92] de leurs salariés.

Par ailleurs, afin de lutter contre les soi-disant menaces de « méchants pirates » qui font courir des risques au réseau Internet et à nos « libertés », la Liberty Alliance est chargée d'élaborer des spécifications techniques communes pour les applications de services web, et en particulier pour les services d'authentification en ligne. Ce consortium, fondé en 2001, comporte parmi ses membres des groupes comme AOL,

[89] "Le vote électronique en France: opaque & invérifiable", Chantal Enguehard du laboratoire informatique de Nantes Atlantique, juillet 2006
(http://www.sciences.univ-nantes.fr/info/perso/permanents/enguehard/perso/RI_halshs-00085041.pdf)

[90] "Voting computer: a security analysis", Rop Gonggrijp, Willem-Jan Hengeveld, etc., octobre 2006
(http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf)

[91] www.zdnet.fr 18/10/2006

[92] www.zdnet.fr 8/12/2006

Intel, American Express, HP, Vodaphone, mais aussi Nokia, France Telecom, Sony, et environ 140 autres entreprises ou organisations figurent parmi ses sponsors, partenaires ou associés.
Considérant que les services d'authentification en ligne ne sont plus suffisamment sécurisés par le couple identifiant/mot de passe classique, le consortium international va mettre en place des standards pour le développement d'une seconde couche de sécurisation. Celle-ci pourra être une carte à puce contenant des données biométriques, des certificats logiciels ou matériels ou encore un système qui passe par les téléphones mobiles. Ces 2 « couches » s'appellent dans le jargon la « strong authenfication ». Michael Barrett, Vice Président en charge de la sécurité chez American Express souligne en effet que « l'absence de seconde authentification sur les espaces en ligne est l'une des causes les plus significatives de vol d'identité ». Même recommandation pour la FFIEC (Conseil fédéral américain des institutions financières) qui reconnaît que les mots de passe sont désormais insuffisants comme seul moyen d'authentification en ligne.
Là encore, sur un sujet qu'on nous fait uniquement passer pour technique, mais qui est en réalité avant tout éthique, les citoyens ne sont jamais consultés. Pourtant ce sont bien eux qui vont devoir prouver à deux fois leur identité. Et même paradoxalement prouver deux fois leur degré de culpabilité, puisque tout le monde sera présumé coupable et que tout devra être signé biométriquement sur le réseau. D'où l'impossibilité de nier. On fera, puisqu'elles se basent sur des données signées et donc réelles, **une confiance totale aux preuves que nous fournira le réseau**, grâce à sa mémoire infaillible et absolu. Et peu importe ce que l'accusé répondra : sa mémoire, après tout, n'est qu'humaine…

Déjà, à cause d'intrusions réalisées **en interne** (qui représente quand même 44% des cas d'intrusions au total), les directeurs informatiques aux Etats-Unis[93], pour enrayer le phénomène que n'arrive pas à résoudre la panoplie des outils classiques (pourtant équipés à 98,2% d'antivirus, 90,7% d'un pare-feu, et à 75% d'une solution globale contre le code malveillant : anti-spyware, anti-phishing…) en viennent à **étudier la solution extrême, c'est-à-dire celle de remonter à la source absolue, l'individu lui-même**. Ainsi, dans les entreprises américaines, déjà 4% des directeurs informatiques ont opté pour la biométrie, et 7% pour des cartes magnétiques.

3-5 Exemple d'outils au service du contrôle

« Personne ne devra se rendre compte qu'il est surveillé par des ordinateurs »
Jeffrey Ullman, spécialiste du Data mining

On peut légitimement se poser la question : mais comment pourrait-t-on me contrôler puisque mes appareils communicants et moi-même laissons des traces au milieu de millions d'autres ? Je suis noyé dans une information mondiale et je vois bien mal comment je pourrais attirer l'attention.

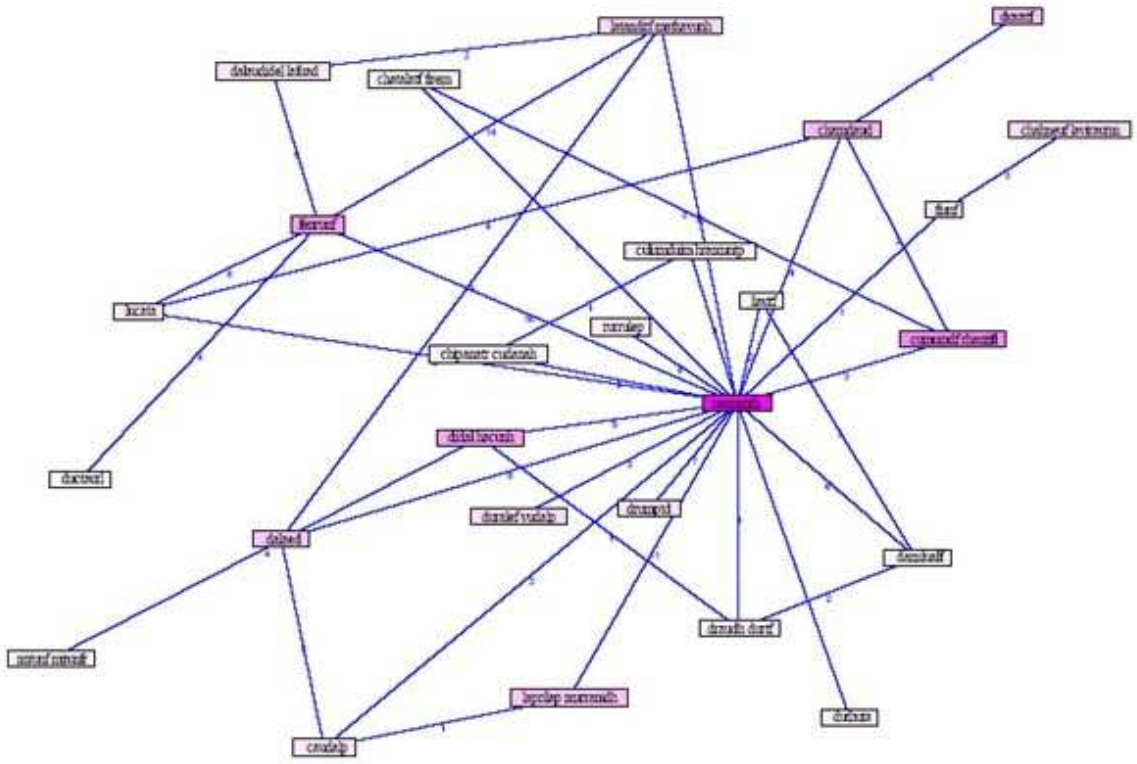
Ces remarques pouvaient dans l'informatique d'hier rester valables, car certes si des traces sont produites sur le réseau, ce ne sont que des suites de données brutes et de tableaux de chiffres, qui sont exploitables au cas par cas dans des enquêtes par exemple, mais qui ne peuvent pas donner une vue d'ensemble.

[93] Dans une étude menée par le FBI sur 2000 sociétés américaine en 2005-2006

C'était sans compter les progrès fait dans le domaine du « data-mining » et qui a donné naissance dans ces toutes dernières années au « link analysis ».
L'analyse de tableaux croisés est aujourd'hui la principale méthode pour identifier les associations entre des variables contenues dans une base de données. Lorsque le nombre de modalités est très important, cette méthode est inadaptée. Il est difficile en effet d'analyser des tableaux comportant plusieurs milliers de lignes et de colonnes. Ces logiciels permettent donc d'**extraire** de grandes bases de données des **liens de cause à effet dont on ne soupçonnait pas jusqu'alors l'existence**. Au départ, on sait ce que l'on étudie (comportement d'achat, interactions entre médicaments, phénomène astrophysiques…) mais on ne sait pas exactement ce que l'on recherche. **C'est la machine qui va mettre en avant les corrélations les plus intéressantes**. Les enseignements tirés sont souvent spectaculaires : comportement des personnes qui fraude le fisc, de celles susceptibles de décéder d'un cancer de la prostate ou de celles intéressées par des réductions sur les vacances de neige.[94]

Ainsi, dès à présent, des outils **dotés le plus souvent d'interfaces graphiques très poussées et simplifiées** sont disponibles sur le marché pour pouvoir reconstruire par exemple les réseaux de communication entre différentes personnes et permettre par un moyen simple et visuel de représenter les relations entre toutes ces modalités.
Ainsi, à partir du dépôt de brevets, il est possible de reconstituer les équipes d'inventeurs. A partir de messages dans lesquels il y a un émetteur et un récepteur (comme des e-mails), on peut représenter le graphe des communications, etc.
C'est probablement de cette manière là qu'on été remontées les filières terroristes de l'attentat de la gare d'Attocha en Espagne. En effet, un téléphone portable devant déclencher une bombe a été minutieusement analysé. On n'a pas pu savoir le nom exact de son propriétaire[95], mais ceux de ses contacts qu'il a ou qui l'ont appelé dans les dernières semaines, ainsi que les contacts des contacts… et cela à l'infini.
Ce « réseau » est représenté dans le graphe ci-dessous. Il est possible de savoir également l'importance que les contacts ont entre eux, la liaison (le trait) entre eux changeant de longueur suivant la « densité » des contacts. Par exemple, la distance entre 2 modalités sera d'1cm pour plus de 10 coups de fil par semaine, 5cm pour moins de 2…etc. Ainsi plus deux individus sont proches sur le graphe, plus ils entretiennent de communications avec leurs portables entre eux.

[94] Tous fichés (Jacques Henno)
[95] en effet, les terroristes ont utilisé dans leur ensemble des téléphones portables sans contrat avec cartes téléphoniques prépayées, c'est pourquoi l'Espagne et d'autres pays Européens vont mettre fin à ce système qui permettait pourtant l'anonymat



Ainsi, par la puissance des outils aujourd'hui accessible, **le travail est pré-maché par les ordinateurs.** Dans l'exemple Espagnol, là où il aurait fallu probablement des semaines d'analyses de données brutes, le link analysis propose une solution graphique beaucoup plus adaptée à l'intelligence humaine et directement exploitable par pratiquement n'importe qui. Ce qui est très clair en tout cas, c'est que ces nouveaux outils logiciels rendent possible l'analyse de grandes quantités de données, inexploitées jusqu'à présent.

Les applications sont bien sur multiples : on l'a vu, dans le domaine policier et de la justice, les enquêtes sont grandement facilitées. En effet, en rentrant dans l'ordinateur des données à priori hétérogènes que sont les adresses des différents suspects et victimes, les numéros de téléphone qu'ils ont appelés, leurs différentes transactions financières sur un laps de temps donné, et leurs différentes relations familiales, les logiciels de « link analysis » en mettant en liaison toutes ces données peuvent faire apparaître des éléments tout à fait nouveaux et cruciaux pour l'enquête, qu'une analyse classique partant de pièces isolées n'aurait jamais pu rendre compte. Le secteur médical, en épidémiologie et pharmacologie fait plus que de s'y intéresser. En veille technologique également, on peut très facilement pour des brevets identifier des équipes d'inventeurs… Les banques et les assurances commencent aussi à s'équiper massivement dans la lutte contre la fraude. Ne doutons pas que les services marketing des entreprises sauront utiliser ces logiciels avec beaucoup de minutie, en rendant clairement exploitable leurs bases de données pour en savoir toujours plus sur le consommateur. Déjà, les trois opérateurs

de téléphonie français (SFR, Bouygues Telecom et Orange) estiment que grâce aux modèles comportementaux qu'ils ont élaborés grâce au data-mining et au link analysis, ils peuvent repérer à l'avance les clients susceptibles de passer à la concurrence ou ceux capables de souscrire des forfaits plus chers.[96]

Si ces outils sont mis en place, ce qui à l'air d'être le cas, à vaste échelle, le contrôle systématique et dynamique (avec de multiples évolutions dans le temps) est donc à portée de main. On comprend alors mieux **l'enjeu de la conservation des logs** (qu'on détaillera plus tard dans pour le cas français) menés par l'Europe et les gouvernements nationaux, lors des communications Internet et téléphoniques. En effet, la réunion des logiciels de link analysis alliée à la sauvegarde de toutes les données de connexion (logs) pendant une durée indéfinie vont placer le citoyen dans les mailles d'un filet extrêmement serré où sa liberté deviendra très contrôlée et où le temps ne jouera pas pour lui.

C'est probablement à ce type de système, que Jeffrey Ullman, ancien professeur à Stanford et spécialiste du Data mining, pense aujourd'hui : « Il faut financer un très important effort de recherche en informatique pour mettre à la disposition des services de renseignements un outil qui permette de trouver ce que ces tarés de terroristes mijotent… Il faudra peut-être dix ans pour mettre au point ce système, mais il faut le réaliser, **même si cela implique d'installer des capteurs électroniques à tous les coins de rue** pour repérer les suspects, **les comportements anormaux** et les substances chimiques dangereuses. C'est une question de survie pour l'Occident »[97].

La France n'est pas en reste pour innover et proposer des outils toujours plus graphiques et conviviaux pour toujours mieux surveiller. Jeune « pousse » lyonnaise, la société Foxstream[98] à mis sur le marché un système de **vidéo surveillance intelligent (!)** qui **donne du sens** aux images récoltés. D'abord focalisé sur les sites sensibles (usines pétrochimiques, zones militaires, sites industriels, prisons…), le logiciel FoxVigi est en train de s'attaquer aux marchés grand public, notamment la vidéosurveillance en milieu urbain, dans les transports, et la détection d'événements rares. Le logiciel est capable par exemple d'enregistrer l'heure à laquelle une personne âgée se lève le matin habituellement. Si un jour la personne ne bouge pas, l'alarme est déclenchée.
En fait le logiciel analyse les images des systèmes de surveillance, détecte les mouvements et identifie leur origine, y compris les événements anormaux, comme une personne profitant de l'entrée d'une voiture pour pénétrer dans un parking. Autre atout de taille : ce système intelligent différencie, entre plusieurs événements, ceux devant déclencher une alerte. Pour éviter de renforcer les effectifs chargés de surveiller les écrans 24h/24 puisque de multiples caméras rendent la somme d'informations à traiter vite ingérable pour quelques personnes, FoxVigi propose une solution qui peut intéresser effectivement à la fois le public comme le privé. La production d'image avec le renforcement un peu partout de la vidéosurveillance est tellement importante que **le nombre d'applications est malheureusement presque infini.**

[96] Tous fichés (Jacques Henno)
[97] Tous fichés (Jacques Henno)
[98] www.01net.com 26/10/2006

Et tous ces outils sont financés par une machine qui s'emballe. Examinons maintenant de plus près certains rouages de notre « toute puissante » économie.

3-6 Le néo-capitalisme : fin d'une mort annoncée ?

« Le métier de TF1, c'est d'aider Coca Cola à vendre son produit.
Ce que nous vendons à Coca Cola, c'est du temps de cerveau humain disponible. »
Patrick Le Lay, PDG de TF1

Adam Smith, père de l'économie moderne croyait en une « main invisible » (le lieu de rencontre d'égoïsmes rationnels) qui répartirait les revenus de façon juste et équitable pourvu que tout le monde « participe » de son mieux à la vie économique. Walras et Pareto prétendent démontrer que non seulement le marché est la forme la plus parfaite d'exercice de la liberté en économie, mais qu'il permet aussi la répartition la plus efficace des ressources et la meilleure satisfaction des consommateurs.
De la même manière en 1625 est écrit un texte fondateur de toutes les utopies de la liberté : le « De jure belli acpacis » de Grotius. Il proclame que l'homme ne doit pas obéir à une quelconque Loi divine, mais choisir les lois les mieux adaptées à son temps, organiser la comptabilité entre libéralisme économique et liberté politique, marché et démocratie, propriété privée et intérêt général.
Pourtant, dans les faits aujourd'hui **le capitalisme n'a jamais autant été porteur de déséquilibre sur notre planète**, à l'échelle des nations comme des individus. C'est un truisme de le rappeler, mais comme à aucune autre époque les pauvres ne sont devenus si pauvres, et les plus riches encore plus riches.

Comme lors d'une agonie, depuis quelques années maintenant, on sent que le capitalisme se démène pour trouver d'autres leviers d'action pour arriver à survivre.

Pour faire un très bref rappel historique de son évolution au 20ème siècle, c'est dans ses premières années qu'est né la véritable face du capitalisme, qui a **exclut très vite l'homme du centre du débat**, avec la production à la chaîne et l'organisation scientifique du travail échafaudé par Taylor (OST). Au départ, c'était l'offre de produit qui menait la danse, et le reste suivait par déduction. Par exemple, avec la Ford T, Henry Ford créa le 1er grand produit standardisé avec des modèles uniques en tout points, tous de couleur noire par exemple. Le problème en fait au départ était seulement de savoir produire. Il n'y avait pas de problème pour la demande, tout ce qu'on mettait sur le marché était acheté.
Les temps immédiats d'après guerre, avec des pays entier à reconstruire, ne posait pas non plus encore de problèmes au niveau de la demande…pratiquement tout ce qui était fabriqué était vendu.
C'est seulement dans les années 60 qu'on vit apparaître ce qu'on appelle le « marketing » ou « art » de mettre sur le marché des produits. C'est l'époque où l'on commençait à voir que produire n'était plus suffisant, il fallait aussi savoir vendre. D'où l'essor incroyable à cette époque de la publicité par exemple.
On commença alors à utiliser plusieurs leviers d'action : le premier fut le prix. En effet, entre 2 produits concurrents identiques, le consommateur préfèrera le moins cher. On retrouve ici les théories économiques de Smith et Ricardo. Cependant, le marché n'était pas encore pur et parfait comme dans la théorie. Le 2ème levier

d'action pour faire qu'un produit soit acheté plutôt que son concurrent fut la publicité (promotion). En effet, la ménagère de moins de 50 ans aura tendance à acheter en priorité le produit dont elle a entendu parler. Le 3ème levier sera le produit lui-même. Pour cela, il faudra que le produit soit « positionné » pour plaire à une catégorie donnée de consommateurs. D'où la naissance de discipline comme le packaging ou le merchandising pour essayer (en vain !) de donner une âme au produit.
Le problème est que ces leviers ont tous aujourd'hui atteint leur paroxysme. D'où une profusion dans tous les médias, d'une publicité à outrance vantant tel mérite ou tel prix d'un produit par rapport aux autres. Nous sommes tous devenus, par ces effets de martèlement, de vrai « **homo œconomicus** », en nous coupant, s'il était encore possible de le faire, de notre véritable être spirituel, en privilégiant uniquement notre confort matériel.
C'était encore sans attendre l'arrivé d'**Internet** qui permit **l'application de la théorie néo-classique d'un marché pratiquement pur et parfait.** En effet se sont créés sur la toile des sites de ventes aux enchères (classiques ou inversés), de groupement de consommateurs, de marchands plus classiques…etc., sites qui font tendre les prix des produits à leur minimum puisque le consommateur potentiel à d'un clic de souris accès à tous les concurrents et à leurs offres par rapport à un produit sélectionné. Cela veut dire que pour être encore plus attirante, la sphère capitaliste devra encore trouver d'autres « leviers » pour faire émerger le concurrent le plus attractif avec le prix le plus bas. Pour nous **ces leviers sont au moins au nombre de trois**, que l'on commence seulement à percevoir depuis quelques années.

Le 1er est le facteur humain. Ce n'est pas intégralement un nouveau levier car il était utilisé déjà depuis longtemps en face des « machines ». L'homme, complètement aliéné, était considéré seulement comme un facteur de production. On pourrait se dire que de ce côté là les choses ont bien évolué et c'est vrai…les ouvriers sont moins nombreux et probablement mieux traités et avec plus de droits qu'à cette époque (entendu que nous ne parlons ici que des pays occidentaux). Cependant ce qu'on appelle aujourd'hui les « ressources humaines » a évolué dans une voie plus qu'incertaine. L'évidence est de dire, si l'on considère toujours le facteur prix comme essentiel dans notre économie aujourd'hui, que moins le personnel sera nombreux pour produire un produit ou un service, plus le prix sera bas. Tout est donc bon pour augmenter la productivité sans augmenter les salaires, et donc travailler à partir d'un minimum de personnel. Cette tendance s'est bien sur accélérée avec le recours au travail temporaire et précaire, pour fournir aux entreprises le « juste de main d'œuvre » nécessaire, et rien de plus. Malheureusement depuis quelques années, une autre tendance forte du monde du travail à été révélée : le harcèlement moral. En effet, pour ne pas avoir à payer le plus souvent des primes de licenciement, les services de ressources (véritablement) « inhumaines », souvent grâce à la collaboration de certains collègues « intéressés », forcent des salariés à partir d'eux-mêmes, souvent en les décourageant psychologiquement[99]. Plusieurs techniques sont bien sûr utilisées : la mise au placard, les moqueries, le refus d'obéir…Bref les procédés sont nombreux et coûtent pourtant cher à la société et en l'occurrence à l'assurance maladie. On voit donc **dans ce harcèlement moral l'un des derniers leviers de l'économie qui tend vers une déshumanisation totale du travail.**

[99] Le harcèlement moral, Marie France Hirigoyen, Pocket

2ème levier, essayer de **faire croire que l'économie va donner un sens aux choses matérielles**. En effet, et c'est là aussi une tendance de fond, il y a une progression très forte des fondations d'entreprise (qui remplacent petit à petit les associations humanitaires, ou en tout cas qui les financent). Il y a là une continuité dans le paradigme sauveur/victime, les nations « riches » finançant la pauvreté du Sud. Or on comprend bien que seul **un équilibre « partagé »** pourrait solutionner durablement les choses, sans domination de pouvoir bien souvent assise sur l'argent. Ainsi on peut s'attendre dans la période qui s'annonce à avoir pour certains produits de véritables campagnes de pub à la sauce « humanitaire » pour nous faire croire qu'en consommant tel chose on va solutionner tel problème. Et en essayant par-là de redonner une certaine âme au produit ou au service, qui, le pauvre on le comprend, est à cours de recettes pour réussir à se faire vendre. Dernier coup d'échec de l'économie qui dans sa terrible agonie essaie de sauver sa peau ?

Le dernier élan de générosité « mondial » provenant des dégâts humains et matériels du tsunami en Asie a probablement ouvert la brèche. Les hommes, en quelques jours ont réussi, par un élan du cœur, à réunir plusieurs milliards d'Euros. On peut supposer que des néo-capitalistes vont voir là une manne financière à exploiter extrêmement importante. A n'en pas douter, la sphère « humanitaire » va être progressivement aussi happé par la sphère économique. Déjà les grandes associations caritatives dans leur fonctionnement et leur organisation ressemblent à s'y méprendre à de grands groupes industriels, avec des services marketing extrêmement pointus et développés pour aller toucher en profondeur l' « âme humaine » des donateurs. Cette fois ci **le néo-capitalisme à pour but de rentabiliser les sentiments humains**, la compassion des uns envers les autres pour toujours plus de profits.

Un autre exemple récent est la multiplication de certaines « pétitions » sur Internet. Le mécanisme en est simple : il faut trouver un sujet digne d'intérêt à connotation humanitaire ou écologique (récemment une pétition est apparue qui annonçait la déforestation annoncée de la moitié de la forêt amazonienne par le gouvernement brésilien) puis la diffuser et surtout expliquer à chaque signataire de la faire suivre à une dizaine de correspondant au moins de leur carnet d'adresses électronique. Ensuite, il suffit de dire qu'à chaque 500 signatures, un exemplaire doit être renvoyé à l'email d'origine de la pétition pour pouvoir rassembler toutes ces « signatures », et commencer à faire pression. Et alors, diriez vous, c'est ici agir pour la bonne cause. Et bien non, détrompez-vous. Les initiateurs n'en ont que faire de la forêt amazonienne. Ce procédé permet à des sociétés de récolter en un temps record des milliers d'adresses e-mail qu'ils pourront revendre au prix fort pour faire la plupart du temps du spam, ou en tous les cas de la publicité non désirée. Ainsi, sous couvert de cause légitime, on peut comprendre comment « l'économique » prend le dessus sur tout. Ce type de « **charity business** » affiche des promesses de développements exponentiels. Les plus innocents d'entre nous, pour ne pas dire naïfs, s'y feront prendre, à coup sur.

Dernier exemple avec Microsoft en France qui essaie de gagner des parts de marché par l'intermédiaire de sa fondation. Celle ci crée dans des villes françaises des associations dénommées « Clique sur ta ville » pour soi-disant « **lutter contre** l'exclusion numérique ». Ce qui est intéressant, c'est qu'apparemment Microsoft entend par ce biais faire parler de lui le moins possible en passant par des personnes morales associatives. Les villes n'ont qu'à dire « oui » et auront droit à plusieurs postes informatiques gratuits, à des licences logicielles à ne pas savoir qu'en faire, à des scanners, imprimantes, appareils photos numériques…, et à des

formations Microsoft pour les animateurs des associations locales. Eric Boustouller, Président Directeur Général de Microsoft France déclarait alors : « Il est aujourd'hui indéniable que les TIC jouent un rôle majeur dans la lutte contre l'exclusion et pour la réinsertion. **Il était tout naturel** que Microsoft France s'associe à cette démarche à travers le programme « clique sur ta ville » ».
Toujours dans la même entreprise, l'opération « Docteur Souris », cette fois ci lancée au niveau national, doit contribuer à l'amélioration de la qualité d'accueil aux enfants dans les hôpitaux, en fournissant aujourd'hui plus de 1000 ordinateurs portables wifi. Selon Microsoft, ce projet « aide les enfants et adolescents hospitalisés à rompre leur ennui et à communiquer avec l'extérieur grâce à l'informatique. » Rien à redire sur le papier, les résultats sont là. Pourtant, pouvons-nous vraiment croire les arguments philanthropiques de Microsoft, qui comme toute entreprise, doit pouvoir rendre des comptes à ses actionnaires, et **nous faire croire qu'elle compatit à la souffrance humaine ?**

Deux remarques. Premièrement, l'économie et le marketing confirment être, sous des aspects engageants, le cheval de Troie d'un contrôle qui pourrait devenir systématique. En seconde lieu, on pourrait avancer que les associations et les fondations, contre qui, pratiquement, aucun argument défensif ne tient, souvent parce que le côté « émotionnel » des choses prend vite le dessus, sont en train de devenir insidieusement aussi un alibi légitimant toutes les dérives de l'économie et du marketing.
Conséquence toute logique : le contrôle systématique pourrait bien être orchestré par une « sauce » humanitaire, contre personne, doté d'un cœur et de compassion, ne pourrait s'insurger, à moins d'en comprendre le mécanisme caché.

Enfin, **le 3ème levier** très prisé aujourd'hui pour être toujours plus compétitif, c'est **la montée en puissance du « renseignement économique »** ou encore « intelligence économique » dans les entreprises. Qu'en est-il exactement ? Cela consiste à obtenir l'information la plus fiable et pertinente possible sur un marché donné pour que les décideurs prennent la bonne décision au bon moment pour la bonne marche économique de l'entreprise. C'est **le monde du renseignement** étatique **appliqué à la gestion de l'entreprise**. Admettons à la limite (malgré la perversité du système) que les objectifs de survie de nos entreprises dans un monde hyper concurrentiel en passent par là. Ce sont les moyens pour y arriver qui peuvent paraître moins légitimes. En effet, ces cellules de « veilleurs » pourront, suivant leur degré d'éthique, piocher dans *l'information blanche* (l'information qui circule librement et qu'on trouve sans aucun problème, comme sur Internet, donc autorisé), *l'information grise* (qui se trouve être à la limite de la légalité, comme par exemple la fouille des poubelles d'une entreprise) ou l'information noire (information que l'on se procure au moyen de procédés cette fois ci complètement illégaux, comme par exemple le vol d'un ordinateur portable…). Il apparaît donc en filigrane que **pour être toujours plus compétitif et pour afficher des tarifs toujours plus bas, il devient nécessaire parfois de se mettre « hors la loi ».**

3-7 Le marché de la vie privée et l'Intelligence Economique, les derniers bastions d'une économie agonisante

« Notre liberté se bâtit sur ce qu'autrui ignore de nos existences. »
Soljenitsyne

L'économie, quelle que soit la forme qu'elle prenne se veut en apparence toute puissante. Pourtant, même en raisonnant en pure économiste, ce ne peut être à long terme qu'une illusion. « Les arbres ne montent jamais jusqu'au ciel et l'on ne voit pas comment les marchés boursiers pourraient continuer à croître de 10% par an quand les taux de croissance annuels des économies occidentales sont de l'ordre de 2 à 3% » analyse Jean Peyrelevade[100]. Les partisans de la « décroissance » montrent scientifiquement que si tous les pays du monde vivaient sur le même élan de consommation que les pays riches occidentaux, il faudrait 4 planètes Terre pour satisfaire tout le monde !

Dans le chapitre précédent, on a vu que l'on s'achemine de plus en plus à **la limite du possible** dans le monde économique et de l'entreprise, à savoir **du côté humain à la frontière entre santé mentale et maladie psychique** (harcèlement moral), puis **à la confusion marketing entre matériel et spirituel** (âme et sens du produit), et **du côté juridique, à la frontière entre le légal et l'illicite** (Intelligence économique).

Or il faut voir que tous ces éléments, nourris préalablement dans la sphère économique sont en passe de **se répandre à grande vitesse dans les cadres de vie personnelle de chacun**. Et ce désordre se propagera définitivement une fois que le marché de la vie privée deviendra parfaitement organisé.

Un exemple dans le domaine de la santé, domaine de la vie privée par excellence : Norbert Paquel, consultant spécialisé dans les applications médicales de l'Internet, cité par l'AFP, imagine que dans quelques années "les contrats d'assurance maladie demanderont aux clients de porter des puces électroniques en permanence et qu'ils imposeront des obligations - ne pas fumer, boire, manger certains aliments - dont le respect pourra être vérifié en continu à distance grâce à l'Internet".

Les Etats-Unis semblent aussi montrer la voie[101]. Toujours pour des bonnes raisons (épouse volage, mari infidèle…), moyennant une centaine de dollars n'importe quel individu peut se procurer les relevés de communications téléphoniques mobiles de la personne de son choix. De Locatecell.com à Bestpeoplesearch.com, on ne compte plus les sociétés qui ont investi ce créneau particulièrement lucratif. En effet, des douzaines de sociétés américaines opérant sur Internet se sont spécialisées dans la revente de relevés de communications sur téléphone portable. Selon le Washington Post, pour parvenir à leurs fins ces voleurs d'informations d'un nouveau genre utilisent trois techniques. Il leur arrive de disposer d'un « correspondant » employé par un opérateur de téléphonie mobile, qui leur fournit de petits services. Autre solution : détenir (frauduleusement) le numéro de sécurité sociale d'une personne (l'identifiant comme possesseur d'une ligne mobile) et usurper son identité afin de récupérer les informations concernant ses communications (noms des personnes

[100] Dans « Le capitalisme total » (2005)
[101] www.01net.com 13/01/2006

appelées, durée des appels...). Enfin, une dernière solution consiste à essayer d'accéder en ligne et sans son consentement au compte personnel d'un abonné. Interrogé par CBS, Noah Wieder, le responsable de l'une de ces sociétés, Bestpeoplesearch.com, tenter de minimiser le phénomène. « Il ne s'agit pas d'une activité illégale. Disons que le secteur s'autorégule. C'est comme l'alcool. Si vous le laissez entre de mauvaises mains, cela peut devenir dangereux. » !

Toujours aux Etats-Unis, pour apurer les comptes d'une association d'utilisateurs HP (Hewlett Packard), la justice est allé jusqu'à mettre son fichier d'adhérents aux enchères, cédant au plus offrant un fichier contenant des informations relatives à plus de 100.000 personnes. Il est vrai qu'une telle opportunité avait de quoi faire saliver beaucoup de services marketing, car le fichier répertoriait les adresses personnelles des responsables informatiques et des informations relatives à leur équipement. Le prix de départ était fixé à 15.000 dollars. Les adhérents ont, on le comprend, grincé des dents, et craignent en plus que le fichier soit vendu plusieurs fois et que leur email professionnel devienne la cible de spammeurs.[102]

L'Intelligence Economique (I.E), dernière invention de nos économies modernes pour survivre, commence depuis quelques années à acquérir en France ses lettres de noblesse parmi les pratiques de gestion des entreprises, et son évolution rapide est intéressante à observer. Alain Juillet, le « Monsieur Intelligence Economique » Français, directement rattaché au Premier ministre, affirme que l'I.E. provient du mariage de la mondialisation d'une part, et des nouvelles technologies d'autres part : pour que les dirigeants d'entreprise puissent aller trouver les opportunités dans le monde pour prospérer économiquement, les TIC permettent, parmi les milliards d'informations qui existent, de les analyser, de les synthétiser et d'en extraire l'essentiel. Pour lui en effet, nous sommes en train de changer de paradigme (mais pas le même dont nous parlerons plus tard). D'une économie dictée préalablement par la loi de l'offre et de la demande, à l'heure où tout va de plus en plus vite, c'est « l'information » qui prend, selon lui, désormais le relais. Disposer de l'information plus vite que ses concurrents, pour acheter ou pour vendre et pour prendre les meilleures décisions, est désormais crucial pour « **ceux qui veulent survivre** », dans un contexte ou chacun désormais, y compris les pays en voie de développement, veut des parts du gâteau de la « croissance » internationale. Ainsi en stratégie d'entreprise, on considère que les sociétés peuvent prendre deux voies pour attaquer un marché : la stratégie de prix, ou celle de différenciation. Or, avec le très faible coût de la main d'œuvre dans les pays émergents, les occidentaux ont compris que la seule bataille qu'ils peuvent remporter se situe sur le terrain de **la différenciation**. L'innovation et la « matière grise » sont alors essentiels à maîtriser, et c'est bien souvent l'I.E. qui permettra aux entreprises, grâce aux informations fiables qu'elle amène, de développer un avantage concurrentiel, sur ces concurrents, au moins pour un temps. Parler de « guerre économique » aujourd'hui n'est pas un vain mot.

Et pour arriver au bout de cette logique neo-capitaliste, chaque nation qui veut « gagner » doit être « solidaire » à tous les niveaux. C'est pourquoi notamment, « public » et « privé » doivent travailler ensemble pour permettre au pays de ne pas être devancé par les autres. Aux Etats-Unis, les liens entre la communauté du

[102] www.01net.com , 28/10/2005

renseignement et les entreprises privées sont devenus si étroits que l'on peut parler de complexe « secréto-industriel », à l'image du complexe « militaro-industriel ». Les entreprises américaines n'ont plus aucun scrupule à collaborer avec les services de sécurité, voire à se substituer à eux dans certaines tâches de surveillance.[103] Drôle de vision de la solidarité lorsque celle-ci s'ingénue à s'approprier « le plus possible » au détriment des autres nations. Ainsi, au nom de cette « fraternité économique » ou autre **« patriotisme économique »,** peut-être demandera-t-on au « public » de permettre au « privée » d'accéder à toutes ses bases de données pour être plus efficace contre les autres pays dans la « guerre économique » qui démarre. Richard Stallman, figure emblématique du monde de « libre », analysait[104] d'ailleurs le renversement de situation : « de nos jours évidemment, alors que les états obéissent aux entreprises, il est presque impossible d'avoir un projet de loi qui soit bon…On ne peut pas attendre une bonne loi tant que les entreprises dominent les lois ».
Et à l'inverse, en gage de bonne réciprocité, le privé devra peut être fournir aux Etats leurs informations sur chaque « consommateur » pour compléter, qui sait, leur fichage, comme ce qui à put déjà commencer aux Etats-Unis, ce que nous verrons plus loin. Qui oserait s'insurger contre le rassemblement de « toutes les énergies autour d'un véritable patriotisme économique »[105] ? « Tous dans la même galère », on nous conjurera de donner au monde économique toutes les informations pour qu'il devienne un « gagnant » dans la compétition mondiale et pour assurer notre modèle social. Dans cet ersatz de fraternité, toutes les dérives deviennent alors possibles.

C'est ainsi que dans cet esprit tout un tas de techniques sont inventées pour encore mieux espionner les entreprises… et pourquoi pas aussi son voisin. Parmi celles-ci, le « **Keylogging** ». Un petit programme, dit « keylogger » est installé sur l'ordinateur à l'insu de son utilisateur. Ce logiciel va enregistrer toutes les frappes au clavier. Ainsi, à petite échelle, un employeur va pouvoir surveiller avec une grande proximité ce que font réellement les salariés. Il fut très utilisé aussi par les pirates pour connaître le sésame des clients des banques utilisant le web pour consulter leur compte en ligne et faire des virements. Ainsi, identifiants et mots de passe pour se « logger » à la place du client n'avaient plus de secret pour eux. A plus grande échelle, et dans la guerre économique qui commence à faire rage, il peut être fort intéressant (et facile avec ces techniques) de savoir à quel type de brevet s'intéresse telle ou telle firme, quelles innovations elles sont en train de développer…etc. Et c'est là que le privé aura à son tour besoin des « grandes oreilles » des nations du pôle économique pour lequel elle a entamé la partie.

[103] Tous fichés (Jacques Henno)
[104] Interview de Richard Stallman par VNUnet.fr du 13/06/2006 par rapport au projet de loi DAVIDSI
[105] Dominique de Villepin, 27/07/2005 à propos de la rumeur d'Opa hostile sur Danone

La différenciation en gestion, c'est lorsque l'entreprise développe une gamme de produitd et une stratégie marketing de haut niveau de façon à bénéficier d'une position de référence : la plupart des clients préfèreraient acheter cette marque s'il n'existait pas de barrière de prix. Seul une différenciation effective permettra de pratiquer un prix plus élevé, justifié par une valeur accrue aux yeux du marché. L'innovation est souvent la clé pour y arriver.

Les **Keylogger** sont des programmes, commerciaux ou non, d'espionnage. Ils peuvent être installés silencieusement et être actifs de manière totalement furtive sur votre poste de travail. Ils effectuent une surveillance invisible et totale, en arrière-plan, en notant dans des fichiers cachés et compressés le moindre détail de votre activité sur un ordinateur dont toutes les touches frappées au clavier, d'où leur nom de "keylogger". Ils sont aussi capables de faire un film de tout ce qui se passe à l'écran, en continu ou par capture d'écran à intervalles réguliers... Ils notent quels programmes sont utilisés et pendant combien de temps, les URL visitées, les e-mails lus ou envoyés, les conversations de toutes natures... dès la mise sous tension de la machine. Ils permettent, par la même occasion, de lire les champs habituellement cachés comme les mots de passe, les codes secrets etc. Dans le même esprit on a vu récemment l'apparition des « jitterbugs » qui sont « physiquement » introduits dans des périphériques informatiques tels que la souris, les câbles, la webcam, le micro… dans le but de dérober, là encore, des données, en les envoyant via n'importe quelle application logicielle interactive utilisant le réseau.

Mais, bien entendu concernant le marché de la vie privée, c'est sur la « Toile » elle-même que les plus grosses dérives apparaissent. La société Intelius.com créée en 2003 aux USA, avec un CA autour de 40 millions de Dollars en progression de 760% depuis le 1er exercice s'est vu attribuer la palme par l'American Business Awards de la « meilleure nouvelle compagnie ». Ce sont chaque mois plus de 30 millions de visiteurs qui se connectent pour vérifier, par exemple, qui est leur nouveau voisin ou les personnes que leurs enfants fréquentent. Contrairement à la France où le croisement de fichiers est strictement réglementé, Intelius et ses concurrents peuvent s'en donner à cœur joie aux Etats-Unis. Tout y passe : commandes sur catalogues, abonnements à des magazines, enregistrements de propriété immobilière, les arrêts de cour de justice, blogs personnels, questionnaire en ligne. On peut presque tout savoir.

Intelius se fait forte, pour 7,95 dollars (environ 6,20 euros), de retracer la vie privée (mariage, divorce, nombre d'enfants, déménagements) de n'importe qui au US. S'affichent aussi son revenu, la valeur de son bien immobilier. On va connaître la surface de sa maison, le nombre de pièces et même le mode de chauffage. La photo satellite du bien est certes un peu floue, mais le plan du quartier est précis, et une fiche indique même le «profil» de la population environnante : pourcentage de Blancs ou de Noirs, niveau d'éducation et de revenus.
Ira-t-on jusqu'à vérifier ses antécédents judiciaires ? Moyennant 49,95 dollars (environ 39,10 euros) de plus, Intelius y incite fortement pour *the peace of mind,* comme ils disent (pour avoir la « tranquillité d'esprit », cher à tout discours sécuritaire). Intelius propose de scruter le passé «criminel» de n'importe qui, histoire

de vérifier s'il a, par exemple, été ou non condamné pour *«offense sexuelle»*. L'idée étant d'amener tout parent à se poser cette question : *«Connaissez-vous réellement la personne qui s'occupe de votre enfant ?» «Et, au fond, savez-vous qui est son coach sportif* ?»
Pour se couvrir, l'entreprise rappelle à ses clients qu'ils ne doivent pas utiliser les informations obtenues sur une personne pour la *«harceler»* ou la *«menacer»*[106] ! Et pourtant, ce business n'alimente que très peu les débats outre atlantique. On pourrait espérer une autre perception si ce concept venait à débarquer dans l'union européenne.
Une fois de plus les nouvelles technologies détériorent la confiance que pouvaient se porter entre eux les êtres humains. En voulant « tout savoir », en voulant « la vérité » sur chacun, ne risque-t-on pas de mettre à mal ce pilier fondamental du règne humain ?

3-8 Les TIC : une « création » de l'homme, à son image ?

« En nombre del progreso y de la revolucion
Quemaron tradiciones y pisaron el honor »
Mecano

L'être humain, par la matérialisation obtenue par ses connaissances, c'est-à-dire la technologie, est en train de créer son œuvre ultime, à travers les ordinateurs et le réseau Internet.
On peut ainsi dire, et nous allons le montrer, que l'ordinateur individuel est l'image matérielle de l'être humain, et que le réseau Internet n'est autre que l'image matérielle de l'humanité, voire peut être même de sa conscience collective.
Les humains seraient ils sur le point de se prendre pour Dieu en créant un Univers, dans la matière, qu'ils auraient l'impression de contrôler et de dominer ? Vanité humaine et toute puissance de la Science ?
Le Web est en effet devenu un super organisme d'une nature et d'une taille encore jamais vu sur Terre à ce jour. D'ores et déjà il comprend plus d'1 milliard de correspondants potentiels, c'est-à-dire de machines capables d'émettre et de recevoir des messages : PC, téléphones portables, Internet des objets. Ceux-ci ont généré près de 50 milliards de pages. Dans 10 ans, il connectera des milliards, voire des dizaines de milliards de terminaux de toutes sortes et aura créé un nombre de pages et de messages pouvant atteindre le milliard de milliards.[107]

L'intelligence
La guerre de l'intelligence a déjà débuté sur Internet. Les moteurs de recherche type yahoo, msn ou autres google rivalisent d'ingéniosité dans leurs algorithmes de classification des pages pour offrir aux internautes les classements les plus pertinents lors de leurs interrogations.
Voici ce qu'on trouve sur le site de Google France quant à sa technologie de classification appelée « Page Rank » :

[106] Inspiré de www.liberation.fr 11/08/2006
[107] http://philoscience.over-blog.com/ « Le web est il un cerveau global ? », 3/02/2006

« PageRank permet de mesurer objectivement l'importance des pages Web. Ce classement est effectué grâce à la résolution **d'une équation de 500 millions de variables** et de plus de **8 milliards de termes**. PageRank utilise la vaste structure de liens du Web comme un outil de classement. Pour simplifier, Google interprète un lien d'une page A vers une page B comme un " vote " de la page A pour la page B et évalue ensuite l'importance d'une page en fonction du nombre de votes qu'elle reçoit. »… « Nous avons développé une technologie de recherche avancée qui fait appel à une série de calculs simultanés réalisés généralement **en moins d'une demi seconde, sans intervention humaine** ».

L'intelligence, derrière ces milliards de variables, dont fait preuve le réseau Internet commence à rentrer en compétition avec celle du règne humain. La mesure, même inconcevable par l'esprit humain, d'une **infinité de variables** et d'un **amour inconditionnel** est peut-être le plus juste pour essayer d'approcher ce que de nombreuses Traditions appelle la Création. Pourtant la course est lancée et la technologie s'essaie à concurrencer l'infini : un PC mis sur le marché en 2005 est tout juste capable de traiter quelques centaines de millions d'opérations par seconde. La NSA travaille à l'élaboration d'ordinateurs capables d'effectuer 10 exposant 24 opérations par seconde, c'est-à-dire un million de milliards de milliards d'opération par seconde ! Pour Joël de Rosnay, « la densité des nœuds du réseau (internet) associée à la capacité de tisser des liens entre eux peut être comparée aux neurones d'un cerveau et à ses ganglions inter neuronaux : chaque neurone (il y en a 15 à 20 milliards dans notre cerveau) est connecté à 10.000 autres neurones, ce qui donne une idée de la densité de ce réseau. Qu'on le veuille ou non, **le Net est en train de se constituer à la manière d'un cerveau**, avec ses synapses, ses interconnexions, ses dendrites… »[108]

La mémoire

La bataille pour la connaissance est aussi, on le pressent intuitivement, en cours. Au niveau de l'ordinateur individuel, c'est le disque dur qui fait office de « mémoire » et qui emmagasine les connaissances.
Internet, lui, comme notre réseau de neurones dans nos cerveaux humains, est émietté dans un réseau de « serveurs » qui distribue ainsi la connaissance planétaire à qui la demande. Internet constitue une mémoire Eidétique, c'est-à-dire une mémoire totale.
Qu'est ce que cela signifie concrètement, pour nous. En fait, selon Denis Ettighoffer, Président d'Eurotechnopolis Institut « le réseau, en interdisant l'oubli, pourra retenir tous les actes d'un individu. Actes anciens librement disponibles à tous, parfois déformés ou sujets à interprétations discutables car traités ou saisis par des hommes faillibles. Un individu, pour sa part, ne retient consciemment qu'une très faible partie de sa vie. Il dispose de multiples possibilités, de multiples voies pour réussir sa vie. Mais c'est l'oubli des parties les plus dures, les plus difficiles, **l'oubli des erreurs ou des fautes passées qui permet à l'individu de survivre et de se reprendre pour réussir, enfin, une vie parfois mal partie.** » A l'opposé, toute démarche de lecture ou d'écriture sur le web est mémorisée quelque part, sans limite de temps. Cela signifie que se créent à chaque fois des liens nouveaux entre données jusqu'ici non reliées. Si je vais lire le contenu d'un site, je crée un lien entre mon adresse IP et

[108] La révolte du pron@tariat, Joël de Rosnay, Fayard, 2006

celle de ce contenu. Le Web devient donc une gigantesque mémoire, une immense base de données qui, 24h sur 24, n'arrête jamais de travailler et de s'étendre, et qui me trace par les différents objets qui mémorisent les liens, physiques ou virtuels, que j'établis sans cesse dans ma vie sociale.
Le problème avec cette mémoire eidétique, c'est que, déjà actuellement, elle ne possède pas « d'inconscient », c'est-à-dire d'endroit où chacun puisse laisser aux oubliettes des actes passés, pour permettre de s'ouvrir à autre chose et donc, d'évoluer. Le réseau n'a pas de « mémoires mortes » qui, comme chez l'homme, cachées ou masquées par le temps, permettent les oublis nécessaires à la vie en commun. Du coup, **le réseau n'oublie pas** les vieilles rancunes, le dénigrement, les mauvais souvenirs, les erreurs passées. Ainsi, il devient pour quiconque très facile de mettre son prochain en difficulté, en retrouvant, par exemple, chez un collègue de travail dont on envie jalousement sa place, des détails croustillants sur sa vie privée, sur d'éventuelles condamnations, sur des erreurs de trajectoires, qui pourront ainsi le faire chuter. Qui pourra dans ce cadre se montrer « parfait » ? L'homme est un être en devenir, jamais sclérosé, toujours et à chaque instant en perspective d'évolution. Le réseau ne nous le ferait-il pas prendre pour ce qu'il n'est pas, un amas de matière sans futur, tout juste bon à dénoncer son prochain.
Les politiciens, précurseurs dans ce qui pourrait peut-être s'étendre un jour à l'ensemble des citoyens, commencent à faire depuis peu les frais de cette « mémoire » qui n'oublie ni ne pardonne plus rien. Le sénateur Démocrate John Kerry s'est attiré un feu nourri des républicains en ayant déclaré à des étudiants américains que s'ils n'étudiaient pas avec assez d'assiduité, ils se retrouveraient « pris en Irak ». Malgré ses excuses, la mauvaise blague du Sénateur ne s'est pas éteinte d'une belle mort comme cela aurait pu se passer il y a quelques années encore. Au contraire, Internet a eu un effet démultiplicateur en relayant non seulement la nouvelle, mais en l'amplifiant énormément. Des clips ont par exemple été publiés de la part des 2 camps sur le site de partage de vidéo YouTube.com . «À peu près tout ce que dit toute personne de renom est susceptible d'être publié et rendu visible de façon régulière, non ponctuelle. La marge d'erreur est presque réduite à néant de nos jours pour les personnes du domaine public», estime Stephen Hess, ancien rédacteur présidentiel et enseignant dans le domaine des médias et des affaires publiques à l'Université George Washington. Et même si des caméramans professionnels ne sont pas présents forcément lors de toute situation pouvant concerner la vie publique, il n'y a pas de doute qu'une webcam ou qu'une personne dotée d'un téléphone cellulaire avec caméra relaiera l'événement et en fera partager la terre entière en le publiant immédiatement sur son blog. La question reste toujours la même : les hommes sauront ils faire bon usage d'une telle liberté (ou devrions nous dire plutôt de ce « pouvoir ») qui paraît devenir sans limite ?

Pour donner un exemple concret aujourd'hui de cette mémoire eidétique, on peut revenir quelques instant à l'exemple Google. D'après Silicon.fr[109] « Google a imaginé, dès sa création, une architecture de stockage capable de stocker des milliards de fichiers, pour une capacité cumulée de plusieurs Po (1Po = 1 000 000 Go)…et pour satisfaire les requêtes planétaires, ce type de configuration existe en plusieurs lieux de la planète… » Cela peut laisser rêveur…
Dans le même ordre d'idée, la très secrète NSA aux Etats-Unis enregistre chaque jour 650 millions d'événements (conversation téléphonique, émission de télé ou radio…). Mais l'agence ne conserve qu'une partie des écoutes (180 millions de

[109] Du 26/01/2006

communications à l'heure) pour cause de capacité de stockage limité. Mais ce n'est qu'une question de temps car très bientôt, de nouveaux serveurs lui seront livrés et lui permettront de garder disponible pendant plusieurs années toutes nos communications[110] !

Le **disque dur** est un périphérique de stockage magnétique. Il a remplacé efficacement les tambours (aujourd'hui obsolètes) et les bandes, seulement utilisées de nos jours pour l'archivage et la sauvegarde. Inventé en 1956 par IBM, leur capacité augmente très rapidement tandis que **leur encombrement et leur prix se réduisent très vite.**
En informatique, la mémoire fait référence aux technologies permettant de conserver fidèlement des données sous forme numérique.
(Source : Wikipedia)

La communication

L'homme est par tous ses aspects un être de communication, qu'elle soit verbale ou non verbale. L'informatique lui a simplement repris ses caractéristiques.
Dans toute communication quelle qu'elle soit, il y a toujours deux pôles : l'émetteur et le récepteur, qui s'échangent l'un après l'autre des informations. Pour le côté récepteur, comme l'homme par ses 5 sens, l'ordinateur possède ainsi plusieurs caractéristiques : il peut recevoir des informations depuis son clavier, depuis des disquettes ou maintenant de clés USB, depuis un scanner, etc.
Concernant l'émetteur, là aussi comme l'homme doté de paroles et de gestes, l'ordinateur transmet des informations via tout simplement l'affichage des données sur l'écran, via l'écriture de données sur des supports de mémoire (disque dur, clé usb…), également par le biais d'une imprimante, etc.

Sur le réseau Internet, symbole de la communication par excellence, on raisonnera davantage en terme de flux entrant et de flux sortant. En effet, et c'est tout à fait visible quand on utilise un firewall, chaque partie du réseau s'échange des informations, pouvant en même temps gérer l'émission et la réception, l'upload des données et le download.
D'après Jean Paul Baquiast[111], le cerveau humain n'a des capacités cognitives que parce qu'il est relié à un corps qui le distingue de l'univers extérieur et avec lequel il interfère en permanence grâce à des organes sensoriels et des organes moteurs. Or la « Machine du web » fonctionne aussi de la même manière : son corps et ses organes sont faits des innombrables utilisateurs du web, humains ou machines qui deviennent ses organes sensoriels et moteurs. On peut imaginer aussi que ces utilisateurs soient assimilés sur le réseau à des neurones cérébraux, plus ou moins passifs (tout le monde n'est pas connecté en permanence, du moins pas encore), participant au fonctionnement du web.
Là encore, comme pour la **mémoire** et **l'intelligence**, **la caricature de la communication humaine** par les technologies informatiques est quasi-parfaite, du moins du point de vue du quantitatif. Mais l'homme, par son libre arbitre, a le choix de ce qu'il veut divulguer ou pas aux autres, et ce d'une manière plus inconsciente, de ce qu'il « reçoit » des autres. Il possède donc là **un « espace » de libre choix**

[110] Tous fichés (Jacques Henno)
[111] http://philoscience.over-blog.com/ « Le web est il un cerveau global ? », 3/02/2006

qui n'existe plus avec les TIC. En effet sur un réseau Internet qui devient omniprésent, chaque communication laisse des traces indélébiles et impérissables, qui ne permettent plus à l'homme d'apprendre de ses erreurs et d'évoluer, mais qui le juge et peuvent le rendre fautif.

Ainsi on peut dire que le réseau Internet et son devenir dans l'évolution, que ce soit par son intelligence, sa capacité de mémorisation proprement gigantesque, sa capacité à communiquer tout aussi impressionnante (et certains prédisent qu'avec les perfectionnements technologiques on pourra voir un jour sur le web **l'apparition d'une quasi « conscience »**) peut être vu comme une parodie, extrêmement bien réalisée d'un point de vue quantitatif, de ce que les grandes religions révélées appellent « Dieu ». Pour être parfait en somme, il n'y manquerait… que l'Amour.

3-9 Un disque dur et une connaissance planétaire

« Quand j'aurai le don de tous les mystères et de toute la connaissance…Si je ne n'ai pas l'amour, je ne suis rien »

Lettre de Saint Paul aux Corinthiens, XIII

Les éditeurs Internet se démarquent par toujours plus d'ambition dans la quête sans fin de parts de marché planétaire. En effet, Google et son « Google Desktop » dans ses deux premières versions se proposent, depuis assez longtemps même, sur un ou plusieurs mots clés tapés au clavier, de faire des recherches sur le disque dur de l'ordinateur personnel de l'internaute. Non seulement, l'internaute peut effectuer une recherche dans ses courriels via cette barre d'outils mais aussi dans tous ses documents Word, Excel, Power Point et dans ses conversations effectuées grâce aux messageries instantanées de type Msn. En effet concrètement, lorsque l'application est lancée, le navigateur Internet s'ouvre sur une page Google classique, à cela près que le bouton « Search the web » est remplacé par un bouton « Search Desktop ». C'est la seule différence en apparence.
Mais c'était sans attendre la dernière évolution de Google aux Etats-Unis avec son Desktop 3ème version, lancé début février 2006. En effet, jusqu'alors, la frontière était encore séparée entre recherche de contenu sur le web et recherche sur les disques durs personnels. Ce qu'on pouvait prendre pour de l'anticipation n'en n'est plus : Google propose aujourd'hui un outil global qui permet, en même temps une **recherche à la fois sur le web et sur les disques dur des particuliers** ! Ce système est baptisé « Search Across Computers » et permet à présent le partage élargi des données, suivant en cela une philosophie inspirée des systèmes peer-to-peer. Mais c'est beaucoup plus préoccupant car via Google**, « il devient possible de chercher et de récupérer des documents stockés sur un ordinateur distant, même si celui-ci n'est pas connecté ou sous tension**. Ce qui implique que Google maintienne à jour sur ses serveurs, par le biais d'Internet, **une copie de la mémoire de chaque ordinateur** (appartenant à des particuliers) ayant activé la fonction Search Across Computers »[112]. Le fossé entre web (espace collectif) et donnés stockées sur le disque dur (vie privée) s'atténue donc fortement. Le marché voulant toujours plus, Google et (probablement d'autres plus tard) propose donc à leurs utilisateurs de lancer des requêtes non seulement sur le web mondial, mais sur

112

tous les disques durs des particuliers de la planète à la fois, à la condition express, pour le moment, que ceux ci aient donné leur accord. Techniquement c'est donc aujourd'hui réalisé. Il suffisait que l'opinion publique soit suffisamment assez « désinformée » pour mettre tout cela en pratique.

Mais les choses vont encore plus loin. Lancé en Août 2005, Writely (qui à été depuis racheté par Google) est une application du web 2.0 qui permet à ses utilisateurs de rédiger et de mettre en forme des documents en ligne (du type de Word). **Plus besoin de logiciel, ni de disque dur, tout est accessible à distance !**[113] Début Juin 2006, le célèbre moteur de recherche lançait aussi Google Spreadsheet (concurrent d'Excel) et certains analystes pensent qu'il pourrait **lancer une suite bureautique en ligne** complète. **Internet pourrait devenir progressivement une véritable plateforme** (voire qui sait un jour un gigantesque système d'exploitation mondial) **pour chacune de nos applications** : il ne serait plus nécessaire de les installer sur nos ordinateurs puisqu'elles fonctionneraient depuis l'Internet. On peut supposer qu'il s'agit là d'une tendance forte du développement de l'internet : les applications (type word, excel, photoshop…) seront « prêtées » gratuitement par les grandes multinationales du web, et en apparence sans contrepartie. Sauf que là encore, et c'est la grande force de Google qui l'a compris avant les autres, l'ensemble des documents sur lesquels travaille un internaute seront stockés sur les serveurs de ces « fournisseurs de service » qui pourront établir, puisqu'il y aura donc beaucoup de matière pour cela, des profils quasiment « exhaustifs » de chacun d'entre nous. Et renforcera aussi le fait **que toute production humaine sera désormais présente et accessible à tous sur le réseau**.

Neuf télécom annonçait fin 2005 le lancement d'un disque dur virtuel de 9Go (ce qui est assez considérable), c'est-à-dire « un espace dématérialisé sur le web qui permet de stocker des fichiers de toutes sortes et de les partager avec ses contacts » selon Patrick Asdaghu responsable marketing chez Neuf Cegetel. « L'utilisateur pourra se connecter aux fichiers stockés depuis n'importe quel ordinateur s'il est muni de son identifiant et de son mot de passe ». La stratégie des poids lourds du web semble donc converger. Avec les débits vertigineux de l'Internet à venir, **l'espace de stockage des informations est peut être en voie de disparition sur les disques durs des particuliers et des entreprises, pour prendre place sur des serveurs de multinationales du web.** Drôle de mélange de la vie privée à la sauce Internet. Microsoft et Google ont ainsi lancé respectivement leur projet « Live Drive » et « Gdrive ». Véritables disques durs à distance, ces services permettent aux utilisateurs de stocker aussi bien des films, de la musique, des vidéos conférences très haute définition ou tout autre sorte d'information. L'un des arguments avancé pour utiliser ces solutions est que toutes les informations ainsi enregistrées seront protégées des virus et consultables depuis n'importe quel ordinateur. Utopie ultime du nomadisme ? Streamload, l'un des pionniers de ce que l'on commence à appeler des « coffres virtuels en ligne » surfe sur la vague d'un business de stockage de toute forme de données. Selon Steve Iverson, le PDG de cette firme prometteuse de San Diego, les gens vont commencer à sauvegarder sur Internet et non plus sur des disques durs privés (bandes magnétiques, clés usb, disques durs externes ou internes…), et cela pour 4 raisons : « la facilité, **la sécurité**, l'accès et le prix. »[114]. Par exemple, « lorsque vous nous confiez vos données, elles sont stockées et

[113] www.webrankinfo.com mars 2006
[114] www.lexpansion.com 08/09/2006

répliquées sur nos serveurs étudiés pour fonctionner 24h sur 24. » Concernant le coût : « le prix du stockage et de la bande passante ont énormément baissé. Au point que nous pouvons offrir gratuitement 25 giga-octets à tout le monde ! »

L'administration française s'y met aussi avec le projet d'administration électronique Adele. Il s'agissait d'expérimenter en 2006 la création « d'un espace de stockage personnalisé accessible en ligne » à partir duquel l'usager pourra communiquer avec les administrations et **conserver les informations et documents** nécessaires à ses démarches. En 2007, les Français qui le veulent pourront archiver leurs documents officiels sous forme électronique dans un « coffre-fort virtuel »[115]. Sur un espace personnel situé sur un serveur appartenant à l'Etat et accessible depuis n'importe quel ordinateur, pourront être stockés « tous les éléments nécessaires à ses démarches » pour éviter d'avoir à en faire régulièrement des copies, par exemple comme les bulletins de salaires, le livret de famille ou les relevés de comptes bancaires. Bref, tous ces documents officiels qui, peu à peu, prennent une forme électronique.

La virtualisation et la « connaissance », comme elles se doivent, dans nos sociétés modernes, d'être « pratiques » pour attirer à elles un nombre croissant de personnes, doivent déboucher, puisque la facilité d'utilisation est un point crucial, à des « synthèses graphiques » aisément compréhensibless et manipulable par tous. C'est là qu'entre en jeu encore Google avec son Google Earth, ou plus modestement l'IGN sur le territoire français, dans cette course à la représentation 3D virtuele du monde. Exemple très concret, le GPS de demain est en cours de développement dans le cadre d'un accord entre Volkswagen et Google. Bientôt, les voitures seront équipées d'un système GPS utilisant Google Earth générant, au fur et à mesure de l'avancée des véhicules, des images en 3 dimensions de la route à suivre. En outre le système pourra recueillir des données sur Internet en les intégrant au fur et à mesure. Ainsi, le conducteur pourra connaître en temps réel l'état du trafic, du temps ou même des accidents éventuels. On est très proche de la réalité virtuelle. Il sera par exemple alors très facile de localiser les prochaines stations essences, leurs heures d'ouverture, de repérer des restaurants ou des cinémas sur la carte. Il suffira d'un clic pour connaître le menu ou les heures des projections. Les passagers pourront savoir les prix auxquels se vend un produit dans les différents magasins du quartier traversé[116]. Ils pourront également consulter des photos prises par les internautes sur la région sélectionnée. En effet, il est désormais possible, comme avec le site www.flickr.com de « géolocaliser » ses photos, c'est-à-dire de désigner sur un plan (comme avec Google Maps ou Yahoo Maps) l'endroit où à été pris le cliché. Lors de son ouverture en Aout 2006, Flickr à vu se géolocaliser 1,2 millions de photos en 24 heures !

Ce système GPS amélioré, selon nous, ne se bornera pas simplement aux véhicules. Car l'une des mutations majeures concernera **l'évolution vers l'internet des objets**. Nous avons un aperçu de ce que sera cet « Internet des objets » à travers la technologies des puces RFID, dont nous avons déjà largement parlé, qui remplaceront progressivement les codes barres sur les produits manufacturés, mais aussi sur les cartes « sans contact » ou encore les passeports. Le code présent dans la puce donnera accès via internet à des informations dynamiques réactualisées en

[115] www.lexpansion.com 12/07/2006
[116] www.atelier.fr 15/03/2006

permanence sur l'objet en question (informations sur l'origine, le transit, la traçabilité des denrées alimentaires, etc.). Selon Viviane Reding, commissaire européenne à la société de l'information « **la mise en relation de Galileo, du Wi-fi, du RFID et de l'intelligence artificielle va créer une architecture intelligente**. Chaque objet pourra avoir une adresse sur Internet. On se dirige vers une fusion du monde des données et du monde des objets ». Vinton Cerf, l'un des pères fondateurs d'Internet devenu VRP de luxe pour Google renchérit : « Du moment où un équipement possède un identifiant unique (l'étiquette RFID) vous pouvez lui définir un historique. On pourrait utiliser le système des noms de domaine, par exemple en créant une adresse avec le numéro RFID suivi d'un .rfid. Et on stockerait toutes les informations sur le réseau. »[117]. On pourra par exemple suivre un courrier de l'endroit du dépôt jusqu'au destinataire en suivant toutes les étapes de son cheminement. Ainsi, depuis son terminal mobile connecté, on pourra à peu près tout savoir quant à la localisation et aux caractéristiques d'un produit ou service quel qu'il soit et sur toute la planète. Ca devient terrifiant quand on pense aux applications sur les êtres humains. On pouvait déjà géolocaliser un individu grâce à son téléphone portable. La puissance du rendu 3D de Google Earth nous permettra pratiquement de le voir évoluer dans son environnement. Les utilisations paraissent ainsi infinies dans la quête du marché de la vie privée…

La route en 3D pour mieux s'y retrouver

L'état du trafic est symbolisé par des zones de congestion oranges et des zones libres vertes.

[117] www.01net.com 10/03/2006

Dans cette course à l'information sur-matérialisée dans les disques durs de la planète (alors qu'on parle à l'inverse couramment aujourd'hui de la dématérialisation de l'information), le phénomène Wikipédia, cette encyclopédie planétaire est un véritable rouleau compresseur en action : elle existe en 50 langues, comprend 2,5 millions d'articles et s'enrichit de 4000 articles par jour ! N'importe qui et de manière anonyme peut s'il le désire modifier à sa guise n'importe quel entrée. Pas de cooptation, pas de contrôle, pas de validation. C'est le summum du principe libertaire sous jacent à la communauté du logiciel libre. Selon Luc Fayard[118], « les wikipédiens (ceux qui se sont inscrits comme auteurs potentiels) ont l'ambition de développer le meilleur modèle de partage de connaissance du monde…la « connaissance » façon wiki est le rabotage systématique de toutes les idées originales ou dérangeantes. Elle ne peut produire qu'un PPCM (plus petit commun multiple) de l'intelligence, un consensus mou sur lequel plus personne n'aura envie de discuter ».
Mais finalement peu importe les points de vue conflictuels, car on en revient toujours à une **dictature de la Connaissance et de la Raison**, qui, comme on le verra en conclusion vise à s'immiscer de partout (et même « physiquement » notamment par l'intermédiaire des technologies Wi-fi). Et qui, dans nos vies quotidiennes, nous empêche de voir et nous font oublier que des alternatives et un nouveau paradigme sont possibles. La virtualisation du **monde** donne l'impression que celui-ci n'est qu'une **masse quasi-infinie de connaissances** écrites dans des mémoires informatiques de plus en plus petites. Et que les solutions à tous nos problèmes ne viendront que d'actions découlant du cortex rationnel humain, héritage de *l'homo sapiens.*
Les grandes Traditions nous le font pourtant bien pressentir : la Connaissance est utile et elle a déjà beaucoup aidé l'humanité ; cependant **elle est subordonnée à l'Amour**. L'une découle de l'autre et vouloir transgresser les lois de l'Univers nous expose à de grandes difficultés. L'intelligence du cœur, après des siècles de guerre et d'atrocités au nom de la raison et de la Connaissance, paraît être une voie bien peu explorée, ou en tout cas bien mal récompensée pendant ces longues périodes de sacrifice. Mais les temps changent et le succès de notre évolution individuelle et collective pourrait bien passer par un retour en douceur de l'Amour au sens noble et méconnu du terme. Et pour en prendre conscience et se faire son opinion, rien ne vaut sa propre expérience individuelle.

3-10 La maison et l'homme de demain

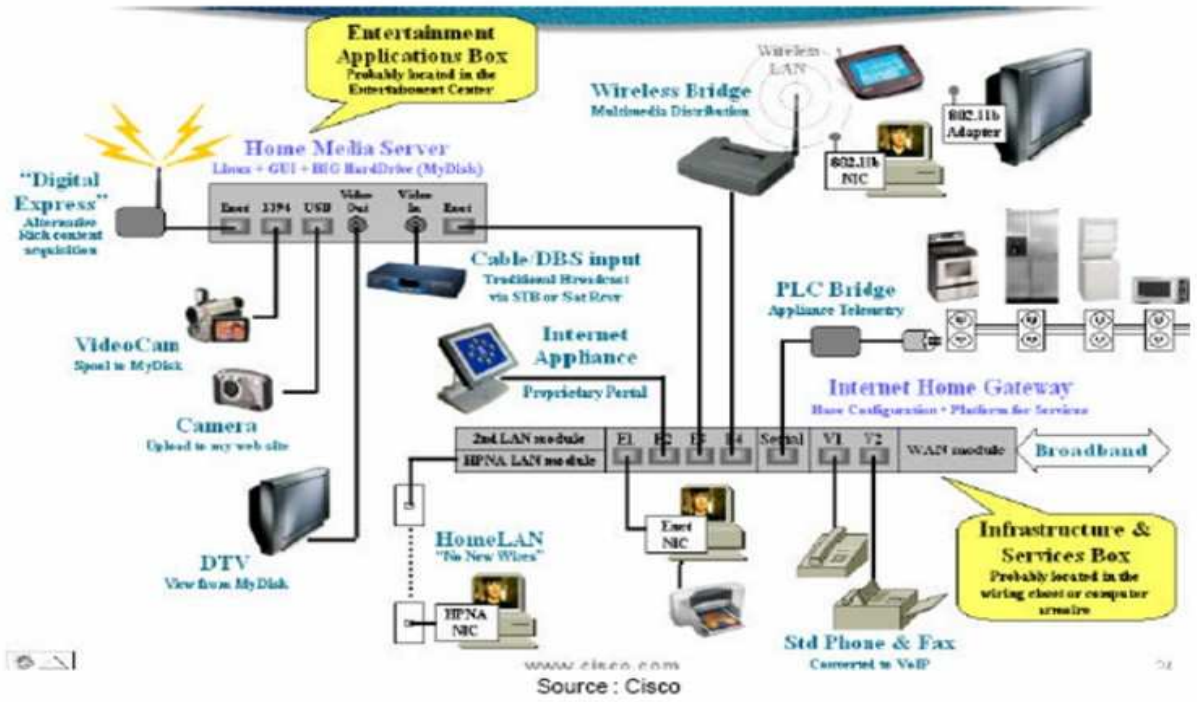
« Chacun a droit au respect de sa vie privée… » Art. 9 du Code Civil

«Une belle journée commence. AIBO, votre cyberchien vous réveille en douceur. Muni de votre télécommande domotique, vous ouvrez les volets, réglez le chauffage et mettez la musique. La haute technologie est omniprésente, et les robots envahissent notre quotidien, pour notre bien. Ils aspirent, repassent, tondent la pelouse, lavent le linge et nous amusent. En clair ils sont là pour nous faciliter la vie. Dans la maison tout devient interactif. Le réfrigérateur se connecte à Internet pour faire les courses en ligne. Equipé d'un capteur de puces RFID, il contrôle en

[118] Dans une interwiew des Echos, 29 nov. 2005

permanence la présence des aliments que vous jugez essentiels. Il suggère des recettes en fonction de ce qu'il contient, et son écran intégré diffuse votre feuilleton favori. Les machines à laver adaptent leurs cycles de lavage au degré de salissure des vêtements ou de la vaisselle. Quant à la télévision et à l'ordinateur, ils communiquent entre eux – sans fil -, deviennent des éléments décoratifs de la maison, et surtout de véritables centres multimédia, compacts et design… »

Figure 2 : Exemple d'application domotique : la maison connectée selon Cisco



Source : Cisco

Ce document de « Cisco » date un peu (à l'heure d'aujourd'hui, tous les fils auraient été remplacés par des connexions Wifi), mais reste cependant très pertinent pour envisager notre quotidien si la voie technologique est poursuivie[119].
Tous les appareils de la maison seront en fait connectés par un réseau local, lui-même connecté au réseau des réseaux. Toutes les informations aboutissent aux différents écrans et haut-parleurs du foyer : dalles plasma, moniteurs d'ordinateurs, afficheurs des téléphones portables, kits d'enceintes home cinéma, écouteurs des baladeurs numériques....sont leur destination finale. La maison, la douce « home sweet home » des américains, à été considérée à presque toutes les époques comme un lieu de ressourcement, où l'on pouvait revenir à ses racines, en famille, partager ensemble des expériences vécues en toute intimité…etc. Or dans un futur proche celle-ci pourrait avoir tous les attributs d'un « lieu public » puisque Internet y pénètre par toutes les ouvertures et que la « confidentialité » n'y est plus assurée. Chaque appareil de la maison (+ tous les appareils nomades comme les téléphones portables, les agendas…), voire chaque produit (grâce aux puces RFID) aura sa propre « adresse Internet », reconnaissable sur le réseau. On appelle cela déjà

[119] voir aussi www.digitalworld.fr/maison-numérique et la vie selon Microsoft : www.microsoft.com/france/chezvous//mamaisonnumerique/defaut.mspx

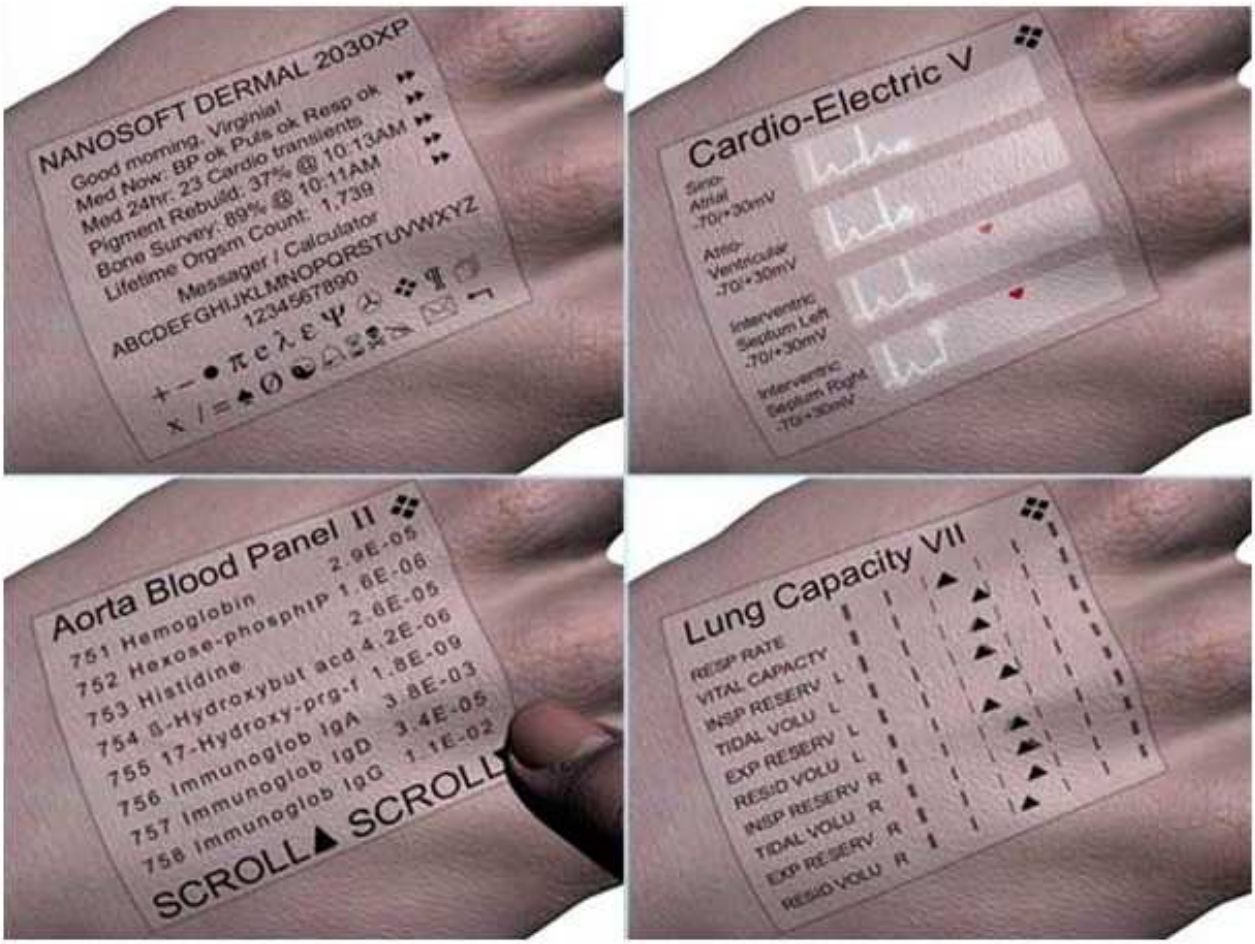
« l'internet des objets ». C'est le protocole IPv6 que nous avons déjà évoqué qui permettra cette « prouesse ». « Dans le futur, les étiquettes RFID ne seront plus limitées aux magasins, on en trouvera aussi dans les domiciles », expliquait un représentant de la société Métro sur son stand durant le grand salon du CeBIT à Hanovre en 2006. Par exemple, le frigo pourra avertir son propriétaire qu'il n'y a plus de beurre ou de yaourts après avoir détecté l'absence d'étiquette RFID. Un four à micro ondes pourra aussi, avec ce système, dès qu'on approche un plat surgelé, en donner le temps de cuisson. « **Dans 3, 4, ou 5 ans**, les prix des étiquettes auront suffisamment baissé pour qu'on arrive à **mettre du RFID sur tous les produits** » indiquait Zygmunt Mierdorf, le directeur des systèmes d'information de Métro.[120]

Microsoft a déjà, avec des partenaires, lancé sur le marché des PC estampillés « Media Center » destinés à devenir le « cœur » de la maison numérique et pouvant communiquer et commander, sans recours à des câbles (ce qui devrait faciliter son adoption), tous les autres appareils électroniques. Tel un chef d'orchestre, le PC media center vous permet d'accéder à l'ensemble des contenus multimédias numériques depuis un menu unique, via une simple télécommande.
Le revers de la médaille, c'est qu'en théorie, « on » pourra savoir, à n'importe quelle heure de la journée, ce qui s'est passé dans le giron familial et ce qui est en train de s'y dérouler en direct : la télé-réalité est en passe de rentrer maintenant chez les particuliers !
C'est une proposition à laquelle chacun peut désormais réfléchir et qui peut être déclinée. Là encore, le choix, comme dans beaucoup d'autres domaines aujourd'hui, nous est offert. A chacun de décider.

Dernière anecdote insolite qui nous vient tout droit de Londres : la puce qui espionne dans les poubelles. A Croydon dans le sud de la capitale, les autorités ont décidé de fournir aux habitants de nouvelles poubelles à roulettes, équipées de puces. Leur mission : espionner littéralement le contenu des poubelles pour vérifier que les citoyens trient correctement leurs déchets. A défaut, ils recevront la visite d'un conseiller qui les informera sur la conduite à tenir pour que le recyclage se fasse mieux. Questions : à quand la brosse à dents intelligente rendue obligatoire par les autorités sanitaires ? Le réveil matin qui vérifie que vous ne vous êtes pas levé trop tard ce matin ? La puce qui contrôle votre consommation d'eau et vous dénonce au voisinage si celle-ci est trop élevée [121] ?

Le mot savant pour parler de la maison intelligente est **la domotique**. C'est l'ensemble des technologies de pilotage de la maison elle-même et de ses appareils électroménagers.

[120] www.01net.com 10/03/2006
[121] www.atelier.fr 16/02/2005



(Source : Gina Miller et Robert A. Freitas Jr)

Mais la maison n'est pas le seul terrain d'expérimentation. Des projets similaires, notamment grâce à l'émergence des « nanotechnologies » sont sur le point de voir le jour chez l'être humain. Qui pourra s'en insurger s'il s'agit de sa santé, que l'on veut protéger (même) à tout prix. Ainsi, grâce à des implants sur le dos de sa main (cf photos) agencés sous forme d'écran de contrôle, l'individu pourra s'informer de son état de santé en détail et surtout en temps réel. « Cette technique appelée « programmable dermal display » consiste à implanter une population de 3 milliards de robot-pixels sur une surface de 6X5cm, et dont les photons émis par ces pixels produiraient une image à la surface de la peau. Cet écran, qui pourrait être activé ou désactivé par un tapotement du doigt sur la main, serait programmé pour afficher nombre d'informations, obtenues via des capteurs, par exemple des données médicales comme la concentration d'oxygène dans le sang, le taux de glucose, la courbe des battements du cœur, la tension artérielle ou toute donnée physiologique importante. » [122] Autre « progrès technologique », la miniaturisation aidant, les puces électroniques commencent à être utilisées pour établir des diagnostics médicaux. La pillcam, d'ores et déjà vendue par Given Imaging renferme une mini webcam et joue le rôle d'un endoscope. Minuscule (11 X 26 mm pour un poids de 4g), elle voyage à travers le corps en transmettant ses images sur des capteurs enregistreurs qui ont

[122] www.automatesintelligents.com

été préalablement placés au niveau de la ceinture du patient. Huit heures plus tard, une fois la pilule extraite par les voies naturelles, le patient pourra retourner voir son médecin avec ses « radios »[123].

Ce sera alors la grande victoire de la médecine (technicienne) allopathique, qui pourra ainsi prescrire aux vues de ces analyses. On peut voir là une caricature assez bien faite des médecines dites « traditionnelles » (c'est-à-dire ce qu'on a qualifié pour beaucoup d'entre elles en Occident de médecines dites « douces » ou « alternatives ») qui prennent l'être humain dans sa globalité, et non en le « saucissonnant » en petits morceaux. Ce qu'il y a d'intéressant, c'est que ces médecines basent leur diagnostic et aussi souvent leur intervention sur un organe qui donne à lui seul une vision d'ensemble du corps. On pourrait prendre pour exemple l'iridologie (avec pour base l'observation de l'iris de l'œil), la réflexologie palmaire ou plantaire (mains ou pieds), l'ostéopathie (le dos)…etc. Ainsi, par exemple, cette nano-main, c'est-à-dire nos technologies, pourraient avoir pour ambition d' « imiter » l'extraordinaire densité d'information que contiennent à elles seules certaines parties de notre corps. Là aussi **la question du choix nous** est encore posée. A qui allons nous faire confiance : à la matière et ces avancées technologiques fulgurantes ou bien en l'homme et en ce qui le transcende, par la reconnaissance de l'infini perfection de nos corps physiques ? Ou peut-être encore à une synthèse de ces deux points de vue ?

Les nanotechnologies sont l'ensemble des techniques visant à produire, manipuler et mettre en œuvre des objets et des matériaux à l'échelle du nanomètre, soit 10 puissance -9 mètre. Plus précisément, on considère qu'une technique relève des nanotechnologies si elle manipule des objets dont la taille se situe entre 1 et 100 nanomètres. Il s'agit donc de manipuler directement des molécules voire des atomes. Richard Feynman est considéré comme le fondateur de cette discipline et prendra pour objectif l'écriture de l'intégralité des 24 volumes de l'Encyclopaedia Britannica sur une tête d'épingle. (Source Wikipedia).

[123] www.01net.com 26/10/2005

4 Vers une dictature « acceptée »

« Wake me up, Wake me up
S'il te plaît réveille moi. »
Mathieu Mendes

4-1 L'égo-démocratie : le pouvoir en apparence laissé aux citoyens ou l'hyper individualisme

Dites-leur ce qu'ils veulent entendre.
Lénine

Le temps des Robespierre et des Danton est définitivement révolu. L'histoire ne répète pas ses apparences. La guillotine et sa barbarie sur la place publique sont de l'histoire ancienne car leur matérialisation dans l'un de nos pays démocratiques provoquerait un tollé général. En revanche, un scénario de terreur, beaucoup plus subtil et masqué est peut être en train de subrepticement se mettre en place sur la planète. Sous couvert de démocratie totale, de lutte contre l'ennemi (aujourd'hui les terroristes, demain ceux qui ne rentrent pas dans la norme de l'homo oeconomicus moyen), la loi du marché pourrait avoir le dernier mot.

Les apparences sont trompeuses. Qui voudrait se révolter contre une démocratie et un état providence ? La « sécurité » matérielle de l'individu pourra être au cœur des arguments pour justifier le contrôle. En apparence, et grâce au vote Internet notamment, les individus auront l'impression d'exercer leur pouvoir. Déjà, le député UMP des Vosges, François Vannson constatait en mai 2006 que « l'expression du scrutin et le processus de vote en France paraissent désuets », (...) et qu'ils « n'ont pratiquement pas évolué depuis la Troisième République »[124]. Il a donc décidé de présenter une proposition de loi « tendant à autoriser le vote par Internet », notamment pour faciliter le dépouillement, mieux impliquer les jeunes, et renouveler, avec l'e-vote, la vie politique. Mais, y aura-t-il toutes les sécurités pour rendre le vote totalement anonyme ? De plus, influencés par le consensus médiatique, la liberté de choix des électeurs ne sera-t-elle pas entravée ?

En effet, revenons un instant sur la définition du mot liberté. Celle ci a en fait deux sens : dans l'action il faut distinguer le temps de la décision, et ensuite le temps de l'exécution. Or ce temps de la décision ou « liberté intérieure » est en fait de plus en plus compromis. Il l'est déjà, et le sera encore plus par le déferlement médiatique et publicitaire qui nous empêche de se fier à notre propre discernement. Mais avec l'apparition des technologies qui permettent à l'Internaute de devenir un véritable « émetteur » sur le réseau, ce sera probablement pire. On pourra, en connaissant ses préférences et habitudes guider un individu là où on a envie de le mener. **L'amoindrissement de cette liberté intérieure condamne à terme aussi la liberté extérieure, c'est-à-dire la liberté d'exécution**. En fait la liberté d'action devient

[124] www.01net.com 11/05/2006

dérisoire si la liberté de décision ne nous appartient plus.

Dans un passionnant article[125] sur les partisans et détracteurs du fameux « bracelet électronique », Georges Fenech, député UMP et auteur d'un rapport parlementaire sur le sujet confie au débateur : « Le travail que j'ai effectué avec les responsables de la chancellerie, tout ce que nous avons entendu, à l'étranger et ici va dans le même sens : au-delà de 6 mois, 1 an, 2 ans maximum la personne ne tient plus. La nature humaine est ainsi, **on ne peut pas rester sous surveillance en permanence**, avec le risque constant d'enfreindre ses obligations. Psychologiquement, le condamné ne peut plus se soumettre ». Voilà qui devrait nous inspirer quant aux directions collectives à prendre : le climat de **paranoïa réel** qu'inspire déjà le bracelet électronique aux prisonniers pourrait se propager demain, qui sait, si les tendances au tout-sécuritaire s'accéléraient, aux porteurs de téléphones portables, de puces RFID sous cutanées… Effectivement, aucun être humain n'est capable psychologiquement de supporter un tel étau mental sur le moyen terme : personne n'est fait pour vivre en esclavage. Et pourtant : le Garde des Sceaux Pascal Clément a assisté le 1er août 2006 à la première distribution d'un bracelet électronique d'un nouveau type destiné aux détenus sous liberté conditionnelle pour leur permettre d'être « mobiles » et non plus assignés à domicile comme c'était le cas auparavant. Ce qui peut sembler en apparence comme un « progrès » est en tout cas plus certainement une fabuleuse opportunité pour tester des technologies poussées de surveillance. Le contrôle de ce dispositif en France est confié à une société privée. Les mouvements du sujet peuvent être suivis en temps réel grâce à un système GPS de positionnement par satellite. En cas de non-respect des zones d'assignation par le détenu, la société privée prévient immédiatement l'administration pénitentiaire[126].

L'arrivée des très nombreuses innovations technologiques que nous vivons actuellement va-elle plutôt contribuer à m'aliéner, ou bien sera-elle source de mon épanouissement en étant considérée simplement comme un « moyen » ? On serait bien entendu susceptible de pencher pour cette seconde proposition. Pourtant, dans une société ou l'hyper individualisme devient la règle, on peut très facilement se faire aveugler. En témoigne les derniers « joujous » technologiques, qui même s'ils comportent cette dualité (ce ne sont que des « outils » laissés à leur bonne ou mauvaise utilisation par leurs usagers), pourraient, orientés par les pressions politiques, médiatiques, économiques et pragmatiques, se voir utiliser pour servir les fins les plus inavouables. Exemple de cet hyper individualisme technologique, qui n'est aujourd'hui qu'à l'état de possibilité mais qui pourrait bien prochainement se manifester : la clé universelle. Son ancêtre pourrait être la clé USB actuelle, et elle pourrait rapidement prendre la forme d'une simple empreinte biométrique (empreinte digitale par exemple). Ce serait en sorte la fusion du **marketing one to one**, de **la technologie** et de **l'individu-roi**.

Celui ci a le désir de toujours emmener avec lui son « **environnement** », c'est-à-dire tous les objets et personnes avec qui il aime à être. Ce projet, impossible à matérialiser dans notre monde de tous les jours, est en passe d'être réalisé grâce au TIC sur le réseau Internet. Les exemples sont déjà nombreux : parmi ceux-ci, l'internaute qui branche son ordinateur et qui peut d'un clic de souris sur Msn tchater

[125] L'Express du 9/02/2006
[126] www.01net.com 01/08/2006

avec ses proches et personnaliser son environnement de travail. Microsoft propose ainsi à ses membres de se créer une page web « ultra personnalisée » très facilement qui à pour nom « mon msn »[127] (voir en exemple la page ci-dessous) C'est ainsi que sur une seul page web, l'internaute, d'où qu'il se trouve (chez des amis, d'un cybercafé…) peut avoir accès à tout son environnement : son carnet d'adresses (et les coordonnées de tous ses proches), les informations web qu'il préfère (en effet il peut s'abonner uniquement aux « news » qui l'intéressent), son horoscope, les performances de toutes ses valeurs boursières, ses sites web préférés, etc.

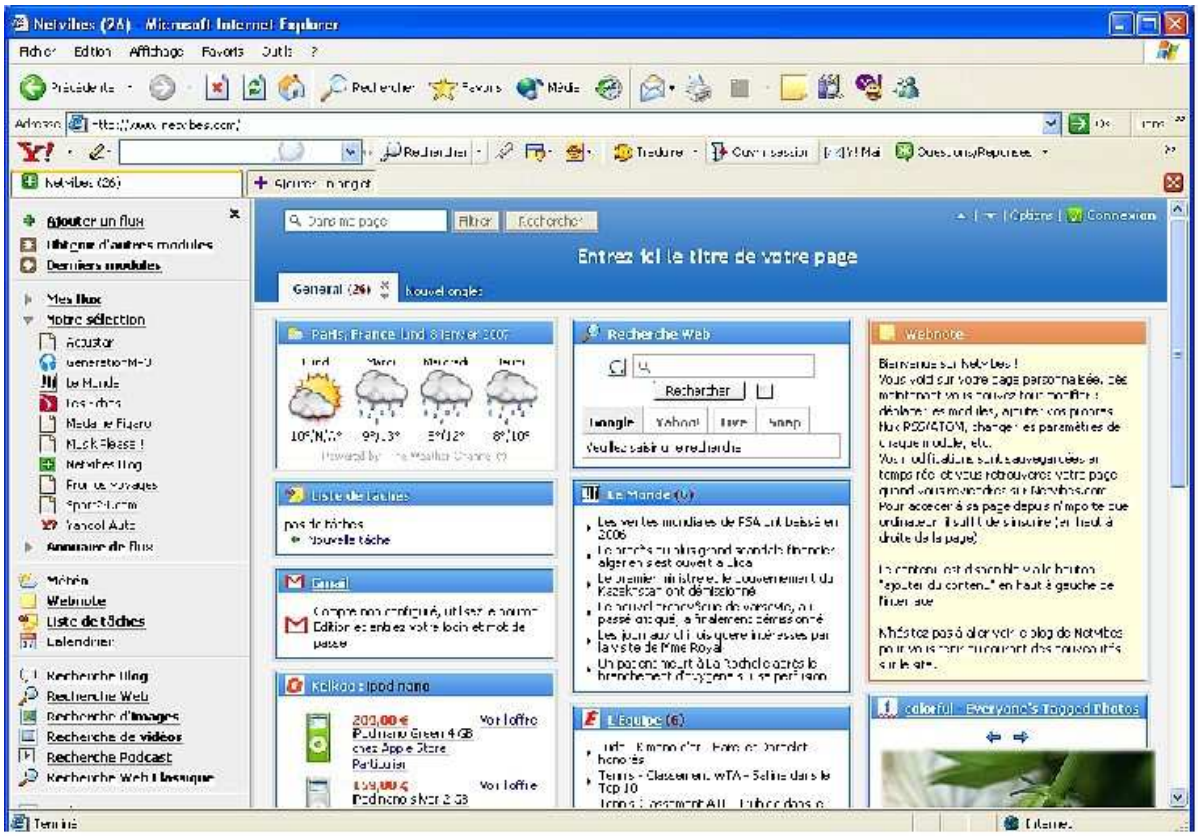
Ainsi, chacun pourra avoir la possibilité de se constituer son « univers », son « environnement » sur un serveur (msn, google…) du réseau. Ce qui signifie que les données personnelles vont être déposées, par son détenteur lui même, à la disposition de grandes firmes privées, et qui sait ensuite, aux yeux de tous. En réalité, n'importe qui, de n'importe où et n'importe quand peut déjà accéder à son environnement personnel. Peut-être avant que d'autres n'y parviennent également.

C'est ce que certains appellent la liberté…

C'est bien l'hyper individualisme qui pousse à cette apparente victoire de la liberté en faisant apparaître au grand jour au monde entier sa vie privée. L'invasion, et le succès rencontré, de la télé-réalité sur nos petits écrans, est tout à fait symptomatique de cette tendance qui ne fait que démarrer et susceptible d'envahir notre quotidien. Les émissions de télé-réalités estampillées comme telles invitent le téléspectateur à « voter » pour son candidat préféré, ou pire, à montrer du doigt ceux qui ne doivent pas continuer l'aventure. Ce sont les premiers pas du cyber-citoyen-justicier qui à bout d'emails et de SMS **dénonce, ou en tout cas juge** son alter ego. C'est la victoire absolue de notre démocratie qui en apparence se construit par les appréciations de ses citoyens.

Toujours pour de soi-disant bonnes raisons, Microsoft UK, allié à l'organisme gouvernemental anglais de protection de l'enfant sur Internet Child Exploitation and Online Protection à récemment dévoilé son dispositif d'alerte dans les versions britanniques de Msn Messenger et Windows live Messenger en cas de propositions de nature sexuelle. Il s'agit d'une icône sur la partie gauche de l'interface. L'icône *"Report abuse"* permet d'alerter, en un clic de souris, en ligne la police britannique dès que l'internaute estime être victime de propositions indécentes. Il est à parier que d'autres initiatives de prévention des abus en ligne devraient voir le jour à l'avenir sur ces nouveaux outils de communication[128], d'autant plus si elles sont cautionnées par des ONG ou autres organisme **luttant contre** les fléaux de la société… peut être les premiers pas vers un réseau où l'on ne fera bientôt plus confiance à personne.

[127] Voir aussi des sites comme www.netvibes.com ou http://fr.my.yahoo.com , leaders dans ce domaine de l'ultra personnalisation technologique.
[128] www.vnunet.fr 24/08/2006


Entrez ici le titre de votre page
Ajouter un flux
Mes flux
Votre sélection
Recherche Web
Webnote
Liste de tâches
Gmail
Calendrier


Bienvenue
Today on MSN
From Bleak House to Beautiful
Les prévisions météo
Bourse
Ajouter des modules
MSNBC Front Page news
Mes liens favoris
MSNBC local news
Outils de Communication MSN
Votre horoscope au quotidien
Boîte de réception MSN Hotmail

Déjà, l'apparition des auditions du juge Burgaud retransmises en direct à la télévision en Février 2006, dans cette malheureuse affaire de pédophilie, nous montre l'appétit de notre époque pour ce genre de phénomène et les dérives que ce système pourrait apporter. Ces auditions n'étaient-elles pas perçues comme un artefact de procès pour le citoyen où celui ci aurait bien aimé intervenir pour rendre lui-même justice ? Et tourner ainsi au pugilat.
L'information et la vérité sont, on le sait, manipulables à souhait, et ce d'autant plus lorsqu'il s'agit d'images télévisées. On peut facilement créer de toutes pièces un bouc émissaire et le faire ainsi lyncher sur la place publique. Dans ces conditions, est-ce vraiment un progrès démocratique que de vouloir remettre à un citoyen tout puissant des pouvoirs aussi étendus ?

Dans le même esprit du « citoyen justicier », et dans une rhétorique que nous commençons désormais à bien connaître, les délinquants sexuels des 50 Etats américains sont maintenant répertoriés sur un site *(*www.nsopr.gov) qui permet de consulter gratuitement leurs fiches en faisant une simple recherche par nom, ville, Etat ou code postal[129]. On y trouve, pour plus de 500.000 personnes enregistrées, leurs noms, les dates et le détail de leurs condamnations, et bien souvent la photo. Le plus incroyable reste cependant que l'on puisse consulter leur adresse actuelle, et voir le type de véhicule qu'ils conduisent. Ce site permettrait de satisfaire la curiosité « des parents et des citoyens inquiets », a indiqué le département de la Justice américaine dans un communiqué. En avril 2006, dans le Maine (nord-est) un jeune homme de 20 ans avait tué deux anciens délinquants sexuels dont il avait trouvé les noms sur ce fichier. Le jeune homme s'était suicidé juste avant son arrestation… Courant novembre 2006, au Royaume Uni, la Police britannique a pour la première fois lancé un avis de recherche sur un nouveau site web lancé à l'échelle nationale, concernant cette fois ci 5 pédophiles condamnés, mais ayant omis de signaler leur déplacement. Nom, photo, caractéristiques physiques (cicatrice, par exemple), zone géographique de prédilection, éventuelles fausses identités et surnoms : toutes les informations les concernant sont désormais en ligne et accessibles à tous sur le site du Centre child exploitation and online protection ! Et avec cet appel national**, se réjouit (!!!) son président**, Jim Gamble, **"il n'y aura plus d'endroit où se cacher".**
Déjà le site Internet « Crimestoppers most wanted » qui traque les plus dangereux criminels du pays en fuite à inauguré ses 1 an d'existence et à reçu déjà de la part de la population plus de 40 millions de pistes[130] ! Vous avez dit délateurs ?

Le plus inquiétant aujourd'hui est qu'une partie très significative des individus, et encore plus dans la jeune génération, rêve d'être exposée (phénomène télé-réalité, blogs…), ce qui suggère qu'une information sur chaque personne sera peut-être un jour facilement disponible pour tous, et ce d'autant plus que chaque concerné contribuera à la « mise à jour » de son image.

A ce titre, la télévision (et Internet, qui vont probablement converger d'ici peu vers un média unique), peut être vu comme le plus grand inspirateur des foules. Toute personne qui se rend dans des concerts retransmis ou des émissions de télévision peut en témoigner : quitte à écraser littéralement les autres, une part importante du public est prête à tout pour montrer sa jolie frimousse sur les écrans aux yeux et vue de tous.

[129] La vie du Net, 04/07/2006
[130] www.lci.fr 18/11/2006

Marketing One to One : Vision d'un marketing totalitaire. Propose en effet de traiter des millions, voire des dizaines de millions de consommateurs en donnant à chacun l'impression qu'il est traité individuellement, comme s'il était seul au monde. Les marques qui le pratiquent peuvent ainsi à nouveau développer les valeurs de proximité et d'intimité qu'elles pratiquaient à l'origine avec leurs clients quand ils étaient peu nombreux.

4-2 Vers un encouragement du contrôle et de la délation

« On n'peut pas tomber plus bas »

Zazie, « Rodéo »

Economistes et juristes américains du Pew Project, ont réalisé en 2004 une étude sur les craintes actuelles en relation à Internet auprès d´industriels américains. En ressort une réelle préoccupation vis-à-vis de la sécurité, avec 60% des interrogés prévoyant une attaque massive globale du système Internet, un Pearl Harbour digital d´ici 2016. En conséquence, l´étude prévoit un renforcement de la sécurité, envisagé par 60% des interviewés.

L'opinion publique des Occidentaux dérive en effet de plus en plus vers une demande de renforcement de la sécurisation des systèmes d'information. Par média de masse interposé qui forcent les opinions, la population continue donc de tisser sa propre toile dans laquelle, peut être, elle se fera elle-même prendre au piège.

Pourtant, des expériences de contrôle, notamment au travail, ont déjà eu lieu dans l'histoire. En avons-nous tiré les conséquences ? Le 22 germinal an XI (12/4/1803), sous Napoléon, une loi instaurait le livret d'ouvrier en France et selon l'arrêté du 9 frimaire an XII (1/12/1803) puis de la loi du 14 mai 1851, tous les ouvriers de l'un et l'autre sexe attachés aux manufactures, fabriques, usines, mines, minières, carrières, chantiers, ateliers et autres établissements industriels ou travaillant chez eux pour un ou plusieurs patrons devaient s'en procurer auprès du maire. **L'ouvrier ne pouvait travailler sans le présenter**, ce livret devait énoncer : le nom, prénom de l'ouvrier, son âge, le lieu de sa naissance, son signalement et sa profession. Il constituait un moyen de pression de la part des fabricants ; en cas de conflit avec l'ouvrier, son livret ne lui était pas rendu, empêchant toute embauche postérieure. L'ouvrier ne pouvait quitter un employeur qu'après que celui-ci eut signé un quitus sur le livret, la signature devant être certifiée par une autorité, et ne pouvait quitter une commune sans le visa du Maire ou de la Gendarmerie, avec indication du lieu de destination. L'ouvrier était tenu de présenter son livret à toute réquisition des agents de l'autorité sinon il était considéré comme vagabond et **pouvait être arrêté et puni comme tel.** La perte du livret interdisait aussi de travailler et de quitter la commune du dernier domicile.

Un exemple d'aujourd'hui, cette mésaventure arrivée à une journaliste américaine travaillant en France qui devait un jour comprendre pourquoi elle ne trouvait plus de travail aux Etats-Unis : son dossier personnel accessible par le Net indiquait tous ses changements d'emplois, d'adresses, son divorce, ses mésaventures avec les tribunaux ou les banques pour des affaires vénielles.

Il faut dire qu'aux Etats-Unis, la loi Sarbanes-Oxley, adoptée en 2002 dans le sillage du scandale d'Enron, contraint les entreprises côtées à mettre à disposition de leurs salariés un numéro vert ou une adresse Internet où ils peuvent dénoncer discrètement comportements contraires à la déontologie et actes frauduleux. Une loi qui s'applique aussi aux filliales françaises de ces groupes. D'ailleurs, déjà en 1997 une enquête de l'Université de l'Illinois a révélé qu'un quart des cinq cents plus grands groupes américains livraient des informations sur leurs salariés aux agences gouvernementales.[131] D'autres part, d'après une étude de Proofpoint[132], plus du tiers (36,1%) des grandes entreprises américaines ont des employés chargés de lire ou d'analyser les courriels sortants afin « de s'assurer qu'ils ne contiennent pas de renseignements pouvant constituer une menace. » Et que 26,5% d'entre elles avaient l'intention d'embaucher des salariés chargés d'épier les messages. En outre, entre mi 2004 et mi 2005, 27% des firmes interrogées auraient congédié un employé pour violation de la politique interne relative au courrier électronique. Une autre étude[133] révèle que 5% des entreprises sondées utilisent le GPS pour suivre à distance les déplacements d'un salarié via son téléphone portable. De plus, 36% des employeurs scrutent « le contenu, les saisies claviers (cf. Keylogger) et le temps passé sur ce dernier ». 50% enregistrent et conservent pour examen les fichiers informatiques de leurs salariés. La vidéo surveillance fait aussi outre atlantique de plus en plus d'adeptes pour « suivre les performances des salariés au travail » : 10% des sociétés réalisent des enregistrements de certaines catégories de leur personnel, et 6% de l'ensemble de leur effectif[134].

Outre Manche, la BSA (Business Software Alliance), consortium d'éditeurs voué à la lutte contre le piratage informatique a carrément décider de récompenser avec largesse la délation en offrant aux salariés qui dénoncent leur employeur utilisant des logiciels pirates la coquette somme de 20.000 livres sterling. Et ça fonctionne. En 2005, le consortium a mené plus de 420 investigations suite à ce service de délation[135] !

Et la France dans tout cela ? Il faut voir que quelques évolutions récentes du droit français encouragent aussi la dénonciation. La CNIL doit créer un régime d'autorisation simplifié pour les entreprises souhaitant installer ce qui est joliment désigné comme un « dispositif d'alerte éthique » pour le moment limité au domaine comptable et financier. Ces mesures doivent permettre aux salariés de signaler à leur direction des comportements « supposés fautifs » constatés sur le lieu de travail. La Cnil insiste sur le fait qu'il faudra que les émetteurs d'alerte s'identifient, ce afin d'éviter tout « dérapage vers la délation et la dénonciation calomnieuse »[136] Dans le même esprit, en entreprise, la Cnil à déjà autorisé, en restreignant (pour prévenir les dérives) à 4 cas de figure, la géolocalisation par GSM/GPS des véhicules des

[131] Tous fichés (Jacques Henno)
[132] www.branchez-vous.com 09/06/2005
[133] Réalisée par l'AMA (American Management Association) e l'ePolicy Institute en mai 2005
[134] www.zdnet.fr 19/05/2005
[135] www.latelier 02/05/2006
[136] www.01net.com 15/11/2005

employés[137].

De plus, la loi autorise désormais, sous certaines conditions les témoignages sous X. Les indics de police et de gendarmerie touchent déjà une très officielle rémunération – comme c'est le cas depuis belle lurette pour les « aviseurs » des douanes et du fisc. En légalisant l'infiltration, la loi Perben du 3 mars 2004 a créé des délateurs professionnels. Dans ce cas un officier de police judiciaire se fait bandit, puis dénonce. C'était connu dans les romans policiers et les thrillers américains ; c'est désormais possible en France !

A Chambéry, des travailleurs sociaux ont vu rouge quand l'association qui les emploie a signé avec le conseil général, la police et la gendarmerie un protocole jugé infamant : en vertu de celui-ci, tout éducateur ayant « connaissance de faits constitutifs d'une infraction ou d'une tentative d'infraction pénale » doit avertir sa hiérarchie.

Le nouveau système autour du statut de repenti est aussi intéressant à analyser. « Ces personnes, une fois arrêtées, choisissent de dénoncer leurs complices de la veille pour échapper à la prison ou pour bénéficier des réductions de peine absolument considérable que la loi prévoit », explique Henri Leclerc[138] de la LDH. A condition que les dénonciations soient avérées, sinon nous auront à faire à « une société, qui pour des raisons de sécurité, organise un système qui risque d'envoyer des innocents derrière les barreaux. », comme ce fut le cas en Italie dans certains procès mafieux.

Le rapport de l'Inserm de février 2006 sur les troubles de comportement chez l'enfant avait, lors de sa sortie, marqué l'actualité française. En effet, il s'agit de repérer les signes annonciateurs de la délinquance afin de les prévenir, chez les enfants à partir de 36 mois ! Se dessine ainsi une entreprise de médicalisation de l'enfance supposant que chaque enfant sera désormais accompagné au long de sa vie et de son parcours scolaire d'un dossier médical contenant des informations sur ses « conduites » et ses « comportements ». D'après l'article du Monde[139], « même des personnes obnubilées par le discours sécuritaire ne pourront lire le rapport sans frémir, car il les met elles mêmes et leurs enfants sous surveillance, dans une suspicion généralisée qui réunit futures victimes et futurs criminels dans le même ensemble de la « population ». Le rapport de l'Inserm raisonne très démocratiquement en supposant que tout le monde peut être coupable. La « population » comme telle est à risque, elle est une classe dangereuse potentielle. Et c'est pourquoi elle doit être mise sous surveillance médicale, dans son ensemble et au plus tôt…Mais il faut encore comprendre que les parents appelés à surveiller leurs enfants seront eux même mis sous surveillance par les médecins, ceux-ci étant seul habilités à repérer l'enfant dit difficile ».

Parents à qui l'on délègue également le contrôle de leur progéniture sur Internet via le « contrôle parental » que proposent maintenant tous les fournisseurs d'accès Internet Français. Les parents pourront ainsi utiliser un logiciel de filtrage avec une distinction entre les enfants et les adolescents : pour les premiers le logiciel fonctionne avec une « liste blanche », c'est-à-dire qu'ils ne pourront accéder qu'à certains site limitativement. Pour les adolescents, c'est le concept de liste noire avec des sites dont l'accès est totalement bloqué[140]. Première étape, qui paraît aujourd'hui

[137] www.01net.com 02/05/2006
[138] www.lexpress.fr 04/04/2005
[139] Gérard Wajcman, Le Monde, 4 mars 2006
[140] www.zdnet.fr 16/11/2006

en apparence légitime, d'une formation au contrôle numérique des citoyens entre eux ?

En tous les cas le pas a déjà été engagé pour les enfants, à l'autre bout de la planète, à Honk kong. Pour gagner du temps lors de l'appel et combattre l'absentéisme, une école primaire s'est dotée de lecteurs d'empreintes digitales. Dès qu'ils auront franchi les portes de l'établissement, les élèves glisseront le doigt dans l'un des cinq appareils qui serviront aussi probablement pour la cantine et la bibliothèque. Au Japon, une société de service a commercialisé en octobre 2005 une solution de surveillance via mobiles des écoliers entre leur domicile et l'école. Les parents et les professeurs s'informent de la position des écoliers via un site web spécial, ce dernier servant également de feuille de présence des élèves, ainsi qu'à envoyer des informations aux familles[141].

Mais revenons pour finir quelques instants au cas Français. André Comte Sponville dans une interview[142] tempère les choses en avouant que « les français sont mal à l'aise avec la dénonciation…nous sommes des latins. Nous nous solidarisons plus volontiers avec les fraudeurs[143/144] qu'avec les contrôleurs, avec les arnaqueurs qu'avec la Police. **Nous n'avons pas envie de vivre sous le regard inquisiteur du voisin** ou du collègue de bureau. Enfin nous sommes viscéralement réfractaires à une société de l'ordre moral, dans laquelle chacun de nous serait un dénonciateur en puissance. » **Les Français ne voudraient donc pas d'une république de délateurs** : c'est une très bonne nouvelle, car démocratie faisant, ce sont encore les citoyens qui décident de leur sort aujourd'hui. Espérons qu'ils saisissent le message pour agir fermement en ce sens.

Attardons-nous maintenant sur les projets sécuritaires menés par nos voisins d'outre atlantique, puis européens, avant d'aborder le cas spécifiquement français.

4-3 Les projets délirants américains

« Nous allons connaître les restrictions les plus fortes de notre histoire sur nos libertés »

Sandra Day O'Connor (Juge à la Cour Suprême)

C'est donc bien le 11 septembre qui « a marqué en matière de respect des droits de l'homme aux Etats-Unis une rupture très nette. Au nom de la « juste guerre » contre

[141] L'atelier, 14/10/2005

[142] www.lexpress.fr 04/04/2005

[143] Selon une étude réalisé en 2006 pour l'IDC, avec 47% de logiciels piratés, la France enregistre une hausse de 2 points et se positionne comme le plus mauvais élève de l'Union Européenne.

[144] Pour Jean Dominique Michel, anthropologue, « un système qui éliminerait d'emblé toute fraude serait par définition un système totalitaire ».

le terrorisme beaucoup de transgressions ont soudain été permises. En témoigne l'ouragan de mesures liberticides adoptées. Dès le lendemain, une justice d'exception s'y mettait en place. Le ministre de la justice, M.John Ashcroft, faisait adopter une loi antiterroriste dite « loi patriotique », le Patriot Act, qui permet aux autorités d'arrêter des suspects pour un temps quasi indéfini, de les déporter, de les faire incarcérer dans des cellules d'isolement, de faire surveiller leur courrier, leur conversations téléphoniques, leur communication via Internet, et de faire fouiller leur domicile **sans autorisation judiciaire**. »[145] C'est en effet la section 215 du Patriot Act qui est la plus critiquée : le FBI peut obliger toute personne physique ou morale à lui remettre tous les documents dont il estime avoir besoin dans le cadre d'une enquête de lutte contre le terrorisme. Cela signifie que n'importe quel organisme peut être amené à communiquer aux agents fédéraux ses fichiers informatiques. Et c'est en décembre 2003 que le Président Georges W. Bush signa un décret autorisant le FBI à se passer de l'avis d'un juge pour réquisitionner les fichiers des organismes financiers[146]. Des responsables du Federal Bureau of Investigation (FBI) sont allés jusqu'à proposer que certains accusés soient extradés vers des pays amis (Maroc, Tunisie, Egypte, Jordanie), où la torture est couramment pratiquée, pour que la police locale puisse les interroger…Le recours à la torture à été ouvertement réclamé dans les colonnes de grands magazines. Sur la chaîne CNN, le commentateur républicain Tucker Carlson a été très explicite : « La torture ce n'est pas bien. Mais le terrorisme c'est pire. **Aussi, dans certaines circonstances, la torture est un moindre mal** »[147] .

Le Patriot Act 2 parle lui aussi de lui-même. Aussi nommé Domestic Security Enhancement Act, il propose un fichage ADN des étrangers soupçonnés de certains délits ou d'Américains soupçonnés de terrorisme.
« Il faut aborder différemment les libertés publiques en temps de guerre » explique le Sénateur Américain républicain Trent Lott. Créé le 20 septembre 2001, le bureau de défense du territoire, premier volet du plan, a pour mission de centraliser le renseignement, de coordonner les efforts et de prendre les mesures nécessaires à la prévention et à l'action contre le terrorisme. Il repose sur une telle concentration des organes répressifs de l'Etat qu'il pourrait devenir une super-agence d'espionnage donnant aux forces armées des pouvoirs de police impressionnants. En somme la nouvelle législation représente l'une des offensives les plus vastes contre les libertés aux Etats-Unis depuis plus d'un demi-siècle. Elle ne procurera vraisemblablement aucune sécurité supplémentaire aux Américains. Mais elle les rendra moins libres.
A tout cela s'ajoute la censure rampante. « Les gens doivent faire attention à ce qu'ils disent et à ce qu'ils font ». Comme l'avait proclamé le Président G.W.Bush à la suite des attentats, « vous êtes avec nous ou avec les terroristes. » Mettre en question les pratiques et les politiques de l'Etat serait devenu un acte antipatriotique. Les dissidents refusant les appels à la guerre, ou ceux qui tentent d'examiner les causes sous-jacentes du 11 septembre, n'ont guerre droit à la parole et sont souvent stigmatisés si d'aventure ils la prennent.

Le 5 janvier 2004 marquait le commencement du programme US-Visit où tous les étrangers se rendant sur le sol américain sont mis en fiches avec photos et

[145] Manière de voir n°71, Obsessions sécuritaires, le Monde Diplomatique, Octobre/Novembre 2003
[146] Tous fichés (Jacques Henno)
[147] Manière de voir n°71, Obsessions sécuritaires, le Monde Diplomatique, Octobre/Novembre 2003

empreintes digitales à l'appui pour une durée officielle d'au moins… soixante-quinze ans. Ainsi certaines informations personnelles seront livrées aux douanes des Etats-Unis par la compagnie aérienne avec laquelle ils s'apprêtent à voyager. Avant même qu'ils entrent dans l'avion, les autorités des Etats-Unis connaîtront leur nom, prénom, âge, adresse, numéro de passeport et de carte de crédit, état de santé, préférences alimentaires (qui peuvent traduire leur religion), voyages précédents, nom et âge des personnes les ayant accompagnés, organisations ayant financé certains déplacements, etc. Le 6 octobre 2006, un accord est reconduit entre l'Europe et les Etats-Unis qui imposent aux compagnies aériennes qui opèrent des vols vers les USA de transmettre 34 types de données différentes sur chaque passager avant chaque embarquement pour, vous l'aurez compris…des raisons de terrorisme. Ces données seront transmises au département de la Sécurité intérieure, qui pourra ensuite les fournir «aux agences chargées de combattre le terrorisme», telles que la CIA ou le FBI, a expliqué Franco Frattini, le commissaire européen à la Justice. La seule concession que l'Europe à obtenu est sur la durée de détention des données : elle ne sera « que » de 3 ans et demi alors que les Etats-Unis réclamaient une durée infinie[148].
Tous ces renseignements seront livrés à un dispositif de filtrage baptisé CAPPS (Computer Assisted Passenger Pre-Screening ou Système assisté par ordinateur de contrôle préventif) pour détecter au départ d'éventuels suspects. En contrôlant l'identité de chaque voyageur et en la croisant avec les informations des services de renseignements policiers, du département d'Etats, du ministère de la justice et des banques, le CAPPS évaluera le degré de dangerosité du passager.
« Le but est d'instaurer un monde plus sur. Il faut être informé sur le risque que représentent les personnes qui pourraient un jour entrer dans notre pays », a affirmé M.James Lee, un responsable de ChoicePoint, l'entreprise qui achète ces fichiers pour les revendre à l'administration des Etats-Unis. Car la loi Américaine interdit de stocker des informations personnelles. Mais pas de commander à une société privée de le faire pour le gouvernement. Ce sous-projet n'est en fait qu'un aspect du très secret programme « surveillance totale » (en américain TIA : Total Information Awareness) dont nous allons parler un peu plus loin.
Mais tout n'en reste pas là avec l'Europe. L'institution financière géante Belge (spécialisé dans les échanges de données informatisées entre institutions financières internationales) dénommée SWIFT, qui gère plus de 11 millions de transactions par jour pour près de 8000 banques dans 200 pays, est accusée par Bruxelles d'avoir violé la législation Européenne en transférant aux Etats-Unis des informations aux mépris des données personnelles. Après les « données passagers » que nous venons d'aborder, une nouvelle fois **le vieux continent n'entend pas de la même oreille que les USA la façon d'aborder la lutte contre le terrorisme, et surtout pas au détriment du respect de la vie privée.** Conjointement, la BCE (la Banque Centrale Européenne) et Swift en appellent à l'ouverture de négociations américano-européennes pour trouver une issue légale au problème[149].

Même si les attentats du 11 septembre 2001 ont accentué la xénophobie, les étrangers ne sont pas les seuls à faire l'objet d'une surveillance accrue. Les citoyens américains n'échappent pas à l'actuelle paranoïa. De nouveaux contrôles, autorisés par le Patriot Act, remettent en question la vie privée, le secret des correspondances et la liberté d'information. L'autorisation de mise sur écoute téléphonique n'est plus

[148] www.zdnet.fr 06/10/2006
[149] www.lemondeinformatique.fr 27/11/2006

requise. Les enquêteurs peuvent accéder aux informations personnelles des citoyens sans mandat de perquisition. Ainsi le FBI demande aux bibliothèques de lui fournir les listes de livres et de sites Internet consultés par leurs abonnés pour tracer un « profil intellectuel » de chaque lecteur...[150]
Et avec le projet Intellipedia, version secrète dévoilé fin 2006 du bien connu Wikipedia (l'encyclopédie libre que tous le monde peut mettre à jour sur Internet), les 16 agences constituant la communauté des services de renseignements américains vont pouvoir « **partager** » leurs informations entre elles. Ce sont les analystes des services de renseignement et d'autres responsables qui ont la charge de contribuer et d'éditer du contenu sur le réseau secret Intelink Web. Ce « wiki » un peu spécial compte déjà 28.000 pages et 3600 collaborateurs inscrits. Les responsables des services de renseignement montrent un tel enthousiasme devant le rendement d'Intellipedia qu'ils prévoient d'en donner l'accès à l'Angleterre, au Canada et à l'Australie. Même la Chine pourrait s'en voir offrir l'accès, pour aider par exemple à produire une estimation de renseignements non-classifiés sur la menace mondiale posée par les maladies infectieuses[151]…

Mais le plus délirant de tous les projets d'espionnage illégaux est celui qu'élabore le Pentagone sous le nom de code Total Information Awareness (TIA), système de surveillance totale des informations. Celui-ci (cf l'excellent livre de Jacques Henno, « Tous fichés », aux Editions Télémaque) consiste ni plus ni moins à mettre en fiche chacun des 6,5 milliards d'individus de la planète en collectant une moyenne de 40 pages d'information et en en confiant le traitement à un superordinateur. « En centralisant, en croisant et en traitant toutes les données personnelles disponibles – paiement par carte, abonnements aux médias, mouvements bancaires, appels téléphoniques, consultations de sites web, courriers électroniques, fichiers policiers, dossiers des assureurs, informations médicales et de la sécurité sociale – le Pentagone compte établir la traçabilité complète de chaque individu »[152]. Mesures totalement démesurées par rapport à l'objectif. Les **Américains croient en la suprématie de la technologie et pensent que c'est le moyen de lutter le plus efficacement contre les menaces terroristes.** Mais à quel prix ! Ce bouclier technologique doit leur permettre, grâce à « l'indexation » systématique des populations de repérer dans cette gigantesque masse d'informations les comportements déviants ou suspects dans les détails les plus intimes de nos vies privées. Et donc de prévenir tous les risques possibles. Comme dans le film de Steven Spielberg, *Minority Report*, les autorités américaines pensent pouvoir ainsi prévenir les crimes avant qu'ils ne soient commis.
Voici ce qu'on est en train de choisir pour nous : « Il y aura moins de vie privée, mais plus de sécurité », estime M.John L.Petersen, président du Arlington Institute, « nous pourrons anticiper le futur grâce à l'interconnexion de toutes les informations vous concernant. Demain, nous saurons tout sur vous. »[153]

L'ex-amiral Poindexter, patron du projet « surveillance totale » veut passer au peigne fin les transactions de toutes sortes. Et comme vous l'avez deviné, toujours pour les mêmes raisons, à savoir la lutte contre le terrorisme. « Il y applique ainsi une

[150] Manière de voir n°71 / Le monde diplomatique / Obsessions sécuritaires / Octobre Novembre 2003.
[151] www.canoe.com 01/11/2006
[152] Manière de voir n°71 / Le monde diplomatique / Obsessions sécuritaires / Octobre Novembre 2003.
[153] Manière de voir n°71 / Le monde diplomatique / Obsessions sécuritaires / Octobre Novembre 2003.

méthode déjà utilisée contre d'autres formes de criminalité, en particulier le blanchiment d'argent sale : identifier les criminels grâce aux messages qu'ils échangent et grâce à leurs transactions commerciales. Selon lui, « ces gens émettent forcément un signal qu'il nous faut capter parmi les autres transactions. C'est comparable à la lutte anti-sous-marine où il faut repérer les submersibles au milieu d'un océan de bruits. » » [154]

Ainsi, selon le magazine USA Today, l'Agence pour la Sécurité National (NSA) aurait surveillé les communications de millions d'Américains et créée une gigantesque base de données, en dehors de tout cadre légal[155]. Ce qui met bien sur mal à l'aise le clan Bush.

Officiellement, la Surveillance Totale ne survit pas longtemps au départ de son concepteur en août 2003 pour cause d'un scandale dont il fut l'épicentre. « Le Sénat et la Chambre des représentants, inquiets des conséquences liberticides du projet y mettent ensuite un terme. Pourtant, il est précisé que les élus n'empêchent pas les services de renseignements américains « d'utiliser des outils de traitements, d'analyse et de partage d'informations dans le cadre de la lutte contre le terrorisme étranger ». Traduction : les agences de renseignements ont interdiction d'utiliser ce qui existait déjà de surveillance totale pour espionner des citoyens américains. Mais pour les autres habitants de la planète elles ont carte blanche. » [156] Surveillance totale a bien l'ambition d'espionner la planète entière…

Et l'histoire n'est pas close puisque l'EFF (Electronic Frontier Fondation) a entamé fin 2006 une poursuite judiciaire contre le Département américain de Justice pour obtenir davantage de renseignements sur une base de données secrète (dénommé IDW pour Investigative Data Warehouse) du FBI contenant des informations personnelles sur des millions d'individus. Cette base de données contiendrait la photo, des éléments biographiques, la localisation physique ainsi que des détails financiers sur des millions d'individus plus ou moins liés aux enquêtes sur le terrorisme. Le FBI a indiqué récemment que l'*Investigative Data Warehouse* contient plus de 560 millions de documents différents et qu'ils peuvent être consultés par 12.000 de ses agents. L'EFF demande aussi à la cour de forcer le FBI à dire si les informations collectées ne concernent que des citoyens américains ou également des citoyens provenant de différents pays[157]. Affaire à suivre…

Cependant les choses avancent et des artistes, notamment, critiquent sérieusement la politique menée par Bush. En janvier 2006, le chanteur Américain Harry Belafonte affirmait que « Bush est un terroriste, ne valant pas mieux que Ben Laden »… « Je crois que le terrorisme est au cœur du programme de notre gouvernement. Quand vous mentez aux Américains, quand vous les trompez, que vous avez conduit nos fils et nos filles sur des terres étrangères pour y être tués et que vous regardez des dizaines de milliers de femmes et d'enfants arabes et de gens innocents tués chaque jour, **prétextant qu'il s'agit de dommages collatéraux**, je pense qu'il y a quelque chose qui ne tourne pas rond chez nos dirigeants »… « **Je pense que ces gens ont perdu toute intégrité morale.** Je pense que ce que nous faisons aux Américains et aux autres peuples dans le monde est immoral ».

Le problème reste que ces mesures sécuritaires, on l'a vu avec le programme US-

[154] Tous fichés (Jacques Henno)
[155] www.zdnet.fr 12/05/2006
[156] Tous fichés (Jacques Henno)
[157] www.branchez-vous.com 18/10/2006

Visit, phénomènes au départ strictement Américains, ont débarqué aujourd'hui dans les autres Etats occidentaux sous la pression de Washington qui commence à « déléguer » ses pouvoirs de Big Brother. Autrement dit les étrangers sont maintenant en passe d'être contrôlés dans leur propre pays. En effet, c'est par exemple à la demande express du Président Bush que les FAI et les opérateurs télécoms devront, en Europe, mettre à la disposition des services de police toutes les données de connexion.

4-4 Une Europe poussée malgré elle ?

« Notre objectif est de traiter toutes les bases de données éparpillées dans le monde comme un seul fichier »

Amiral John Poindexter, Responsable du projet américain « Surveillance totale »

Alors qu'on pouvait croire jusqu'à maintenant à un respect de plus en plus grand de l'homme et de ses libertés dans l'Europe, ses états les plus influents (Royaume Uni, Allemagne Espagne, France…, et bien d'autres comme nous le verrons ensuite) ont depuis 2001 renforcé très largement leurs législations répressives. Peut on croire que la « grande Europe », fondée essentiellement au départ sur des idéaux de paix pour ne plus avoir à revivre les tragédies du passé, se dirigerait ainsi, petit à petit, vers une structure de plus en plus policière ?

L'espace Schengen en Europe est l'exemple type de cette dérive : créé pour assurer la libre circulation des personnes dans l'Union, il est devenu un redoutable instrument de contrôle et de fichage informatique des citoyens.
Le Système d'Information Schengen (SIS), abrité sous haute surveillance à Strasbourg dans une construction classée « anti-terroriste », à déjà enregistré des millions d'informations sur les criminels poursuivis, les étrangers interdits de séjour dans l'Union, les véhicules dérobés, les armes et les suspects à mettre sous contrôle…Il y aurait actuellement 15 millions d'enregistrements[158] (dont 90% concernent des objets et 10% des personnes) et il est prévu d'ici quelques années d'en gérer plus de 35 millions. Car une nouvelle version du SIS, dit « SIS II » est en préparation pour permettre de régir toute l'Europe élargie dès 2007/2008. Ce système dispose d'une structure de gestion centrale (à Strasbourg), et chaque Etat-membre a la charge de réglementer sa propre connexion au SIS. La France par exemple a autorisé des accès à environ 15.000 terminaux d'ordinateurs répartis entre gendarmerie, police nationale, douanes, préfectures, ministères de l'intérieur et des affaires étrangères. En 2004, ce sont près de 35 millions d'interrogation du SIS qui ont été réalisées dans notre pays. L'efficacité et la rapidité du système ont déjà été prouvées : une inscription dans le SIS faite en Allemagne peut être disponible dans les 5 minutes qui suivent en Finlande. En effet il permet en temps réel aux autorités compétentes de disposer des informations introduites dans le système par n'importe lequel des états-membres.
Parallèlement pour les futurs visas européens, même son de musique puisque l'Europe à déjà préparé le « plus grand système biométrique du monde »[159], appelé

[158] www.senat.fr 13/12/2005
[159] www.01net.com 28/04/2006

VIS (Visa Information System). Fin 2006, la Commission a mis en place un nouveau système informatique de visas qui devra collecter, à terme, les empreintes digitales de 70 millions d'individus.
Car en fait à terme, la Commission Européenne envisage l'interopérabilité entre le SIS-II et les autres banques de données existantes dans l'Europe comme justement le VIS pour les visas ou la base de données sur les empreintes digitales des demandeurs d'asile (EURODAC).
Ainsi, par exemple, si des visiteurs étrangers n'ont pas quitté l'Union après la date d'expiration de leurs visas, ceux-ci seront signalés au SIS II / VIS et marqués comme « illégaux » dans toute l'Europe. Autre cible de taille : les militants alter mondialistes définis comme « des personnes potentiellement dangereuses qu'il faudrait empêcher de rejoindre certains rassemblement internationaux »[160].
Et Bruxelles entend donner « le meilleur » des technologies à ces systèmes d'information (et de surveillance ?) : par exemple, le SIS II renforce le dispositif d'identification des personnes grâce au stockage de données biométriques. Ce sont des photographies numériques (scanner facial) et les empreintes digitales qui ont été finalement choisies[161]. Avec le SIS II vous l'aurez compris, cet outil conçu au départ pour la lutte contre la délinquance transfrontalière se transforme en un système d'enquête beaucoup plus poussé. Un plus grand nombre d'autorités pourront avoir de fait accès à des fins d'information policières au sens large, comme par exemple Europol et Eurojust.

Mais c'est avec l'implication des services de renseignements que les objectifs du système Schengen pourraient changer de nature : ceux-ci aimeraient en effet se voir octroyer le droit de rechercher tous types d'informations intéressantes dans cette base de données, ce qui est une visée en contradiction avec l'objectif initial de ces fichiers, qui était de contrôler et d'accompagner la liberté de mouvement des personnes dans l'espace Schengen[162]. Il est difficile de savoir si les services de renseignement de chaque état ont accès à l'ensemble des bases de données du SIS-II ou autres VIS, même si c'est très probable. En témoigne la présidence espagnole de l'UE qui avait, en février 2002, « invité les états participant au SIS à s'entendre sur la simplification des procédures de mise en alerte et renforcer leur coopération sur l'échange d'informations avec les services de sécurité et de renseignement non militaires des Etats membres[163]. »

Si ces plans aboutissent, le SIS sera passé d'un instrument de contrôle des frontières intérieures de l'Union à un outil pratiquement sans limites d'investigation et de police.

De plus il faut voir qu'un accord de coopération judiciaire a d'ores et déjà été signé entre l'Union Européenne et les Etats-Unis, sans examen parlementaire. A cela s'ajoute les contacts entre Américains et Européens sur le choix de technologies d'interception des télécommunications, ou encore un arrangement obligeant les compagnies aériennes à fournir aux autorités américaines les données dont elles disposent sur les passagers sur leurs vols transatlantiques.
Un document interne du groupe de Schengen le souligne : « l'idée d'utiliser les

[160] European Council "New functions of the SIS-II", Bruxelles, 5/02/2002
[161] www.touteleurope.fr 31/10/2006
[162] Manière de voir n°71, Obsessions sécuritaires, le Monde Diplomatique, Octobre/Novembre 2003
[163] Document A/1900, « La lutte contre le terrorisme international : aspects de défense », assemblée interparlementaire de sécurité et de défense, www.assembly-weu.org , 14/06/2005

données du SIS pour d'autres objectifs que ceux prévus initialement et spécialement pour des buts d'information policière au sens large, fait maintenant l'objet d'un consensus large qui rejoint les conclusions du conseil après les événements du 11 septembre ». Le « consensus large » évoqué par les policiers européens ne procède pas d'un débat public : il émerge des réunions secrètes tenues dans les arrières salles de l'Union européenne.[164]

Autre domaine très débattu dans l'Europe, la conservation des données de trafic enregistrées par les fournisseurs d'accès Internet (FAI) et les opérateurs télécoms.

L'Europe envisagerait donc de se servir de ces données pour faciliter la coopération judiciaire et policière en matière de lutte contre le terrorisme. Le Conseil européen demandait dès le 25 mars 2004 un texte pour juin 2005. Le projet en circulation a été élaboré par quatre Etats membres : la France, l'Irlande, le Royaume-Uni et la Suède. Il prévoit notamment une harmonisation de la durée de conservation des données Internet et télécoms : un an au minimum et trois au maximum. Un «Groupe de travail», rassemblant la Cnil et ses homologues européens, a exprimé ses « doutes». Le projet irait trop loin pour un but mal défini. Dans l'avis qu'il a rendu début novembre 2004, le Groupe ne voit pas bien s'il s'agit de faire de la prévention, de la recherche, de la détection ou de la poursuite d'actes criminels. Au final, il estime que le projet revient à « faire de la surveillance autorisée dans ces circonstances exceptionnelles [le terrorisme, NDLR] la règle générale. » Peter Schaar, coordinateur des Cnil Européennes, au demeurant sans réel pouvoir d'intervention, insiste quand même sur le fait que les données de connexion « ne doivent pas être conservées éternellement. Par ailleurs leur accès devrait requérir l'autorisation d'un juge et ne pas sortir de l'autorité judiciaire. Enfin les autorités policières ne devraient pouvoir les consulter que dans le cas d'infractions graves[165] ». Beaucoup de souhaits qui n'aboutiront jamais en pratique dans les pays européens.
La définition des données à conserver pose aussi problème dans la mesure où elle reste assez large. Il s'agit de données nécessaires pour remonter et identifier la source d'une communication, incluant des « informations personnelles », des « informations sur la mise en contact des interlocuteurs » et des « informations sur le prestataire de service auquel a souscrit l'émetteur ». Plus tout ce qui concerne la date, l'heure et la durée de la communication, l'outil de communication utilisé, le lieu d'où elle part, et si ce lieu change en cours de route. Finalement après 6 mois de débats acharnés, les députés européens ont adopté le 15 décembre 2005 (378 voix pour, 197 contre) la directive proposée par la Commission sur l'épineux problème de la durée de rétention des données. Pour la FFII, cette directive « créera la plus grande base de données de surveillance au monde, traçant et stockant toutes les communications au sein de l'UE. ». En enregistrant par exemple l'origine et la destination de tous les courriels ou les appels téléphoniques que vous passez. La durée de stockage pourra finalement aller de 6 mois à 2 ans et concernera les appels passés par téléphones fixes, mobiles, les SMS et les communications électroniques (mail). Pour l'instant il ne s'agit **en aucun cas de surveiller le contenu des échanges**. Chaque état sera libre de fixer la durée selon ses impératifs, l'objectif étant cependant d'harmoniser les différentes législations des pays européens. Les réactions, on peut le comprendre, ont été assez virulentes. « A partir de maintenant, **tous les citoyens européens serons pistés et surveillés**

[164] Manière de voir n°71 / Le monde diplomatique / Obsessions sécuritaires / Oct-nov 2003
[165] www.zdnet.fr 13/03/2006

comme s'ils étaient des criminels ordinaires » déclarait Pieter Hintjens, président de la FFII (Association pour une infrastructure informationnelle libre). « Le Parlement Européen a raté chaque occasion de protéger les droits fondamentaux et la vie privée » estime de son côté Tony Bunyan, directeur de Statewatch. « Les deux principaux partis du parlement donnent plus d'importance à loyauté interinstitutionnelle au Conseil qu'à leur responsabilité envers les gens qui les ont élus. La façon dont ces mesures ont été adoptées est **une parodie de démocratie**. »[166]

Concernant la biométrie, le Parlement européen a adopté, le 2 décembre 2004, un rapport sur l'introduction d'identifiants biométriques dans les passeports des ressortissants des 25 pays de l'Union européenne.
Il a planché sur une proposition de règlement émanant de la Commission européenne de février 2004, puis validée par le Conseil des ministres en juin. À l'origine, le texte ne prévoyait l'introduction obligatoire que d'un seul identifiant : à savoir la photo numérisée du visage.
Mais le 25 octobre, les ministres européens de la Justice ont décidé d'ajouter les empreintes digitales comme second identifiant sur les passeports européens. Ces données seront stockées sur une puce sans contact RFID. Ils ont également insisté pour que soit instaurée une base de données centralisée. Le tout sans se soucier du travail des eurodéputés, toujours en cours, et de leurs éventuels amendements et protestations. Car **le Parlement n'est appelé à se prononcer sur ce texte que dans le cadre d'une procédure de "consultation", ce qui signifie que le Conseil peut complètement ignorer les modifications qu'il a apportées.**
Les Verts sont l'un des principaux groupes politiques à monter au créneau contre le projet de Bruxelles: «L'introduction de deux identifiants biométriques aura un impact majeur sur les droits civils et pourrait, de façon ironique, représenter une menace pour la sécurité, à travers les risques d'abus, de failles techniques, de manque de transparence et de protection des données ».
«Il ne devrait pas y avoir de base de données centrale des passeports européens (…) car cela violerait le but et le principe de proportionnalité, et accroîtrait le risque que ces données soient utilisées à des buts autres que ceux pour lesquels ils sont originellement envisagés», ont indiqué les députés dans leurs amendements. De même, ils demandent que les données biométriques servent uniquement à «l'authenticité du document et l'identité du porteur», et que les autorités autorisées à accéder à ce type de données soient clairement désignées dans le règlement. **Malheureusement plus personne ne se fait d'illusion sur le sort des amendements des députés européens que lui réserve le conseil de l'UE.**
Le 16 Août 2006, d'après Franco Frattini, Vice Président de la Commission Européenne, de plus en plus de contrôles « d'identifications biométriques » - à partir de la lecture informatique de l'iris ou l'étude des empreintes digitales – pourraient se développer dans les aéroports européens. Et cela suite à une réunion « informelle » à Londres entre les 6 principaux ministres de l'intérieur de pays Européens afin de renforcer les mesures anti-terroristes du « Conter-Terrorism Action Plan »…

Plus anecdotique, le 27 avril 2006, l'Europe a adopté un rapport qui préconise la mise en place d'ici à 2009 du système « e-call ». Ce dispositif se présente comme un système intégré au tableau de bord d'un véhicule automobile qui, en cas d'accident, alertera les services de secours les plus proches par un appel mobile au 112 - le

[166] www.zdnet.fr , 15/12/2005

numéro d'urgence européen. Dans le même temps, il donnera la position géographique du véhicule, via les satellites GPS. Cette solution pourrait permettre de réduire de moitié le temps d'intervention des équipes d'urgence et de sauver 2 500 vies chaque année, d'après le rapport Titley[167]. Un bel exemple de sécurité troqué contre la liberté de déplacement des Européens… Cependant eCall n'est encore qu'un souhait de Bruxelles et n'a pas de caractère obligatoire pour les pays membres de l'Union…

Même en dehors des règles édictées par l'Europe, des Etats européens font figure de modèle dans leur utilisation intensive des TIC. Ces cas sont intéressants à étudier car l'Europe pourrait bien s'en inspirer pour étendre ces mesures aux autres états de l'Union.

On apprenait ainsi que le gouvernement hollandais à voulu faire passer une loi, en avril 2005, obligeant les bibliothécaires à communiquer à la police la liste des livres consultés par leurs lecteurs.

Après les attentats de Londres, la ville de Berlin et l'état régional du Brandebourg ont fait savoir qu'ils comptaient ajouter des caméras dans les réseaux de transport public et prévoyaient de stocker plus longtemps les enregistrements. « Après les attentats dans la capitale britannique, nous ne voulons pas qu'on nous reproche de ne pas entreprendre suffisamment de choses » a dit le patron de la compagnie berlinoise des transports publics (BVG), Thomas Necker.

La Police belge a officiellement, pour la 1ère fois chez Belgacom (FAI Internet), obtenu « le trafic » de l'opérateur pour y puiser ses renseignements. En effet, une personne à laquelle la justice s'intéresse dans le cadre d'un dossier terroriste a été placée sur écoute informatique pendant la nuit du 16 au 17 Août 2006. Et tout y est passé : courriels, chats, sites web visités et fichiers reçus ou transférés[168].

En Italie où un million de caméras sont déjà en place, il a été décidé d'en installer davantage. Et pour l'achat de puces électroniques pour téléphones portables, le gouvernement italien a décrété l'obligation de fournir une pièce d'identité.

Même si la Russie n'est pas Européenne, cela n'aura pas empêché Moscou d'installer un réseau vidéo dans son métro fin 2006, « tous les wagons en seront munis » a déclaré le chef du métro de la capitale russe, Dmitri Gaiev[169].

Mais c'est l'Estonie qui reste en la matière l'une des toutes meilleures élèves européennes puisque l'accès à Internet est même un droit Constitutionnel. Elle organisa fin 2005 pour la première fois un vote en ligne à l'échelon national à l'occasion des élections municipales, et si l'expérience est jugée concluante, le parlement décidera d'étendre ce dispositif aux élections législatives prévu pour Mars 2007. Pour voter de chez soi en ligne chaque électeur dispose d'une carte d'identité électronique, d'un lecteur à carte à puce et surtout d'un code d'accès inhérent a chaque carte et renseigné dans le cadre d'une signature électronique. Sur 1,3 millions d'habitants, ce sont presque 900.000 d'entre eux qui disposent d'une carte d'identité électronique. Crypté et dépouillé anonymement, le secret du vote est protégé. Mais à cette étape de l'exposé, on comprend bien qu'un Etat peu scrupuleux pourrait très facilement faire de l'anonymat du vote un secret de polichinelle.

[167] www.01net.com 03/05/2006
[168] www.lesoir.be 23/08/2006
[169] AFP, 27/07/2005

La palme européenne revient cependant sans aucun doute à la **Grande Bretagne**, citée par L'Expansion comme « **le pays le plus surveillé de la planète »**. L'exemple type ? Un test grandeur nature est mené auprès de la population où bientôt sortir ses papiers d'identité ne suffira plus. Les forces de l'ordre, munies d'un petit boîtier pourront bientôt vérifier, sur présentation des doigts de l'intéressé, ses empreintes dans une base de données centralisée qui en compte plus de 6,5 millions[170] . "La société de la surveillance est devenue réalité sans que nous n'y prenions garde" : c'est le constat effectué par un rapport britannique destiné à la Commission pour l'information, l'équivalent de la CNIL, publié fin 2006, qui dresse un portrait quasi orwellien du pays. Des « **caméras vidéos** [on en compte **4,2 millions** exactement, soit une pour 14 habitants] nous observent en permanence, dans les immeubles et les rues commerçantes, sur la route et dans les quartiers résidentiels ». Pourtant, selon les auteurs, des universitaires du Surveillance Studies Network, ces dernières ne seraient que la partie émergée de l'iceberg, qui remarquent que les comportements de la population sont de plus en plus observés, analysés, enregistrés. Ils citent notamment la collecte des données à des fins commerciales, via les cartes de crédit, cartes de fidélité et téléphones mobiles. Ils soulignent aussi que les services de renseignement « ont accès à la façon dont nous nous servons du téléphone, du courrier électronique et d'Internet et peuvent effectuer une recherche à partir de mots et de phrases clés ». Et rappellent que « nous sommes constamment invités à nous identifier, que ce soit pour recevoir des allocations sociales, des soins de santé, etc. ». L'un des problèmes principaux, selon les auteurs du rapport, réside notamment dans le « **détournement de l'utilisation** », c'est-à-dire **quand** « **les données personnelles collectées et utilisées dans un but unique sont réutilisées ailleurs** ». Et de citer le cas des cartes de transport Oyster à Londres : les données commerciales des transports en commun sont selon eux « de plus en plus utilisées par les services de police dans le cadre de leurs enquêtes ». Le rapport précise que la majeure partie des techniques de surveillance est automatisée et hors de la vue des personnes qui les subissent. Il prévoit que cette observation étroite de la population va aller croissante dans les dix années à venir, et dénonce **l'avènement d'un « climat de suspicion »** au sein de la société. Cette dernière finit par développer selon eux un véritable « tri » entre ses membres, qui depuis les attentats du 11 septembre a par exemple « entraîné un profilage grossier de certains groupes, surtout des musulmans, qui a débouché sur des désagréments, des difficultés et parfois des tortures ». Conséquence, **la société « met l'accent sur l'exclusion des éléments indésirables » et la discrimination s'accentue[171].**

L'Electronic Privacy Information Center et Privacy International publient annuellement un rapport axé sur le respect de la vie privée dans les différents pays. Ceux-ci sont notés de 1 à 5, plus haute étant la note et meilleure étant la protection de leurs citoyens dans ce domaine sur la base des dispositions constitutionnelles, des lois destinées à protéger la vie de tout un chacun, des cartes d'identité, du traitement des données biométriques, etc. Avec un score de 3,9/5, l'Allemagne est le pays qui respecte le mieux ces données en Europe (ce qui se comprend bien entendu pour des raisons historiques). Tout en bas de l'échelle, on trouve assez logiquement le Royaume Uni (1,5/5) et – ce qui reste assez étonnant – les Pays-Bas

[170] www.01net.com 22/11/2006
[171] Ce paragraphe est largement tiré d'un article de www.lexpansion.com du 02/11/2006

(2,3) et la Suède (2,2)[172].

4-5 Une France affaiblit, mais avec un potentiel certain.

« Je ne crois plus à cette guerre de la moitié de la France contre l'autre. »

François Bayrou

A la suite des attentats du 11 septembre, le gouvernement français fait adopter des dispositions destinées à la lutte anti-terroriste. Le 6 octobre 2001, il dépose des amendements au **projet de loi pour la sécurité quotidienne (LSQ)** « *afin de renforcer l'efficacité des services d'enquêtes et combattre plus efficacement les menées du terrorisme* […] *et destinés à assurer la plus grande sécurité des Français dans une période où le risque est accru et actuel. ».* D'après le 2nd amendement, ces dispositions sont censées être **exceptionnelles et temporaires** et doivent prendre fin le 31 décembre 2003. Cette mesure donne accès à l'autorité judiciaire aux logs de connexions conservés par certains FAI et qui sont une première étape pour enregistrer les faits et gestes de tous les citoyens français sur Internet.

Le 21 Janvier 2003, l'assemblée Nationale, après avis favorable du Ministre de l'intérieur M. Sarkozy, adopte en une minute l'amendement Estrosi, rendant **définitive** la mesure « anti-terroriste », initialement exceptionnelle et temporaire, ce qui fait qu'elle est au final totalement séparée de l'existence ou non d'une menace terroriste. Cet amendement sera plus largement intégré dans **la loi pour la sécurité intérieure (LPSI),** elle-même promulguée le 18 mars 2003.

Plus tard, le 10 octobre 2005, la CNIL étudie le projet de loi relatif à la **lutte contre le terrorisme (LCT)** présenté par le ministre de l'Intérieur, et émet un avis particulièrement sévère sur le texte qui prévoit ni plus ni moins que de donner accès aux logs de connexion des Français aux services de Police (DST, DGSE, Renseignements Généraux…) **en dehors de tout contrôle de l'autorité judiciaire pourtant constitutionnellement garante des libertés des français.** Le texte prévoit que les demandes d'accès aux logs de connexion des internautes soient centralisées par l'Unité de Coordination de la Lutte Anti-terroriste (UCLAT), et **autorisées par une personnalité qualifiée placée auprès du ministre de l'intérieur et nommée par lui.** [173]

Si par exemple, un agent des Renseignements Généraux ne respecte pas la LCT en accédant aux logs de connexion pour des raisons autres que la lutte anti-terroriste, la loi prévoit qu'il rende compte de ses actes (en ne prévoyant aucune sanction pénale) au ministre de l'intérieur, qui n'a pas caché son intention de concentrer tous les pouvoirs, et non pas devant la justice !

Parmi les autres amusements du texte, on trouve une mesure encore inédite en France : un dispositif de surveillance des déplacements des personnes sur le réseau routier, à l'aide de fichiers des numéros d'immatriculation et des photos des occupants des véhicules[174] !

En l'état, la LCT place donc tous les internautes français sous techno surveillance policière constante, les considérant de ce fait comme des suspects, **écarte**

[172] www.fr.datanews.be 6/11/2006
[173] www.odebi.org Les logs pour les nuls
[174] www.01net.com 26/10/2005

totalement et volontairement le rôle du juge constitutionnellement gardien des libertés, et instaure sans ambiguïté un état policier numérique. De plus Pascal Cohet, porte parole de la ligue Odebi déplore que « rien n'est prévu pour que l'internaute puisse se retourner contre un éventuel abus de la part notamment des renseignements généraux. »[175]

Le Conseil constitutionnel, qui fut saisi par les sénateurs socialistes estimant que seul un juge doit autoriser l'accès aux données de connexion, ne les a finalement pas suivi, et par une décision du 19 janvier 2006 a validé la disposition décrite dans l'article 6 imposant la conservation des logs par les principaux acteurs de l'Internet (FAI, Opérateurs télécoms, Cybercafés…), en ne remettant pas du tout en cause l'absence de tout contrôle judiciaire… « La décision du conseil constitutionnel laisse quasiment intacte toutes les dispositions de ce projet auxquelles nous sommes fortement opposés » commente pour ZDNet.fr la vice-présidente de la Ligue des droits de l'Homme (LDH).

Par ailleurs, Monsieur Sarkozy affiche publiquement ses intentions : « être à l'écoute de tout, et si possible savoir tout »[176] n'hésitant pas à qualifier de « polémique stérile » les réactions d'inquiétude légitime provoquées par **un projet de loi menaçant** à l'évidence le droit au **respect de la vie privée** et le **rôle protecteur du juge** indépendant et impartial. « Il fallait adapter le dispositif juridique français pour protéger les Français », a-t-il souligné.

La LCT accroît le recours à la vidéosurveillance et la surveillance des cybercafés, de la téléphonie, mais aussi des déplacements de ceux qui se rendraient dans des pays à risque. Nicolas Sarkozy souhaite donc installer des caméras « dans le métro, les aéroports, les gares », à Paris comme en province mais aussi « autoriser les lieux de culte et les grands magasins à les développer sur leurs trottoirs ». Plus de 4000 bus parisiens sont déjà équipés de caméras de surveillance[177]. Les préfets auront également la possibilité de l'imposer « dans les lieux sensibles. La ville de Lyon avait été une très bonne élève puisque dès 2003 une cinquantaine de caméras de surveillance hyper perfectionnées pouvant pivoter à 360° et faire une photo d'identité à 300 mètres avaient vu le jour… Ce qui reste incroyable c'est qu'à l'époque l'installation de ce vaste réseau n'avait soulevé aucune opposition, à gauche comme à droite.

Concernant les cybercafés, la loi les oblige maintenant à conserver leurs données informatiques durant un an, tout comme les services de téléphonie et les FAI, afin de permettre aux services de Police et de Gendarmerie de reconstituer les réseaux. Le décret d'application est paru le 24 mars 2006. Pour l'association Imaginons un réseau Internet solidaire (IRIS), « ce décret représente l'**aboutissement d'une stratégie de contrôle plus large de la population, dont la lutte contre le terrorisme ne constitue qu'un alibi. La rétention des données de communication révèle l'intimité des personnes, cartographie leurs activités et identifie les réseaux de relations tissés entre elles »**[178] (voir à ce propos le chapitre « Exemple d'outils au service du contrôle » pour bien comprendre comment cela se passe).

[175] www.zdnet.fr 30/11/2005
[176] www.nouvelobs.com 26/10/2005
[177] AFP, 27/05/2005
[178] www.zdnet.fr 27/03/2006

Même des instances comme la CNIL (Commission Nationale Informatique et Libertés) qui devrait être des plus conservatrices en matière de libertés individuelles ne joue plus totalement son rôle d'opposition et de régulation. Par exemple depuis des réformes de juillet 2004, elle ne dispose plus maintenant que d'un avis consultatif sur la création de fichiers de Police.

Le Président de la République, Jacques Chirac, va dans le même sens en affirmant : « L'exigence, c'est d'adapter en permanence nos dispositifs à l'évolution de la menace » et « d'être en permanence en anticipation ».

Jean René Lecerf, Sénateur UMP du Nord, fait un pas de plus. Pour lui, « il faut renverser le « syndrome Big Brother ». Montrer que liberté et sécurité ne s'excluent pas mutuellement. Imaginons qu'un fichier central de données biométriques soit créé, qui offrirait à chacun un libre accès, sécurisé et gratuit pour les renseignements le concernant : on saurait quelle instance a consulté sa fiche d'identité et dans quel cadre. Ne serait ce pas là un gain de liberté ? » Mais connaît-il vraiment toutes les facettes de l'Internet pour s'exprimer ainsi ?

La secrétaire générale adjointe du ministère de la Justice, Dominique Cottin, a annoncé la création pour le ministère (normalement pour 2008) d'une « plate-forme qui permettra l'écoute de la voix, l'identification des numéros appelants, la géolocalisation des téléphones mobiles, la réception des informations détenues par les opérateurs et leur renvoi aux services enquêteurs ». Aujourd'hui, les écoutes sont demandées par les enquêteurs aux juges d'instruction, qui ordonnent l'interception par le biais d'une commission rogatoire. Puis, les officiers de police judiciaire se chargent de son application auprès de l'opérateur et du fournisseur de matériel d'interception. En 2005, les dépenses d'interception se sont élevées à 92 millions d'euros, contre 70 millions en 2004. Les 20 000 écoutes téléphoniques effectuées l'année dernière ont représenté à elles seules 30 % de cette somme[179].

Dernier dossier, et de taille pour l'examen au Parlement et au Sénat pour fin 2006/début 2007[180] : le projet de **loi de prévention de la délinquance** définitif présenté en Conseil des Ministres en Juin 2006. Dans un article intitulé « Bienvenue en Sarkoland », Gilles Sainati, magistrat et membre du Syndicat de la magistrature, regrette la mise en place de la structure d'un « nouvel Etat » [181] qui, au regard de celui qui existait il y a seulement 5 ans en France, pourrait être qualifié de beaucoup plus sécuritaire en ce que, par exemple :

- Il remplace l'accompagnement social par un **contrôle tous azimuts des personnes suspectées de déviance**. Le maire devient le supérieur hiérarchique des travailleurs sociaux, un destinataire de toutes les informations sociales, judiciaires et médicales des citoyens sur son ressort. Il est doté de pouvoirs de sanctions civiles et financières à l'encontre des familles, il est le nouveau délégataire de la puissance publique en terme de sécurité. Néanmoins, dans la motion adoptée fin 2006 lors de leur congrès, les maires expriment leur hostilité au texte du Ministre de l'Intérieur qui concerne leur rôle de « pivot » dans la prévention de la délinquance. Les maires refusent de « se substituer à la justice, à la police ou à l'éducation

[179] www.01net.com 06/10/2006

[180] Etant donné la parution de ce présent ouvrage début 2007, nous n'avons aujourd'hui pas toutes les données en main par rapport à cette future loi, c'est pourquoi nous encourageons le lecteur à se renseigner de manière plus approfondie suite à la lecture de ce chapitre.

[181] http://lmsi.net/article.php3?id_article=562 de Gilles Sainati , 29/06/2006

nationale » (dixit leur communiqué). M. Sarkozy a affirmé qu'il voulait seulement que les maires puissent « centraliser toutes les informations » de la part de l'Inspection d'académie ou de la Caisse d'Allocations Familiales en cas d'absentéisme scolaire. Mais la collecte d'un certain nombre d'éléments de plus en plus nombreux « entre les mains » de maires promulgués « Shérifs » sur leurs administrés, même avec les meilleures intentions du monde ne correspond elle pas à un début d'état policier ? Que se passerait-il demain, si une ville comme Toulon, redevenait démocratiquement sous la coupe d'un parti d'extrême droite ?

Quoi qu'il en soit, **espérons que le débat pour les prochaines élections présidentielles, puis législatives, de 2007 fasse une large place à la question des libertés individuelles par rapport à l'usage des TIC.** On pressent en effet que le problème de la « sécurité » sera au cœur des débats. **Il faudra beaucoup de courage aux candidats**, qui en auront compris l'enjeu, **pour s'opposer à la dérive sécuritaire actuelle**. Et redonner l'**essentiel** : de la **confiance** et favoriser l'entraide mutuelle entre les citoyens. Il faut bien comprendre que jamais des mesures sécuritaires ne pourront restaurer une quelconque sécurité dans la société civile. **La France pourrait devenir le fer de lance d'une politique plus harmonieuse** en mettant, contrairement à nos voisins d'outre manche et d'outre atlantique, les libertés des citoyens au premier rang des priorités et en abordant les aspects « sécuritaires » avec toutes les retenues qu'il faut avoir. Les cartes ne sont pas encore distribuées, **la paranoïa dans notre pays n'est pas d'actualité**, les prémices des mesures liberticides pouvant être encore rééquilibrées. Pour prendre un exemple simple, notre pays ne comptera pas, d'ici 2008, si les choses n'évoluent pas d'ici là, plus de 1000 fonctionnaires dans les services de renseignement et de police spécialisés dans la surveillance des réseaux et de la cybercriminalité. A titre comparatif, la NSA (National Security Agency) aux Etats-Unis qui gère le réseau Echelon (réseau qui intercepte l'ensemble des communications mondiales et qui en traite environ 15%, ce qui est déjà énorme) compte plus de 40.000 personnes ! En grande Bretagne, ce sont aussi plus de 15.000 fonctionnaires qui sont derrière Echelon[182]. La France, malgré les pressions économiques qui voudraient inciter l'état à avoir lui aussi de « grandes oreilles » pour tout savoir, pourrait s'essayer à tracer une voie plus médiane, dans le respect des libertés de tous ses citoyens. Et peut-être montrer l'exemple.

Approfondissons maintenant quelques sujets d'actualité Français où politique, économique et social sont intimement liés aux TIC :

*** Le dossier médical informatisé

Chaque bénéficiaire français de l'assurance maladie va se voir très prochainement attribuer un dossier médical personnel (ou DMP) qui sera hébergé sur Internet et comportera tout l'historique médical du patient, c'est-à-dire toutes les données recueillies ou produites à l'occasion des activités de prévention, de diagnostic ou de soins. Le DMP devra fonctionner pour tous les Français de plus de 16 ans le 1er juillet 2007. Les premières expérimentations concrètes ont débuté en Février 2006.

[182] Rapport d'information de l'Assemblée Nationale n°2623 sur « Les systèmes de surveillance et d'interception électroniques pouvant mettre en cause la sécurité nationale » par Arthur Paecht. Le rapport qui date de 2000 est disponible sur le site de l'assemblée nationale.

Le montant de prise en charge financière des actes et prestations par l'assurance maladie sera subordonné à l'accès du professionnel de santé au dossier médical personnel. En mettant nos dossiers médicaux sur fichiers informatiques, en rendant obligatoire l'utilisation de la carte vitale dans sa conception actuelle, la Sécurité Sociale se dote ainsi d'un outil qui pourrait devenir un outil de surveillance sociale, voire de discrimination. De plus, derrière ce projet se cache une drôle de conception du patient, un peu « bêta » car vu comme incapable d'expliquer à un médecin (pris lui-même dans une logique productiviste) ses problèmes de santé en ne disant que ce qu'il souhaite.

L'ADAS (Association de défense des assurés sociaux) a entamé un véritable combat pour informer les assurés sur le sort de leurs données de santé, sur le danger du DMP et sur les failles du système Sésame-Vitale. Les médecins fondateurs de l'ADAS ont d'ailleurs pris d'énormes risques puisqu'ils ont décidé de se déconventionner **pour ne pas avoir à cautionner le fin du secret médical** à travers les multiples projets d'informatisation des données de santé. Le Docteur Martine Marchand dans une lettre au Directeur de la CPAM déclare : « Attendu que, à l'instar du Conseil de l'Ordre des Médecins, je considère que l'obligation de télétransmission à porté atteinte à notre déontologie (art. 4 du Code de Déontologie traitant du secret professionnel et toujours en vigueur) et que la télétransmission nous met donc en état de faute professionnelle »[183]

Dans une dépêche APM du 13 février 2006, on apprend que la CNAMTS (caisse d'assurance maladie des travailleurs salariés) a été contrainte de fermer son service pour corriger des failles de sécurité sur son site Internet, plus précisément pour l'accès au service « médecin traitant en ligne » qui rendait le portail, a priori réservé au professionnels de santé, ouvert à n'importe quel internaute, qui avec un simple numéro de sécurité sociale, pouvait connaître le parcours de soin de n'importe qui. De nombreux autres exemples sont disponibles sur le site de l'ADAS, concernant le manque de sécurisation et les failles du système. On pressent déjà que pratiquement n'importe qui pourra se procurer des informations confidentielles sur la santé d'un autre individu.

On l'a compris, bientôt la moindre information concernant notre santé sera en circulation sur un réseau plus ou moins sécurisé. D'autres pays démocratiques s'y dirigent déjà[184]. Acceptera t'on de rembourser ceux qui refuseront de se plier au système informatisé, mais qui s'engageront à détenir tout leur dossier médical et à la présenter à chaque consultation au médecin de leur choix ?

Les Etats-Unis ont de leur côté dépassé le cap de l'expérimentation. D'après « Information Week », un consortium d'entreprise (Wal Mart, BP, Intel…) a lancé « Dossia », une vaste base de données regroupant les données médicales de leurs salariés. Forcément accessibles aux hôpitaux et médecins, ces informations pourront dans certains cas être aussi accessibles aux… compagnies d'assurance ! Toujours pour des raisons de substantielles économies les salariés des compagnies seront fortement incités à s'y inscrire, tout en sachant qu'ils ne pourront pas en être

[183] www.webzinemaker.com/adas

[184] En effet, au Canada, un logiciel dont l'élaboration et la mise au point a été financé indirectement par les services secrets américains servira à indexer le dossier médical de millions de Canadiens. Le logiciel a été élaboré par la firme Initiate Systems de Chicago, en partie avec des fonds reçus de In-Q-Tel, une société de capital risque créée par la CIA américaine il y a sept ans pour l'aider à identifier et acquérir les technologies les plus avancées. Source : www.canoe.com 18/08/2006

effacées, même pour un licenciement, une démission ou… un décès ! Un représentant d'Intel a en effet expliqué à *Information Week* qu'une fois les informations rentrées dans Dossia, elles ne quitteront plus la base.[185]

*** Passeports et carte d'identités biométriques

Le projet Français Ines est connu sous le terme de Identité Nationale Electronique Sécurisé (certains l'appelle aussi CNIE pour Carte Nationale d'Identité Electronique). Mais le projet à terme pourrait aller plus loin qu'une simple carte d'identité électronique, en regroupant par exemple également « la carte Vitale, le passeport, les permis de conduire, la carte de séjour des étrangers…Tous ces titres seront biométriques à l'aide entre autres d'empreintes digitales et de photos numérisées, au plus tard en 2008 »[186]. Lutte contre le terrorisme, l'immigration irrégulière et les faux papiers sont les fers de lance les plus utilisés pour justifier le projet. En fait, ce projet pourrait viser l'établissement d'une giga base de données policière à l'échelle du pays et de toute la population sur des « puces » lisibles sans contact, c'est-à-dire à la méconnaissance complète de l'individu. Il s'agit de rendre ainsi l'individu totalement transparent tant aux autorités publiques qu'aux opérateurs commerciaux.

Beaucoup d'associations françaises[187] oeuvrant pour les libertés individuelles ont lancé une pétition en mai 2005 contre Ines et déclaraient : « qu'un tel projet met en cause une société dans laquelle l'identité reste fondée sur un principe déclaratif, au profit d'une conception de l'identité imprimée dans l'intimité biologique. **Il nous propose l'abandon d'une présomption de confiance mutuelle au profit d'une généralisation de la suspicion** ». « D'une prévention de la fraude documentaire, on aboutit à un fichier de police », déplore Alain Weber de la LDH. De plus la partie « signature électronique » pourrait être utilisée pour les télé-procédures et autres transactions sur les sites d'e-commerce. « La carte d'identité, ce n'est pas pour aller aux Galeries Lafayette », résume Michel Tubiana, toujours à la Ligue des Droits de l'Homme.

Sous la pression, le gouvernement français à du légèrement revoir sa copie pour offrir une 2ème vie à Ines. Philippe Sauzey, Directeur du programme Ines à présenté en décembre 2005 une esquisse de la nouvelle carte. Il sera prévu qu'Ines soit payante (entre 10 et 20 € avec gratuité pour les personnes les plus démunies), mais **facultative**[188]. « A l'avenir, vous pourrez adopter une pièce de nouvelle génération ou rester aux versions actuelles » a-t-il déclaré. Cela ne convainc pas Alain Weber : « Le système papier disparaîtra au profit de la biométrie, si des facilités lui sont associées. »[189]

Deux grandes catégories de données apparaîtront sur la carte : une partie régalienne et une partie « services ». Les données traditionnelles (nom, prénom, date de naissance, adresse du domicile…) y seront inscrites. Elles seront reprises dans le composant électronique pour la partie régalienne et complétées par des éléments biométriques (à priori des empreintes digitales numérisées et une photo). La puce,

[185] www.01net.com 07/12/2006
[186] www.pcinpact.com, 27 mai 2005
[187] La ligue des droits de l'Homme, le Syndicat de la Magistrature, le Syndicat des Avocats de France, l'association Imaginons un Réseau Internet Solidaire, l'intercollectif Droits et Libertés face à l'informatisation de la société et l'Association française des juristes démocrates.
[188] www.zdnet.fr du 9/12/2005
[189] www.01net.com du 07/07/2006

basée sur la technologie RFID, fonctionne comme on le sait, sans contact. Le citoyen pourra y être identifié par les pouvoirs publics et les polices d'une trentaine de pays partenaires. Quant à la partie « services en lien avec l'identité », elle devrait comprendre deux éléments. Une certification d'authentification du détenteur de la carte et un volet de signature électronique qui « pourrait n'apparaître qu'à la deuxième génération de la carte d'identité numérique » selon Philippe Sauzey »[190]. Les dates n'ont pas changé et devrait donc être mis en place en 2008.

Quelques-uns uns de nos voisins européens sont déjà très en avance puisque ayant déjà délivré les cartes d'identités électroniques. On recensait début 2006 plus de 2 millions de cartes en Belgique par exemple, et début 2007, l'ensemble de la population de plus de 12 ans soit 9 millions de personnes seront équipées. Une eID « light » pour les moins de 12 ans est même prévue, le gouvernement n'ayant pas encore décidé si elle serait obligatoire[191]. Bien difficile donc de rester anonyme, même pour les plus jeune, en Belgique. Pour l'anecdote, Bill Gates, en visite à Bruxelles, en février 2005, a applaudi des deux mains le projet belge de carte d'identité électronique. Le patron de Microsoft a même annoncé que son entreprise allait adapter MSN Messenger, sa messagerie Internet, à cette nouvelle carte. Le mélange du domaine régalien de l'état avec une firme multinationale privée reste à vrai dire assez inquiétant. Pour converser de manière sécurisée, les correspondants devraient ainsi se faire identifier en introduisant leur carte électronique dans un lecteur branché sur leur ordinateur. L'objectif soi-disant officiel de Microsoft et de l'autorité belge est à la fois " de faciliter l'utilisation de l'Internet" et de rendre le réseau "plus sûr pour les enfants". D'autres applications Microsoft seraient concernées.

Avant leur probable fusion avec Ines, le passeport électronique français (qui deviendra ensuite biométrique, mais « pas avant avril 2009 ») continue sa route sous la pression des Américains. Ainsi pour se conformer aux exigences américaines, la France (et de nombreux autres pays membres de l'UE) a eu officiellement jusqu'au 28 août 2006, date buttoir, pour agir et les mettre en circulation[192]. Ce passeport contient une puce et une photo numérique. La puce électronique sans contact (RFID), intégrée dans la couverture du document, renferme toutes les données de la seconde page du traditionnel passeport papier. On y trouve donc des informations personnelles (nom, prénom, nationalité, etc.) et générales (autorité de délivrance, date...).

La CNIL précise que les services de police et de gendarmerie seront autorisés à accéder au fichier national des passeports. La réglementation européenne, adoptée par le Conseil des Ministres fin 2004, a déjà prévu de passer à deux identifiants à l'horizon 2008 : la photo numérique et l'empreinte digitale.

On peut déjà imaginer que l'ensemble de ces cartes électroniques, toujours pour des raisons « économiques et pratiques » pourraient prendre la forme d'un seul support qui verrait alors son usage généralisé à tous les aspects de la vie quotidienne.

[190] www.VNUnet.fr du 05/12/2005
[191] www.vnunet.be 06/06/2005
[192] www.01net.com 28/08/2006

*** La carte navigo

Les clients franciliens de la RATP et de la SNCF doivent payer, dès 2007, pour obtenir un pass Navigo sans être automatiquement fichés dans leurs bases de données.
La RATP a en effet commencé à généraliser depuis l'été 2005 ses cartes Navigo, c'est-à-dire ces titres de transports munis de puces électroniques radio (RFID) et capables de stocker des données personnelles.
Déjà utilisées en titres annuels, elles doivent progressivement remplacer les bonnes vieilles "Cartes Orange" (mensuelles ou hebdomadaires) actuellement en service. Mais le hic, c'est que pour bénéficier d'un pass Navigo anonyme, avec lequel aucune trace des voyages ne sera mise en mémoire, le client RATP devra débourser cinq euros. Aux dernières nouvelles, ce pass un peu spécial devrait voir le jour courant 2007.
«Chaque fois que l'on met en place un système de carte à puce qui permet de tracer des déplacements, il faut proposer aux gens une alternative, qui est l'alternative de l'anonymat. Cette alternative doit être gratuite», affirmait sur France-Info Christophe Pallez, à l'époque secrétaire général de la CNIL.
La controverse a pris tellement d'ampleur que le Stif (Syndicat des transports d'île de France) a dû sortir un communiqué pour remettre quelques pendules à l'heure. «Il est faux de laisser penser qu'il sera possible de connaître les déplacements des voyageurs», souligne-t-il. «Les informations sur les passages aux validateurs sont uniquement utilisées par un système automatisé de détection de la fraude, et [elles] sont automatiquement détruites au bout de 24 heures». Soit une durée inférieure aux 48 heures préconisées par la Cnil dans une recommandation de septembre 2003.
Pour bénéficier d'un pass Navigo, les clients devront toutefois remplir une fiche signalétique, avec nom, prénom, adresse et téléphone. Et donc figurer dans le fichier commercial de la RATP ou de la SNCF, suivant l'organisme auprès duquel la carte a été acquise.
Le STIF garantit que ces informations «ne sont pas inscrites sur la puce mais sur le fichier de gestion», et qu'elles «sont traitées de façon complètement indépendante des données de validation».

A noter cependant qu'à la mi-juillet 2006, un internaute a pu consulter, à cause d'une faille de sécurité sur le site de la Régie des transports parisiens, des données concernant plus de 1000 utilisateurs du pass navigo. Photo du demandeur, nom, prénom, adresse postale, électronique et numéro de téléphone étaient ainsi lisibles par tout un chacun[193].

Une alternative sera effectivement proposée, et payante, à ceux qui ne souhaitent pas figurer dans les fichiers commerciaux. Il s'agira de la carte pour les voyageurs occasionnels, dit «carte Navigo non personnalisée». C'est cette dernière, dotée d'une puce, qui coûtera cinq euros, correspondant à son coût de fabrication selon le STIF.
Le Syndicat justifie cette démarche par «un souci de lutter contre le gaspillage». Il ne veut pas qu'un «voyageur occasionnel puisse chaque fois qu'il en a besoin demander une nouvelle carte sans en supporter le coût».
« Effacer les traces » de son passage devient un service payant et cela constitue

[193] www.01net.com 31/08/2006

peut être en la matière le début d'un nouveau marché qui a beaucoup d'avenir **: il faudra à l'avenir probablement payer pour son anonymat et le respect de sa vie privée.** On prenait dans nos sociétés occidentales ce droit pour acquis. On voit qu'il n'en est rien.

Fin 2005, la RATP faisait un pas supplémentaire en expérimentant Navigo Mobile, une solution de paiement et de validation d'accès par le téléphone portable. Pour prendre les transports en commun, l'utilisateur n'a plus qu'à recharger son compte via son mobile directement à travers un site i-mode RATP[194]. « Techniquement », le système pourrait être au point « début 2008, en étant le plus optimiste », estime-t-on à la RATP[195]. Bien entendu, via un portable, plus question donc d'anonymat…

*** Police et GPS

La Police française veut intervenir deux fois plus vite. Pour optimiser le déploiement des forces de police, le ministère de l'Intérieur met en place des centres d'information et de commandement (CIC) entièrement informatisés.

Vingt-trois minutes. C'est, selon une expérimentation menée à Amiens, le temps moyen qu'il faut à une patrouille de police pour arriver sur les lieux d'une intervention. L'objectif du ministère de l'Intérieur est de diviser par deux ce délai, grâce à un système de géolocalisation. « Nous allons mettre en place un système d'information autorisant la gestion intégrée des interventions », explique Jean-Yves Latournerie, DSI du ministère.

La première phase de déploiement à débuté en novembre 2005 et concernait d'abord une trentaine de centres d'information et de commandement (CIC). Ces derniers sont les lieux de réception des appels au 17, le numéro d'urgence de police secours. Ils sont 135 au total, en comptant ceux de la police nationale, des CRS et de la police de l'air et des frontières. L'objectif principal est d'améliorer les conditions de gestion des appels de détresse. « Notamment en réduisant le temps d'attente à une vingtaine de secondes, contre une cinquantaine aujourd'hui », précise Vincent Niebel, chef du département Affaires Sécurité au sein de la DSI de la place Beauvau.

Comment y arriver ? **En numérisant l'ensemble de la chaîne d'information** qui suit un appel au 17. La téléphonie sera totalement intégrée au système d'information à l'aide d'un dispositif de VoIP (voix sur IP) et d'un serveur CTI (couplage téléphonie informatique). Mais cela ne suffit pas. Intervenir plus vite nécessite également de disposer d'informations sur le déploiement des effectifs.

Pour l'instant, il n'existe pas d'outil assurant une vision précise de la localisation des voitures de police et des effectifs qui les composent. On peut supposer que le projet de l'IGN (Institut géographique national) qui à mis à la disposition de tous les internautes mi 2006 des visions aériennes jusqu'à une précision de 50 cm sur tout le territoire arrive à point nommé pour la Police. En attendant, les véhicules seront donc progressivement équipés du système Egnos (European Geostationnary Navigation Overlay System), un service européen complémentaire du GPS (Global Positionning System). Leur position sera alors connue avec une précision à cinq mètres près

[194] www.lemondeinformatique.fr du 26/10/2005
[195] www.lexpansion.com 18/10/2006

(contre une quinzaine de mètres avec le GPS seul). A leur bord, les policiers se verront dotés d'ordinateurs portables : « Ils pourront ainsi rédiger leur rapport juste après l'intervention, sans attendre de revenir à l'hôtel de police », indique Jean-Yves Latournerie.

Outre le gain de temps, cette « innovation » contribuera à établir une cartographie encore plus précise de la délinquance et de l'occupation réelle des équipages. Ce qui améliorera la répartition et l'organisation des forces de l'ordre. En attendant de la proposer aux autres services d'urgences que sont le Samu, les pompiers ou les douanes. A priori, on peut donc s'attendre à ce que toute activité humaine soit à terme fichée, numérisée, archivée et cartographiée. **L'imprévu sera alors considéré comme suspect.**

4-6 L'homme-produit : «Au nom de la loi consomme !»

Lorsque commencera l'An Mille qui vient après l'An Mille
L'homme fera marchandise de tout
Chaque chose aura son prix
L'arbre l'eau et l'animal
Plus rien ne sera vraiment donné et tout sera vendu
Mais l'homme alors ne sera plus que poids de chair
On troquera son corps comme un quartier de viande
On prendra son œil et son cœur
Rien ne sera sacré ni sa vie ni son âme
On se disputera sa dépouille et son sang
comme une charogne à dépecer

Le "Protocole Secret" (~1050)

Jean de Vézelay

La dernière carte de l'économie, pour poursuivre dans ses rêves de croissance infinie sur une petite planète où pourtant les ressources sont finies, sera peut être d'en venir à considérer l'homme en produit de consommation courante. Finalement sujet et objet, consommateur et consommé.

Quand la science du marketing, qui tire littéralement le wagon économique aujourd'hui jusque dans ces derniers retranchements, s'associe à des pratiques de développement personnel, on aboutit souvent à des conclusions relativement absurdes.

Ainsi, on peut découvrir sur la couverture du livre « Pour en finir avec l'échec : le bon marketing de soi »[196] :

[196] De Brigitte Bloch-Tabet et Catherine Pelé-Bonnard, Chiron Editeur, 2004

« Dans la vie comme en marketing, il s'agit d'adapter le produit que nous sommes à la demande des clients que sont nos proches : nos patrons, nos partenaires, nos conjoints, nos enfants, nos parents, nos amis, nos amours…
Ces clients il faut savoir qui ils sont, ce qu'ils attendent de nous, où les trouver, comment communiquer avec eux.
Nous devons également tenir compte de la concurrence et nous en protéger avec une politique offensive ou défensive, en nous positionnant et en indiquant clairement nos particularités, nos atouts, nos ressources, notre sens de l'innovation, le but étant, bien entendu, de nous faire considérer comme « une marque sérieuse ».
Il est bon de s'envisager comme un capital qu'il faut entretenir et faire fructifier en exploitant à fond ses multiples facettes, et de prévoir des situations de rechange ou de repli en cas d'échec au cours de sa démarche.
Dans toutes nos relations à l'Autre, qu'il s'agisse d'amour, de parcours professionnel, de vie familiale ou de quête de soi, nos attitudes, nos démarches, nos comportements obéissent aux règles du bon marketing. Il suffit d'en prendre conscience et d'adopter les stratégies les plus subtiles de cette branche qu'on attribue habituellement au monde de l'entreprise. »

Le décor est donc posé : si les hommes désirent « évoluer», ils n'ont plus qu'à devenir des produits à part entière pour se « gérer » le mieux possible vis-à-vis de leur « environnement » et optimiser ainsi leur « cycle de vie ». Les dérives sémantiques faisant, le code barre amélioré (puce RFID) prendra tout naturellement sa place dans une humanité en perte des repères fondamentaux, et totalement aveuglée par le « progrès technologique ».

En effet, tout devient consommable dans notre société : nous passons parfois l'éponge lorsque les produits sont fabriqués par des enfants, nous nous posons parfois la question lorsqu'il s'agit de nourriture animale, on s'offusque heureusement encore lorsqu'on parle de trafic d'organes. Un scénario possible, si bien dénoncé dans le film « The Island »[197], pourrait se dérouler sur notre planète, où des humains fortunés, apeurés à l'idée de la mort, ont décidé, via des sociétés d'assurances, de se créer des « clones » qui pourront leur fournir l'organe défaillant intact en cas de grave maladie.

Ainsi, comparer l'homme à un produit revient à le prendre pour interchangeable, jetable, dénué de vie, de sentiments et de conscience. Il n'est qu'un paramètre d'équation à maximiser pour être le plus rentable possible. S'il arrive à la fin de son cycle (tout produit marketing suit en effet 4 phases : le démarrage, la croissance, la maturité, et le déclin), il n'a plus de raison d'être, on peut le mettre au rebus car il coûte alors plus qu'il ne rapporte. Or si on regarde nos sociétés sous cet angle simpliste, les produits en apparent déclin sont nombreux : personnes âgées, handicapés, malades… tous ces « produits » sont des poids morts. Cette façon complètement totalitaire de raisonner, et pourtant sémantiquement assez proche de notre quotidien, feront peut être **le jeu de certains, désirant « optimiser » les « marques » de « produits » et qui proposeront, qui sait, des solutions finales pour être plus « compétitifs ».**

Déjà, le vol dans de gigantesques bases de données privées ou publics laissent entrevoir, peut être, que les « caractéristiques » de chaque individus de la planète seront un jour disponibles à qui le voudra, sur le réseau. En mai 2006, un vol de données sur 26,5 millions d'anciens combattants américains et sur leur épouse, contenant noms, dates de naissance et numéros de sécurité sociale avait défrayé la

[197] Michael Bay, 2004

chronique.

De plus, les premières « puces » implantées tel un code barre sur l'homme, prémices à un contrôle généralisé, voient le jour. Par exemple, un fabricant belge d'armes (FN) teste la faisabilité d'une puce RFID sous cutanée comme moyen de d'identification du détenteur d'une arme. En pratique l'arme ne pourrait être activée que par son seul propriétaire. Et comble de l'ironie, le projet fait référence à une arme dite « intelligente »…Aux Etats-Unis, des employés de Citywatcher, une société de vidéosurveillance[198], se sont fait implanter une puce dans le bras. Le but est de permettre de filtrer l'accès à certains espaces sécurisés dans lesquels la société installe ses équipements. Les autorités sanitaires du pays avaient donné leur aval pour de telles expérimentations dès le mois d'octobre 2004. Dans le domaine de la santé, la société Applied Digital Solutions espère convaincre les Américains de se faire glisser une de leur petite création sous la peau. En cas d'accident, les services de secours n'auraient plus qu'à scanner le bras des victimes pour connaître immédiatement leur groupe sanguin et leur identité…

En France cette fois-ci, l'opérateur mobile Orange du groupe France Télécom débute la commercialisation d'un bracelet doté de fonctions de géolocalisation par GSM et GPS destiné aux quelque 850.000 personnes atteintes de la maladie d'Alzheimer sur notre territoire. Présenté comme une première mondiale, "Columba" répond au problème de la perte de repère spatio-temporel (fugues et/ou désorientation), un des principaux symptômes de cette maladie. Lorsque la personne sort d'un périmètre géographique défini, un message d'alerte est envoyé à la famille sous forme de SMS, d'e-mail ou de message vocal. Les proches du malade vont alors entrer en contact avec un centre d'appels médicalisé qui leur indique précisément où se situe la personne. La famille peut ainsi demander une intervention ou entrer en communication avec le malade grâce à la fonction haut-parleur mains libres du bracelet. La société québécoise fabricante du bracelet a également dans ses cartons un «projet très avancé» de ceinturon pour équiper cette fois les malades cardiaques. Posé sur le thorax, il relève les battements du cœur et envoie une alerte vers un centre d'assistance dès les premiers signes de crise cardiaque[199]…

Mais après les réflexions que nous avons jusqu'à maintenant engagées, peut-on encore parler véritablement de « progrès » lorsque l'homme devient ainsi géré par les machines, comme un produit de consommation courante ?

4-7 Une résistance quasi-impossible sur un réseau de traces

« Tant qu'il y aura des hackers, il n'y aura pas de Big Brother »

(Slogan des hackers)

Internet n'est pas loin d'être un système quasi-parfait sur le papier : relier les hommes entre eux, accès de tous à la connaissance, communication démultipliée et disparition des intermédiaires…Cependant la perfection de l'idéologie est entamée

[198] www.01net.com 08/03/2006
[199] www.zdnet.fr 7/06/2006

par **un inconvénient majeur : la traçabilité et l'enregistrement de n'importe quelle action sur le réseau.**
Beaucoup diront que c'est un point de détail. Cet ouvrage avait entre autre pour but de démontrer le contraire. Sur le réseau, qui va déborder de plus en plus dans la moindre action quotidienne de chaque citoyen, la vraie liberté ne peut passer que par l'anonymat le plus total de chacun. La « trace » laissée et sa possible utilisation font radicalement chuter Internet de son piédestal.
Le rôle des grands média est ici capital. Un quasi-consensus existe aujourd'hui aux niveaux des TIC, comme quoi leur développement est synonyme d'épanouissement et d'évolution pour l'être humain. C'est un progrès. Personne n'ose le réfuter.
Des technologies mégalos développées par des firmes comme Google, ou bien des tentatives de fichages généralisés comme celles entamées par le programme surveillance totale américain, devraient, au-delà des débats techniques et économiques, attirer l'attention. Il n'en est rien. Le Patriot Act 2, qui représentait une forte régression des libertés dans le droit américain, n'a suscité à l'époque que très peu de contestation. « L'information n'a fait guère plus qu'une vaguelette dans les médias américains. »[200]. Les grands réseaux de télévision ont brillé par leur silence, et les journaux par un traitement minimal en pages intérieures.
Ainsi grâce à un traitement médiatique savamment orchestré, les gens redemandent, y compris pour eux même, plus de surveillance et de traçabilité : un sondage publié 10 jours après les bombes du métro londonien indiquait que 74% des Italiens étaient favorables à davantage de caméras dans les lieux publics et 60% à un contrôle plus serré des messages électroniques. [201]

La population continue ses divertissements de télé-réalité pendant que tout se joue en coulisse. Ne devient-il pas urgent, puisque les grandes oligarchies médiatiques et politiques font la sourde oreille, de nous réapproprier enfin notre chemin et de proclamer enfin vouloir mettre un terme à cette matérialisation Orwellienne des choses. Lorsqu'on leur pose la question, les gens paraissent quand même inquiets : une étude de News.com aux Etats-Unis montre la méfiance de la population envers le passeport biométrique américain qui pourrait à terme contenir empreintes digitales et iris de l'œil. Le gouvernement a en effet reçu 98,5% de commentaires négatifs[202].
Mais les applications ont belle et bien commencées. A Ruelzheim en Allemagne, il est désormais possible de payer ses courses au supermarché simplement en posant le doigt sur un lecteur d'empreintes digitales[203]. La chaîne de supermarchés britannique Midcounties Co-operative a mis en place[204] un terminal de paiement à reconnaissance digitale dans trois de ses magasins situés à proximité d'Oxford. Et en plus tout est fait pour rassurer le consommateur et le faire souscrire. Le système est en général simple et gratuit : le client s'enregistre en fournissant une pièce d'identité et ses coordonnées bancaires. En contrepartie, la société scanne son empreinte digitale. Lors de ses achats, le client n'a alors plus qu'à passer son doigt sur le terminal de paiement pour payer ses articles. Exit les cartes bancaires, petite monnaie et autres chéquiers...
La demande de sensationnel de notre époque actuelle n'entraînera probablement jamais dans sa course la révolte des citoyens contre le numérique et ses gigantesques bases de données. Là il n'y a aucun hélicoptères de combat, aucun

[200] Manière de voir n°71 / Le Monde diplomatique / Obsessions sécuritaires / Octobre- Novembre 2003
[201] AFP, 27/07/2005
[202] www.01net.com 26/10/2005
[203] www.wnunet 28/04/005
[204] En mai 2006

porte avions ni autre instrument de guerre. Comment le virtuel pourrait inquiéter quiconque en restant une suite rébarbative de 0 et de 1 recueillie par quelques antennes qui les analysent par millions via des logiciels. En apparence, donc, rien de très intéressant, d'excitant, ni de révoltant pour la population face à la monotonie de ces données binaires[205].
Et ce n'est probablement pas la CNIL qui pourra faire changer les choses en France avec son budget annuel ridicule par rapport à la tache (7 millions d'Euros) et avec un effectif de 80 personnes. Depuis sa création, elle n'a adressé que… 30 avertissements. De quoi permettre au privé comme au public de s'en donner à cœur joie pour l'acquisition, la gestion et la manipulation de données concernant nos vies privées.

Car en coulisse, de sombres manœuvres sont à l'œuvre. Parmi l'une-d'elle un projet de centralisation des systèmes d'information de l'armée qui pourrait lui donner accès aux données de la gendarmerie concernant les justiciables en faisant fusionner ensemble la Direction centrale des télécommunications et de l'informatique et la Direction interarmées des réseaux d'infrastructures et des systèmes d'information (Dirisi). Le problème soulevé est la place réservé aux gendarmes qui sont certes des militaires, mais aussi des officiers de Police et qui tous les jours et à travers tout le pays interviennent dans des enquêtes à la demande des magistrats. Ainsi et en toute discrétion, **les informaticiens de l'armée risquent de compromettre la séparation des pouvoirs entre l'exécutif et le judiciaire** établi pourtant dans notre Constitution.[206]

Certains affirment qu'il est encore possible de « tromper » la biométrie. Des chercheurs japonais ont montré qu'il était possible de reproduire de vraies fausses empreintes digitales, sur des doigts en latex, qui ont leurré 11 des 15 systèmes biométriques testés. A ce sujet on peut évoquer le film « Bienvenue à Gattaca »[207] où l'action se situe dans un monde (biométrique) parfait. Gattaca est un centre d'études et de recherches spatiales pour des jeunes gens au patrimoine génétique impeccable. Vincent (joué par Ethan Hawke), enfant naturel au patrimoine génétique quelconque, mais qui rêve de partir pour l'espace, va déjouer les lois de ce monde moderne pour réaliser son objectif. Ce film pose toujours la même question : est-ce d'un monde comme celui là que nous désirons ?
Un nouveau Staline visant à asseoir son pouvoir ne s'y prendrait pourtant peut être pas autrement que ce que les Occidentaux font d'eux même, c'est-à-dire s'équiper de téléphones portables, d'ordinateurs connectés, de webcams, de GPS… Les systèmes totalitaires de gauche tant décriés – avec raison – par le passé n'ont jamais exercé sur les populations **une surveillance et des capacités de contrôle comme celle qu'annonce et met en place la fusion des TIC et du libéralisme économique.** Des progrès technologiques qui ne servirait qu'à asservir ?

Un autre problème de ces tendances sécuritaires en tout genre, c'est qu'il est extrêmement difficile, une fois le processus engagé, de revenir en arrière. En effet, au niveau législatif par exemple, quel législateur proposerait l'annulation d'une loi anti-terroriste en prenant le risque qu'un nouvel attentat se perpétue. Les services de police ne lâcheront pas non plus leurs nouveaux pouvoirs si facilement. Il ne faut pas

[205] Tous fichés, J. Henno
[206] www.01net.com 10/11/205
[207] De Andrew Niccol, 1997

rêver, ces mesures sont faites pour durer. Même chose pour les firmes privées qui ne laisseront pas fuir leur part de marché si l'on tentait de réglementer quoi que ce soit qui revienne sur leur acquis. N'oublions pas que public et privé se doivent d'être solidaires dans la « guerre économique » que se livrent les nations ! Dernièrement, le FBI a officiellement mis à l'honneur neuf des collaborateurs de Microsoft pour avoir rendu un « service exceptionnel à la cause publique » : ils ont en effet réussi à localiser des pirates informatiques à l'origine d'un virus. Le FBI, grâce à cette information, a réussi à arrêter rapidement les 3 coupables[208].

Les adolescents pressentent bien le carcan dans lequel on veut les faire rentrer. Ils essayent d'y échapper, peut être inconsciemment, à leur manière, avec leurs outils : 6 d'entre eux sur 10 préfèrent utiliser un nom d'emprunt sur Internet pour protéger leur véritable identité[209]. Pourtant à côté de cela, ils sont de loin la génération la plus forte consommatrice en TIC : 95% des jeunes européens âgés de 12 à 18 ans ont leur propre téléphone portable[210]. Et comme l'explique Médiappro : « Il est clair que pour eux, **cela est d'une importance vitale et qu'ils trouveraient difficiles de vivre sans** ».
Car le souci est bien celui-ci : on veut nous faire rentrer dans la norme en adhérant au rouleau compresseur technologique : l'exemple de la « smart vision » (la « vision intelligente ») testée dans les métros de Londres, Paris et Milan est édifiante à ce propos. Ces caméras sont capables de détecter chez les voyageurs les comportements « qui s'écartent de la norme ». « Il y a des endroits dans le métro où il n'y a pas de lieu de stationnement, sinon le système associe cela à une situation dangereuse, du moins suspecte. » Relié à l'ensemble du réseau des caméras, l'ordinateur est muni de logiciels de détection : à peine le « suspect », le vendeur à la sauvette ou le mendiant arrive-t-il dans le métro qu'il est immédiatement repéré. S'il reste immobile plus d'une minute, son image passe au vert sur l'écran de contrôle. Au-delà de 2 minutes, elle vire au rouge et l'alerte est lancée. Rester immobile trop longtemps, ne pas marcher dans le bon sens, stationner en groupe, franchir des zones interdites deviennent autant de comportements louches…que les caméras dénoncent sur le champ. Celui qui ne bouge pas n'est pas conforme au flux incessant des nomades du productivisme.
Une étape supplémentaire a été franchie dans la ville de Newham dans la banlieue de Londres : celle de la reconnaissance faciale. Dans la rue, des caméras biométriques scannent le visage des passants. Systématiquement, l'ordinateur compare ces portraits à ceux des fichiers de la police. Son objectif : détecter dans la foule les personnes recherchées. Difficile de comprendre la tolérance de l'opinion publique envers un tel système de surveillance…L'homme n'a plus le dernier mot : connecté à un immense réseau de caméras, l'ordinateur se transforme en juge implacable[211] .

Déjà le marché anticipe la création et la formation d'une « résistance » à cette guerre du numérique. En témoigne par exemple la création d'un « Spyland », parc d'attraction sur la thématique de l'espionnage, près de Valence en France, dont l'ouverture est prévue début 2008. En outre, des formations en intelligence économique fleurissent un peu de partout et préparent déjà la jeunesse à être acteur

[208] www.fr.computermagazine.be 26/09/2006
[209] www.canoe.com , 09/11/2005
[210] selon une étude menée dans neuf pays européens par le consortium Mediappro.
[211] Manière de voir n°71, le Monde Diplomatique, Obsessions Sécuritaires.

de cette guerre économique. Pour la rentrée des classes 2006, l'Université d'Albertay en Ecosse a même décidé d'ouvrir pour les étudiants des cours de « hacking éthique » qui leur apprennent comment cracker, entre autres, logins et mots de passe pour s'introduire dans les systèmes protégés, suite aux demandes des entreprises qui demandent de plus en plus des spécialistes pour gérer leurs brèches de sécurité. Des experts internationaux de tous domaines interrogés en 2006 pour l'étude de l'institut Pew et d'Elon University prédisent, à 58% que dans le cyber monde qui s'annonce version 2020, des groupes de « refuznik » hostiles à la technologie feront leur apparition et que certains auront recours à des actions terroristes pour perturber le fonctionnement de l'Internet[212] !

La guerre du numérique aura-t-elle lieu ? En tous beaucoup d'Etats occidentaux s'y préparent. Du 6 au 10 février 2006, les Américains ont joué à se faire peur avec une simulation d'attaque informatique baptisée « Cyber Storm ». Elle consistait à reproduire une attaque informatique de grande ampleur touchant les systèmes bancaires, les infrastructures de communication, les transports en commun… Pour être le plus réaliste possible, cette opération a mobilisé quelque 300 personnes, réparties dans cinq pays (Etats-Unis, Canada, Royaume-Uni, Australie et Nouvelle-Zélande) et aurait coûté plus de 3 millions de dollars. Ce type de simulation n'est pas propre aux Etats-Unis. L'Otan en fait aussi avec son exercice annuel baptisé *« Digital Storm ».* Quant à la France, elle organise sa propre opération, « Plan Piranet ». Ce plan de réaction *« en cas d'attaque informatique terroriste d'ampleur »* contre l'Etat a été développé, à la suite des attentats du 11 septembre 2001 aux Etats-Unis. Le premier Piranet remonte à 2003. Le dernier a été réalisé fin 2005. Le prochain est « secret défense »[213]…

Plus généralement, dans un monde parano en devenir (ce qui n'est pas le cas, rappelons-le aujourd'hui, mais une voie dans laquelle si nous n'y prenons pas garde, pourrait s'engager nos sociétés), on peut se demander si désobéir aux règles mises en place par ces états, en apparence démocratiques, deviendra encore possible ? En effet la **toute puissance d'un réseau mondial traçant chaque individu jusque dans le moindre recoin de son intimité grâce aux objets nomades et biométriques**, qui pourront se transformer le cas échéant en prothèse adaptée à chacun, **laisse douter très fortement d'une résistance possible de quelques groupuscules quels qu'ils soient.** A terme peut-être, les mailles seront tellement resserrées qu'une désobéissance serait ainsi devenue quasiment irréalisable.. En attendant, on peut s'engager (une liste des associations oeuvrant concrètement dans le domaine des libertés individuelles est précisée à la fin de l'ouvrage) : la puissance des démocraties est encore au service des citoyens, certes désinformés et avec des parlements affaiblis pour des causes de « sécurité intérieure », mais encore capable du meilleur si nous le voulons bien. Dans tous **ces groupes de réflexions** que vous pourrez constituer, **l'émergence d'un nouveau paradigme** de société pourrait trouver les moyens de se conceptualiser et de faire changer, enfin, radicalement les choses.

[212] www.elon.edu/predictions
[213] www.01net.com 27/09/2006

5 Conclusion

« Une erreur ne devient une faute que si l'on refuse de la corriger »
John Fitzgerald Kennedy

5-1 Vers une redéfinition des buts et fins de la société

« Et les mans faut faire la part des choses
Il est grand temps de faire une pause
De troquer cette vie morose
Contre le parfum d'une rose »
Tryo, L'hymne de nos campagnes

L'association « L'Europe des consciences » à l'époque animée par une vingtaine de personnalités tel que Pierre Rabhi, faisait le constat alarmant que l'Europe, dans sa construction politique actuelle, ne prenait réellement en compte que les dimensions économiques et financières : « Tout entière immergér dans la résolution des problèmes du quotidien, apparemment sans vision sur le long terme, **notre société semble avoir perdu la conscience que les principes de spiritualité, écologie, solidarité sont les fondements essentiels et incontournables d'une société**, qu'ils appartiennent aux lois de la vie, aux lois de l'univers et qu'ils représentent souvent le simple bon sens…Il serait facile de multiplier les exemples qui montrent ce divorce entre une aspiration de plus en plus large à un changement – rupture avec l'idéologie du scientisme, du progrès, de la croissance économique, du bonheur apporté par la consommation, du rationalisme exclusif – et un immobilisme social où se pérennisent attitudes et structures archaïques…Tout entier tourné vers l'avoir et le pouvoir, l'homme moderne s'est trop souvent coupé de sa dimension la plus profonde par laquelle sa vie acquiert sens et plénitude. C'est lorsqu'il est connecté en lui à la source de toute vie que l'homme peut développer vision juste et action juste. Il participe alors à la danse et à l'harmonie de l'univers, et en respectant ses lois, il vit dans la joie, la conscience et la liberté. »

Après la lecture des chapitres précédents, on peut effectivement se poser la question du pourquoi à de telles dérives et surtout à qui cela profite-t-il ? En effet, nous sommes en train, inconsciemment, de tisser notre propre enfer si les choses continuent ainsi sur la voie où elles paraissent s'engager. De soi-disant raisons économiques et techniques contribuent à faire d'Internet un système de plus en plus contrôlé. Mais sans le consentement aveugle de nous, Internautes et citoyens, rien ne se passerait. En fait, grâce aux innovations constantes des TIC, l'individu étend considérablement ses pouvoirs matériels sur son environnement, et il est difficile de sortir de cette excitation permanente du « toujours plus ». Bien qu'il ne s'en rende pas toujours compte dans ces temps de désinformation, l'individu à aujourd'hui devant lui un choix fondamental à opérer, celui de continuer sur cette pente

technologique et matérielle apparemment infinie qui peut lui faire croire qu'il est un véritable Dieu, soit de revenir à un rythme d'évolution en accord avec les lois naturelles et plus responsable de notre humanité. En effet **jamais le rythme de l'information d'une part, et les cycles naturels d'autre part, n'ont été à ce point dissociés**. Une graine prend son temps pour germer, un arbre pour grandir, une vigne pour donner du fruit… Or, les humains, qui sont censés eux-mêmes faire partie du cycle naturel sont pour beaucoup en train de s'en désolidariser en optant pour une course technologique effrénée contre le temps. On peut retenir qu'aujourd'hui, en 24 heures, nous recevons la même quantité d'information que nos ancêtres d'il y a 400 ans recevaient en 6 mois[214] !
Or la finalité de toute société humaine n'est-elle pas de rendre chacun de ses membres heureux, en harmonie avec tous les règnes naturels, et en leur permettant individuellement d'exploiter au mieux leur potentiel d'évolution ? Aujourd'hui c'est une véritable caricature de cette description qui se déroule (très bien illustrée d'ailleurs dans la publicité actuelle).

Réfléchissons maintenant quelques instant à notre système économique. Un ouvrier Y travaille dans une entreprise X. Celle-ci, faute d'être assez compétitive, licencie des salariés, dont l'ouvrier Y. En situation de précarité et avec un pouvoir d'achat, malgré les assurances chômage, à la baisse, Y ne peut plus acheter des produits de l'entreprise X. Si cette démarche est généralisée à l'ensemble du monde économique, les Y n'ont plus les moyens d'acheter les produits des entreprises X. Que faire alors ? Pour gagner en productivité et survivre, les X doivent donc licencier des Y…et ainsi de suite. On arrive donc à un système schizophrène qui s'appauvrit à grande vitesse, où la faute n'est à personne, chacun pensant, de l'ouvrier au patron, faire de son mieux. Lorsque, et c'est se qui se passe, on arrive à de telles aberrations, au niveau mondial, il est sérieusement temps de réfléchir sur les finalités d'une telle société.

Jean Peyrelevade, ancien Président du Crédit Lyonnais est aussi pour sa part devenu assez critique par rapport au système qu'il a servi, aux plus hauts échelons pendant des années. Dans son dernier livre « Le capitalisme total » (Seuil, 2005), selon lui, « le manager, celui qui commande au travail salarié, est lui-même un salarié, certes de luxe : le monarque est prisonnier de sa cour. Soumis aux règles de la *corporate governance,* contrôlé par un conseil largement composé d'administrateurs indépendants, surveillé par un président non-éxécutif, dépendant pour sa condition matérielle d'un comité des rémunérations dont les décisions seront bientôt soumises au vote formel de l'assemblée générale, devant présenter des comptes à un comité d'audit qui appliquera des normes comptables à caractère bientôt mondial, sa marge de liberté est réduite à peu de choses : il n'est plus que l'intendant du domaine, le serviteur zélé de la collectivité des actionnaires dont il lui revient d'assurer l'enrichissement. »… « Force du capitalisme contemporain : d'un côté l'émiettement des actionnaires de bases aux intérêts divergents (s'enrichir), protégés par leur anonymat aussi bien que par leur nombre et la banalité de leur condition qui leur confèrent une sorte de légitimité démocratique. De l'autre, l'industrie des gestions (ils gèrent environ 15 000 Milliards de Dollars) à qui l'on ne saurait imputer les défauts du système puisqu'elle agit non pour son propre compte, mais pour autrui. Où est le crime s'il n'y a pas de coupable ? ».

[214] Biocontact, Décembre 2006

Autrement dit, à chaque niveau de l'échelle de cette « gigantesque société anonyme » que forme le capitalisme moderne, tout le monde essaie de faire de son mieux. Les salariés, en général, font de leur mieux pour garder leur travail et doivent rendre des comptes à leur patron. Les patrons, en général, font de leur mieux pour garder leur travail et doivent rendre des comptes à leurs actionnaires. Une partie de ces derniers (les gestionnaires de fonds par exemple), font de leur mieux pour garder leur travail et doivent rendre des comptes à leurs clients. Le comble, c'est que ces « clients » sont des salariés ou des patrons qui demandent de plus en plus de rendements à leurs actions et qui mettent donc une très forte pression dans les entreprises…où ils travaillent ! Sadomasochisme ? Là encore, la faute à personne ? Pour Peyrelevade, le capitalisme continue de s'étendre, mais « à quelle fin autre que son propre enrichissement, nul ne sait. Personne ne connaît le promoteur de ce vaste chantier. L'architecte en est inconnu et les plans inaccessibles… Nous y consacrons l'essentiel de notre temps de travail…**Nous sommes, sous l'apparence de la liberté, devenus dépendants**. »
Analyse que nous ne suivons pas jusqu'au bout, car une partie des gros actionnaires, eux, n'ont à rendre de compte à personne sinon à eux-mêmes, et demandent, consciemment, toujours plus au rendement de leur capital. Ainsi, lorsqu'on remonte dans les plus hauts échelons de la pyramide, métaphore de nos sociétés Occidentales, on peut, par ce raisonnement, finalement pas si simpliste, retrouver les grandes institutions financières (banques…) et les familles détentrices du grand capital si précocement dénoncé par Marx. Le véritable pouvoir matériel, puisque nos démocraties pyramidales se sont construites sur des rêves de croissances économiques infinies, est donc entre leurs mains.
Même en étant conscient de cet état de fait, la solution ne passe probablement pas par une **lutte effrénée contre** ces assoiffés de pouvoir et d'argent, mais, peut-être, par le fait de s'en **désintéresser** progressivement. C'est bien facile et commode à vrai dire de toujours vouloir trouver **un bouc émissaire** à tous nos problèmes. L'équilibre fondamental à retrouver passera peut-être, d'abord, par une **réappropriation de notre propre pouvoir individuel**.

5-2 Ne pas rentrer dans le jeu de la peur et de la panique

« Nous approchons nécessairement d'un âge nouveau où le monde rejettera ses chaînes pour s'abandonner enfin aux pouvoir de ses affinités internes ».
Teilhard de Chardin

Ce livre n'a évidemment pas vocation à susciter la peur, bien au contraire. En effet, les scénarios, tels qu'exposés dans l'ouvrage sont encore improbables tant que chaque individu n'y soumet pas son propre consentement. Ce livre, se fondant sur des exemples récoltés un peu partout dans le monde, n'est encore que de l'anticipation puisque aucun état n'a encore choisi la voie du « tout numérique ». Le choix est encore totalement à notre portée. Voulons-nous d'une société où l'inconnu n'existe plus, ou tout soit planifié et contrôlé par avance pour garantir une sécurité totale (illusoire) aux adeptes d'un tel système ? Sans doute les dérèglements vont s'intensifier, peut-être les attentats monter encore en puissance, **mais la sécurisation à outrance sur le plan matériel, contrairement à ce que peuvent penser les Américains, n'est pas la solution ultime au problème.** Pour trouver la paix extérieure, la clef ne passe probablement pas par une technologie là aussi toute extérieure, mais par une résolution, au niveau de chaque individu, de ses propres

conflits internes. Il est illusoire de vouloir trouver une paix universelle si chaque personne composant la société n'est pas en paix avec elle-même. **La plus grande chose que chaque être humain puisse offrir à la société** est de **retrouver son propre équilibre**, bien souvent égaré en ces temps de dispersion et d'agitation.

Faisons là une petite digression et constatons que contrairement à ce qu'on a l'habitude de penser, la haine n'est pas le contraire de l'amour : **le contraire de l'amour, c'est la peur**. Effectivement, par la suite, de la peur peuvent découler des sentiments comme la haine, la jalousie, la xénophobie. Si chacun avait le sentiment profond d'être relié par le haut au niveau spirituel à **un amour tellement intense, inconditionnel** et qui nous dépasse tous, alors les guerres et les actes de barbarie auraient pris fin depuis bien longtemps.
La peur est l'arme des puissants qui s'en servent et s'en serviront pour réduire à néant toute opposition à leurs sombres projets. Déjà en avoir conscience, c'est s'en détacher et mettre un espace vital entre soi et la peur. C'est ne plus en être esclave. En grossissant il est vrai un peu le trait, on pourrait dire que des systèmes de panique généralisée sont en train de se mettre en place en France (mais aussi dans le reste du monde), via par exemple email et Sms[215]. Le gouvernement a en effet étendu aux FAI et aux opérateurs de téléphonie mobile l'obligation de relayer les messages d'alerte en cas de catastrophe. Or tous les médecins vous diront que l'angoisse est pathogène et que le stress fait baisser les propriétés du système immunitaire de manière très importante. On imagine bien le climat de panique total que pourrait susciter une alerte par l'envoi massif de Sms dans une grande ville par exemple. Bien sû,r nous ne disons pas qu'il vaut mieux ne pas être informé. Mais une telle opération de peur hyper médiatisée pourrait faire plus de victimes que de rescapés.

Il faut bien discerner que nos sociétés actuelles fonctionnent sur un système pyramidal, avec de plus en plus de pouvoir de contrôle sur la masse au fur à mesure qu'on s'approche du sommet. Le gros souci pour ces « puissants », c'est que la population en général, en proie à devenir de plus en plus consciente des réalités, est sur le point de ne plus vouloir accepter leur « dictature » si bien orchestrée. **Leur dernière carte pour garder le pouvoir** se joue (c'est, bien sûr, seulement une hypothèse), **peut-être** en plusieurs étapes en s'appuyant sur la virtualisation/sur-matérialisation du monde via Internet. Voici ce que pourrait être leur dernière « recette de cuisine » :

- Mélanger délicatement, pendant quelques années, Internet avec des croyances effectivement vraies jusqu'alors, comme quoi il est un formidable espace de libertés.
- Pousser dans la marmite le plus de gens possible, les administrations, le privé… et les inciter à s'y exprimer (web 2.0, mail, VoiP, blogs…) en faisant passer par le réseau toutes leurs activités quotidiennes.
- Une fois la mayonnaise bien prise, passez à l'étape de surveillance systématique et totale des individus.

La question sur la dernière étape de la recette, alors qu'elle n'en est qu'à ses tout début, est : mais qui va la préparer, qui va donc la mettre en place ?
Et bien encore une fois, les « puissants », bien trop peu nombreux, comptent peut-être sur notre belle naïveté et notre incrédulité pour être les acteurs de ce sombre

[215] www.zdnet.fr 21/10/2005

scénario. En effet, il faut bien des « gens » pour contrôler tout le monde, même si les progrès de l'informatique auront simplifiés à l'extrême leur travail en focalisant automatiquement ceux qui sortent de la norme. Effectivement les « puissants » ne peuvent rien sans nous et notre consentement. Exemple de cet extrême déséquilibre entretenu, on sait que la richesse totale du milliard d'êtres humains les plus déshérités est égale à celle des 100 les plus riches, et, encore plus largement que la somme des 350 premières fortunes personnelles correspond à celles des 2,3 milliards d'habitants les plus pauvres !
L'idée est donc peut être, dès le départ, de ne pas rentrer dans leur plan : **« Il n'y a rien à faire contre eux, mais tout à faire sans eux »**[216]. La dignité de l'homme passe par la création d'un scénario qui lui corresponde enfin, et par le rejet de toute sorte d'aliénation comme celle que l'on pressent pouvoir devenir une possibilité.

5-3 Le droit à l'oubli

« La mémoire est souvent la qualité de la sottise »

Chateaubriand

Le droit à l'oubli est une notion issue de la doctrine. Il fait référence à la protection des droits des personnes contre les risques du temps et de la mémoire activée. L'informatique permet de conserver indéfiniment les données personnelles. La loi a donc prévu un droit à l'oubli, afin que les personnes ne soient pas marquées à vie par tel ou tel événement.
La CNIL en France reconnaît ce « droit à l'oubli » au bout d'un certain temps, c'est-à-dire concrètement que les coordonnées d'une personne, inscrites sur des fichiers informatiques que ce soit par des administrations ou des entreprises privées, doivent disparaître au bout d'un certain temps. Sur son site Internet on apprend que « la fixation de la durée de conservation et l'existence de procédés de mise à jour doivent permettre le respect du principe de « droit à l'oubli ». Par exemple pour le fichage d'impayés, ce principe se traduit par la suppression de l'inscription dès régularisation de l'incident ».
La contradiction potentielle entre obligation de conserver et devoir de destruction est particulièrement complexe dans les projets relatifs à l'archivage des e-mails puisqu'on y retrouve invariablement une dimension courrier personnel des salariés censés bénéficier du secret de la correspondance.
En fait, **la question de l'archivage électronique et de la protection des données personnelles** renvoie classiquement à l'univers de **la confiance** : on ne peut pas faire confiance à un interlocuteur qui n'oublie jamais rien et qui finit par mieux vous connaître que vous-même ; qui dispose de la faculté de communiquer cette connaissance à des tiers. Inversement, on ne peut entretenir une relation de confiance avec un organisme amnésique qui ne conserve pas le souvenir des transactions et des engagements.

Ainsi, un équilibre devrait être trouvé entre « le droit à l'oubli » et « le devoir de mémoire » et aboutir à une synthèse adéquate. Malheureusement pour les libertés individuelles, on est peut être en train de s'acheminer vers un extrême, une mémoire « eidétique », c'est-à-dire capable de reconstituer fidèlement tout événement passé.

[216] www.onpeutlefaire.com

La réglementation n'étant pas claire, la CPAM de Toulouse à tranché : « Le cahier des charges prévoit de pouvoir accéder, à partir d'un dossier d'un assuré, à tous les documents le concernant. Dans cette logique, nous prévoyons, pour l'instant, de tout archiver »[217].
Il faut être conscient qu'il existe une pression de la part des pouvoirs publics pour inciter les entreprises à conserver les données, pour être capable de faire face à des contrôles, pour des objectifs de sécurité publique ou de lutte contre le blanchiment. Le 1er septembre 2006, un arrêté du Ministère de la Justice est paru détaillant l'indemnisation prévue par le gouvernement pour les opérateurs de téléphonie mobile et fixe (opérateurs Internet compris) due au surcoût pour la conservation des « logs » de connexion (qui, rappelons-le, est d'une durée de 1 an en France). 25 situations sont ainsi répertoriées et classifiées : par exemple, le détail des communications d'un abonné sur 1 mois (avec date, heure et durée). L'indemnisation la plus élevée concerne le détail géolocalisé des communications d'un abonné sur un mois, avec adresse du relais téléphonique. Le prix : 35 euros, identification de l'abonné non comprise[218].

Deux tendances de fond majeures laisse à penser que la conservation des données va s'accélérer : **le prix toujours revu à la baisse de la mémoire informatique** et **le développement du marché de la vie privée**.
En effet, il paraît assez clair que les traces laissées sur le net (au sens large) vont faire l'objet d'archivage de masse pour assouvir, sans doute, la puissance de certains capitalistes lorgnant sur ce nouvel Eldorado qui s'ouvre à eux. Les politiques comprendront aussi vite l'intérêt de tout ficher et surtout de tout conserver pour toujours les mêmes sempiternelles raisons de soi-disant sécurité du territoire et de lutte systématique contre toute infraction. Pour une fois l'informatique et le marketing partageront une même conception conservatrice. Chez les personnes en charge de la sécurité informatique, on trouvera fréquemment la volonté de conserver au maximum à des fins de traçabilité et de reconstitution. Parallèlement, une certaine vision du marketing décisionnel poussera à adopter le raisonnement suivant : « le datamining fait des progrès continuels en matière de coût et de performance, donc conservons tout, cela pourra toujours servir un jour. »

Comme précisé au 1er chapitre, Internet est bâti sur une infrastructure de traces, et c'est bien ce qui pose problème. Grâce aux adresses IP, sorte de numéro d'identification sur le réseau d'un ordinateur et, bientôt, d'un terminal nomade, on peut savoir qui se connecte à qui ou à quoi et ainsi apprendre beaucoup d'informations sur l'internaute. Mais il faut savoir de plus que ces informations sont **enregistrées dans la matière la plus dense qui soit** : un disque dur ou une mémoire. En effet, et ce en apparence, grâce aujourd'hui à l'ADSL et demain au **Wifi généralisé, les informations paraîtront totalement libres, puisqu'elles circuleront même dans les « airs ».** Mais tout ceci n'est qu'une parodie. Il faut bien voir que ces informations quelles qu'elles soient proviennent d'un terminal doté d'une mémoire (ordinateurs, téléphones portables, PDA…) qui doit au préalable les enregistrer s'il veut les transmettre ensuite sur le réseau. Ainsi les informations que l'on croit voir apparaître comme par magie, sur son ordinateur, par exemple lors d'une connexion à Internet, proviennent d'un disque dur (d'un serveur par exemple)

[217] 01 Informatique, 28/11/2005
[218] www.01net.com 01/09/2006

d'une autre machine. **Elles sont non seulement enregistrées dessus**, mais le mot a perdu de sa force. Nous dirions plutôt **« engrammées » tellement la densification de ces informations est importante** sur un tel support.
En effet il faut voir qu'il y a une énorme faille de sécurité sur la plupart des ordinateurs. Lorsque par exemple sous Windows vous supprimez un fichier, il va directement dans la corbeille. Et une fois que vous « videz » la corbeille, le fichier en question n'est en réalité pas réellement supprimé, mais reste toujours présent sur le disque dur et peut, par certaines méthodes, être restauré, c'est-à-dire récupéré. Certaines sociétés spécialisées dans ce type de prestations de restauration de données explique qu'il faut les « écraser » entre 5 et 8 fois pour être sur qu'on ne puisse les récupérer. Le ministère Américain de la défense a mis au point une technique du nom de code DoD 5220.22-M/NISPOM 8 – 36 grâce à laquelle les données seraient supprimé définitivement. Le must en la matière est la méthode Gutmann. Elle est conforme aux exigences de sécurité de la NSA (National Security Agency) et dans ce cas **l'espace disque est écrasé 35 fois** selon un procédé particulier. A noter que ces technologies sont disponibles pour le particulier depuis de nombreux logiciels traitant d'anonymat et de sécurité.
En août dernier, la BBC pointait déjà les négligences des sociétés britanniques lors du recyclage de leur PC. Les disques durs renfermaient toujours leur précieux butin, en dépit de leur passage par des filières de recyclage censées conduire à un formatage complet. Expédiés pour beaucoup en Afrique, des enquêteurs ont par exemple relevés que les données bancaires de milliers de Britanniques étaient en vente sur le continent pour seulement 30 euros chacune[219]. Pire, si l'on en croit l'éditeur de solutions de sécurité mobile Trust Digital, à partir de 9 appareils mobiles sur 10 achetés sur Ebay (PDA et Smartphone), son équipe d'ingénieurs a réussi à extraire près de 27.000 pages de données personnelles et professionnelles. Parmi les données récupérées, on a relevé notamment des informations bancaires et fiscales personnelles, des notes sur les activités commerciales de certaines entreprises, des dossiers clients, des fiches produits, des carnets d'adresses, des enregistrements téléphoniques, des logs web et des enregistrements de calendrier. Les personnes chargées d'étude ont également relevé des correspondances personnelles et professionnelles, des mots de passe informatiques, des informations médicales et d'autres données privées, ainsi que des informations relatives à des concurrents ou des données potentiellement à risque[220].
Déjà des sociétés se sont spécialisées dans la destruction de données sur micro-ordinateurs portables perdus ou volés. Si la machine demeure en veille pendant une durée spécifiée ou si elle reçoit une alerte par exemple du site web de la société LogMeIn.com, le système nettoiera automatiquement certains fichiers ou dossiers ou bien encore l'intégralité du contenu du disque dur, suivant la configuration choisie par l'utilisateur. Un historique en ligne des portables volés disponibles sera par ailleurs proposé dès que l'utilisateur se connectera au service LogMeIn. Grâce à cette option, l'utilisateur pourra contrôler le lieu et le moment où son ordinateur a été utilisé sur une période donnée. Déjà, aux Etats-Unis, la police a réussi à remettre la main

[219] Les résultats de l'enquête de la BBC arrivent une semaine après ceux d'une étude analogue conduite par l'université de Glamorgan (Royaume-Uni). Sur la base de 317 disques durs d'occasion provenant d'Amérique du Nord, d'Allemagne et d'Australie, les chercheurs ont découvert que 21 % d'entre eux détenaient des données personnelles et 5 % des informations commerciales appartenant à des entreprises. Seulement 41 % des disques se sont avérés illisibles. Source : Jdn solutions, 17/08/2006
[220] www.vnunet.fr 31/08/2006

sur plusieurs portables volés et à appréhender les voleurs, d'après le directeur exécutif de LogMeIn, Mike Simons[221].

Ainsi, Internet apparaît certes, et ce n'est pas un scoop, comme la virtualisation du monde. Mais d'après ce bref exposé, il apparaît également comme **la matérialisation la plus dense de la quasi-totalité des connaissances et des échanges humains.**

N'est-ce pas en fait un peu comme si chaque homme allait **confier au réseau et à une matière ultra-dense, son intimité**, sa vie quotidienne et privée, pour des raisons pragmatiques, économique, etc. ? Mais aussi essentiellement à cause de la « sécurité » qu'il croit que le réseau pourra dans, sa toute puissance, lui apporter pour lui et pour ses pairs. C'est, peut être, trop s'en fier à son petit microcosme technologique matériel que l'homme pense avoir créé pour son bien être, et en oublier sa transcendance spirituelle et l'infini création qui l'a pourtant toujours conduit, soutenu et protégé, jusqu'où il en est arrivé actuellement.

5 - 4 Le gigantesque test planétaire pour le contrôle systématique

« La trop grande sécurité des peuples est toujours l'avant coureur de leur servitude » »

Jean Paul Marat

- Montée de l'hyper individualisme
- Miniaturisation (nanotechnologies) et utilisation croissante des puces RFID
- Recours croissant aux données biométriques
- Convergence dans un seul « tuyau » (IP) de tous les échanges humains, tant sur la forme que dans les contenus
- Emergence du marché de la vie privée
- Vote de textes législatifs légalisant de plus en plus la « surveillance » en tout genre.
- Apparition d'outils (link analysis) de contrôle de réseaux très poussé.
- Multiplication des séries TV et films sur les techniques policières et l'espionnage.
- Discours médiatique univoque sur la voie du « tout sécuritaire »
- Connexion au réseau volontairement ou non de plus en plus systématique
- L'économie, cheval de Troie de la mise en réseau de tous les citoyens.
- Multiplication des formations au « renseignement », notamment économique
- Arrivé dans le monde adulte de la « génération Internet »
- Mémoire quasi infinie du réseau
- Présentation d'un Internet toujours sous son côté « sympathique »
- Argent de plus en plus virtuel (carte bleue, carte moneo, transaction Internet…) et traçable. Disparition progressive

[221] www.vnunet.fr 27/09/2006

de l'argent liquide.

- Intérêts conservateurs convergents des grandes firmes privées et des nations

Ce tableau synthétique peut nous aiguiller sur les grandes tendances que pourrait prendre notre aventure humaine. Ces données, prises individuellement, comme lorsqu'elles sont « saucissonnées » par les grands médias, ne peuvent rien dégager de particulier ou sinon pour quelques-unes un certain enthousiasme quant à l'émergence d'une fantastique société de l'information. Rassemblées, ces affirmations peuvent par contre donner le tournis : elles pourraient faire penser aux prémices d'un **gigantesque film d'espionnage** joué au niveau planétaire, où **chacun surveillerait son voisin pour le bien de la société.** Pourtant, même si l'excitation est réelle au départ, se prendre pour un « James Bond » en puissance n'est en réalité pas une sinécure. Ce modèle de société que l'on est en passe de nous proposer **n'amène que des luttes acharnées** entre les hommes et reporte toujours plus loin le véritable idéal de paix.

Un « big crush » est prévu par de nombreux experts internationaux dans les années qui viennent qui pourrait paralyser, voir détruire en grande partie le réseau Internet (qui à l'heure actuel reste sur beaucoup de points assez artisanal, et donc de fait encore assez protecteur de nos libertés.)
Si ceci arrive, ce pourrait alors être perçu comme une véritable catastrophe au niveau individuel et collectif, la virtualisation ayant, nous l'avons abondamment décrit, pris petit à petit forme dans beaucoup de nos activités quotidiennes. Et des gens de pouvoir pourraient alors décider de **reconstruire un Internet inquisiteur**, à leur image, puisque la technologie est presque mûre, en forçant la population à passer systématiquement par le réseau dans leur vie quotidienne, même sans s'en rendre compte (on a déjà évoqué cet Internet « invisible », notamment par l'intermédiaire du Wifi et des technologies sans fil).
Mais ce pourrait être aussi vu comme **une formidable opportunité** de construire enfin un **véritable réseau solidaire**, ou chaque être humain, conscient de ses responsabilités, pourrait apporter sa pierre à l'édifice. Dans cette conscientisation chez chacun de ses droits mais aussi de ses devoirs (et ce qu'on appelle la responsabilité personnelle), **la confiance mutuelle pourrait enfin apparaître. Cette confiance**, qui nous manque tant aujourd'hui et **que le réseau actuel semble de plus en plus vouloir saper**, impliquerait qu'il ne soit plus nécessaire pour des raisons notamment sécuritaires de tout savoir sur chaque individu. **L'anonymat le plus total pourrait alors être décrété sur le réseau** (avec des IP variables, des remises à zéro régulièrement de certaines mémoires, et sûrement de bien d'autres choses créatives dont vous pouvez aller discuter sur le forum http://vieprivee.forumpro.fr spécialement créé pour cet ouvrage).

La technologie recèle la dualité : en soi, elle n'est ni mauvaise, ni bonne, tout dépend de ce que l'homme voudra bien en faire. Encore une fois **l'humanité a le choix** (ce que nous avons vu à plusieurs endroits clés dans le livre) de savoir quel type de société elle veut développer : continuer à foncer droit dans le mur dans son délire technologique ou développer un réseau qui ne soit pas une fin en soi à la botte des plus puissants, mais qui reste quoi qu'**il en soit toujours au service de tous les hommes et pour le plus grand bien de tous les règnes naturels de la planète.**

Après ce possible big crush, si la solution 100% technologique était poursuivie, les hommes laisseraient alors définitivement leur pouvoir aux forces de la matière. En effet, la sécurité, au niveau du réseau et de la vie de tout un chacun deviendrait la norme. On pourrait alors imaginer un superordinateur (pourquoi pas composé de chacun de nos PC individuels) extrêmement puissant qui enregistrerait toutes les opérations faites sur le réseau, c'est-à-dire la « forme » que prendrait la communication (qui communique avec qui, à quelle heure, combien de temps, etc.) mais aussi le « fond » (c'est-à-dire concrètement le contenu des données échangées et des conversations émises). On pourrait bien sûr continuer le délire totalitaire avec la mise en place sur chaque humain d'une puce (RFID) sous la peau. Plus possible alors d'émettre un seul mouvement sans que le réseau ne soit tenu au courant. **Le vrai totalitarisme n'est pas,** comme on pourrait tout d'abord le penser si on se réfère au passé, **d'interdire la population d'accéder** (via le réseau) **à certaines informations, mais plutôt,** sous des arguments de liberté totale, **de l'autoriser mais de s'en souvenir systématiquement.**
Ils auront alors gagné. Mais qui sont donc ces « ils » alors que **plus de 99% de la population ne veut pas vouloir cela arriver.**
Or la force de la démocratie devrait faire en sorte, en théorie, que le pouvoir appartienne aux citoyens. Bien sur, la désinformation actuelle ne nous pousse pas toujours à prendre les meilleures décisions pour notre avenir. C'est pourtant peut-être plus simple de visualiser des solutions lorsqu'on remet au centre du débat les 4 règnes (minéral, végétal, animal et humain) cohabitant sur la planète. Et surtout de savoir **quelle Terre nous désirons léguer à nos enfants et petits-enfants.** Les arguments techniques et économiques du « toujours plus » cèdent alors la place à des logiques qualitatives tendant vers le « mieux » et, en somme, beaucoup plus saines pour l'homme et son environnement

5-5 Quelques propositions (illusoires ?) dans le système existant

« Tout ce que vous avez à décider, c'est quoi faire du temps qui vous est imparti »
Le seigneur des anneaux, Gandalf le Magicien

Le système Internet existant est pernicieux dans le sens où il est capable de garder trace de pratiquement tout ce qui se passe sur le réseau. Et ceci dans les **2 domaines** où joue la mémoire. C'est-à-dire, **premièrement** dans (le protocole de) la **communication de données entre machines,** via les adresses IP et des fichiers s'y rapportant (les logs) qui sont créés, rendant compte de qui se connecte à quoi, d'où, à quelle heure et pendant combien de temps pour l'essentiel. Ce sont ces données que le Ministre de l'Intérieur M. Sarkozy a mis sous surveillance en faisant voter en France la conservation minimale des logs de connexion. Une communauté internationale non liberticide opterait pour un adressage dynamique (on y reviendra), ce qui permettrait à tout citoyen la garantie de ses libertés les plus fondamentales. **Le dilemme essentiel tient aujourd'hui à la résolution de la contradiction entre les exigences des libertés publiques individuelles** (protéger complètement toutes les communications privées) **et les impératifs de la sécurité collective** (traquer les messages criminels…).

A côté de ces traces de « communication de données » entre machines, il existe bien sûr les traces de **« contenu »** (pages web et mails pour un ordinateur, contenu des communications pour un téléphone portable, etc.) qui sont enregistrées, principalement, sur les ordinateurs et serveurs du réseau. Aujourd'hui, aucun état occidental (sauf l'Australie[222]) ne force à la conservation de ce type de données, mais, comme on l'a vu, le réseau a une mémoire parfaite, et par exemple, des entreprises privées comme celles qui gèrent les moteurs de recherche indexant tout l'Internet peuvent garder dans leur « cache » la mémoire de toute page web créée. Il est donc nécessaire, comme nous l'avons vu, que le législateur puisse y intervenir pour permettre à chacun un « droit à l'oubli » qui semble aujourd'hui tellement nécessaire. Si pour certaines raisons, entre autre sécuritaires, des états allaient légiférer dans le sens d'une **conservation légale** de tous les **contenus** (par exemple la conservation des conversations échangées sur tous les téléphones), et les liaient à **des « données » de communication** (adresse IP notamment), donc à des personnes physiques, alors nous serions probablement rentrés dans une logique totalitaire.

Voyons maintenant quelques solutions encore possibles :

- **Les IP variables :** Comme nous l'avions détaillé lors du 1er chapitre nous sommes actuellement sur une phase de transition entre les systèmes IPv4 et IPv6, fondements techniques de l'Internet. Pour rappel, IPv4 propose un adressage « dynamique » aux ordinateurs (principalement) qu'il gère, c'est-à-dire que l'adresse IP (suite de nombres) qu'il leur donne n'est valable que le temps de la connexion. Pour une connexion ultérieure, ce numéro changera, rendant donc très difficile toute forme de traçage. IPv6 qui prend maintenant petit à petit le relais donne une adresse IP définitive et invariable à chaque objet nomade du réseau, en augmentant de manière considérable le nombre d'adresse IP possible (plusieurs milliards de milliards). A moyen terme, beaucoup de choses dont nous ne soupçonnons même pas (voir le chapitre : « La maison de demain ») dans notre vie quotidienne vont être doté d'une adresse IP fixe (frigo, courrier, billets de banques…et peut-être nous un jour !), et prendra donc vie sur ce réseau de traces dont nous avons tant parlé. Pour résoudre ce problème qui n'était au départ que celui d'ingénieurs, et qui devient aujourd'hui profondément « éthique », il faudrait pouvoir revenir à un adressage « dynamique » comme avec IPv4 et garantir ainsi une traçabilité réduite à la durée de connexion. Ou bien si la connexion devenait permanente, alors opter pour un changement d'adresse à intervalle de temps régulier. **Les fournisseurs d'accès Internet soucieux de la vie privée de leur clientèle** pourrait intervenir auprès des pouvoirs publics pour favoriser la mise en place concrète de telles mesures.

[222] Une nouvelle loi adoptée en mars 2006 par le Sénat Australien autorise le gouvernement à lire les mails privés, les SMS ou toute autre forme de conversation électronique. Le Telecommunications Interception Act autorise les écoutes, sans consentement de la personne surveillée. Cette loi cible toute personne « B partie » ou tierce personne qui est en relation avec un individu suspecté par les forces de police ou les services de renseignement, même si cette « B partie » est totalement hors de cause et n'a rien à se reprocher. Ne sont pas seulement surveillées ses conversations avec le suspect, les forces de police auront accès à toutes ses communications privées (famille, médecin, avocat…) sous le contrôle du procureur. (source : www.latelier.fr 29/03/2006)

- **L'effacement des données personnelles :** L'homme numérique doit pouvoir compter sur la loi pour faire effacer définitivement des données sur le net qui pourraient être attentatoires à son intégrité morale, à sa liberté individuelle, à celle de sa famille, qui limiteraient ou tenteraient d'influencer ses activités privées, publiques ou professionnelles. C'est un droit de remise à zéro (RAZ) sur le réseau, et c'est en cela un garant de la démocratie dans le cyberespace. Le législateur doit intervenir, notamment aux niveaux des administrations et des entreprises pour imposer un « droit à l'oubli » (trop sujet à de vagues appréciations données par la CNIL) qui est, comme on l'a vu précédemment, tout à fait nécessaire à la garantie de nos libertés individuelles. Le problème n'est pas simple quand on sait que les données sur un individu peuvent être présentes dans plusieurs pays, réparties sur de multiples serveurs. Cependant plusieurs pays, comme la France, pourraient montrer le chemin en établissant des règles strictes à commencer sur leur territoire. Ensuite, à des organismes supra-nationaux de prendre le relais et de faire adopter ces mesures par le public et le privé.

Bien sûr, la mise en place d'IP variables et l'effacement des données personnelles sont des solutions intéressantes car dès leur mise en place elles touchent de fait toute la population sans exception. Il faudra du courage à nos dirigeants politiques, qui iront à contre courant des grandes tendances actuelles, pour mettre en œuvre de telles mesures. D'autres chantiers devraient aussi être envisagés pour éviter d'arriver à un flicage systématique. Entre autres : **l'interdiction systématique des étiquettes RFID dans les produits de consommation courante**, et également **un moratoire sur la mise en place de bornes Wifi quadrillant tout le territoire.** Et si l'interdiction des caméras de surveillance peut paraître aujourd'hui utopique, prôner au moins **un gros coup de frein à leur développement** et l'accès à **des plans rendus librement accessibles à tous par les pouvoirs publics sur leur localisation et leur champs d'action exact** (un peu comme pour les radars fixes sur les routes).

Nous allons entrapercevoir dans les lignes qui suivent quelques solutions de **sécurisation « individuelles ».** Le problème de leur utilisation est cependant bien connu, surtout si la société dérive effectivement vers des tendances sécuritaires. En effet, utiliser ces « solutions » individuelles, contrairement aux **solutions collectives, montrent déjà qu'on a peut-être quelque chose à cacher, et de ce fait, on peut attirer l'attention. La véritable clé serait qu'un gros pourcentage des « internautes » les utilise**, ce qui impliquerait que la protection individuelle devienne une norme et ne soit plus « suspecte », et ou tout du moins soit impossible à surveiller étant donné la quantité d'Internaute les utilisant.
Concrètement donc, nous allons donner quelques exemples de ces solutions, sans les détailler, et nous vous laisserons vous-même sur le réseau faire vos propres découvertes.

- La solution la plus complète actuellement, mais assez technique à mettre en place, s'appelle TOR (http://tor.eff.org/index.html.en), et est notamment soutenue par l'EFF (Electronic Frontier Fondation), qui reste aujourd'hui un gage de qualité en matière de libertés individuelles. Elle permet notamment

l'anonymat le plus complet sur Internet (Web, IRC…). En fait les communications, pour arriver d'un destinataire à un autre, passent par un réseau distribué de serveurs, appelés les routeurs « oignons », qui effacent normalement toute trace. Pour simplifier la démarche, des développeurs de hacktivissimo, un groupe de défenseurs des droits de l'homme et d'experts en sécurité informatique, ont développé un nouveau navigateur dénommé Torpak[223] qui s'éxécute à partir d'une clé USB pour ne laisser aucune trace sur les ordinateurs. Ce qui est intéressant c'est que Torpak établit une connexion crytée avec le réseau TOR. «Torpark modifie en permanence, à quelques minutes d'intervalle, l'adresse IP vue par le site web, afin d'empêcher "l'écoute" clandestine et de masquer la source de la demande», explique Hacktivismo dans un communiqué. Dans le cas, par exemple, d'un utilisateur se trouvant à Londres, les sites web verront l'adresse IP d'une université en Allemagne, ou une autre adresse appartenant au réseau TOR. Outre Torpark, les développeurs ont mis au point une application de messagerie électronique, au principe similaire, baptisée Torbird.[224]

- L'utilisation de la cryptologie, science de l'écriture secrète peut avoir son intérêt. Elle englobe la **cryptographie** qui est la technique du chiffrement des messages et la cryptanalyse qui est la recherche du texte en clair sans connaissance du chiffre. Info ou intox, on peut lire çà et là que tous les messages cryptés dans le monde (et qui attire donc l'attention) sont « aspirés » par la NSA ou d'autres agences de renseignement pour être analysés.

- Des logiciels d'anonymat peuvent être également très intéressants à utiliser. Pour beaucoup ils se basent sur la notion de proxy. Sans rentrer dans le détail technique, un serveur proxy (dit aussi serveur mandataire) est un serveur qui a pour fonction de relayer différentes requêtes et d'entretenir un cache des réponses. Ce qui est intéressant à retenir, c'est que le proxy « anonyme » peut servir à masquer sa propre adresse IP. En effet, comme il effectue des requêtes (des questions) et vous les retransmet, c'est son adresse qui est lue par le serveur envoyant l'information, et pas la votre. Ainsi, il se met « entre » votre ordinateur et le site web que vous visitez, et ce dernier ne pourra recueillir aucune information sur vous, mais récupérera uniquement les données du proxy. Pour avoir un état des logiciels de ce type disponibles, vous pouvez vous rendre par exemple sur www.internet-anonyme.com .
- Dans le même esprit, au lieu de passer par un logiciel d'anonymat, vous pouvez passer directement sur des sites web d' « anonymizer[225] » qui effectuent le même travail on-line :
    - Un exemple : http://anonymouse.org/ avec lequel vous pouvez tester le forum de discussion relatif à ce livre.

- Le site www.relakks.com, lié au très officiel « Parti Pirate Suédois » propose aux Internautes un accès anonyme au réseau pour 5 euros par mois. Et le service est un véritable succès. Le principe est simple et il remonte (presque) aux origines de l'Internet. Il s'agit d'une déclinaison des « darknets », ces

[223] Vous pouvez faire des essais et le télécharger sur http://torpark.nfshost.com
[224] www.zdnet.fr 26/09/2006
[225] Vous pouvez en trouver une liste intéressante à l'adresse : http://freeproxy.ru/en/free_proxy/cgi-proxy.htm

réseaux privés, à la réputation parfois sulfureuse, qui naissent et disparaissent dans des recoins de l'Internet en permettant à des initiés de s'échanger des données en tout anonymat. Cependant, que penser d'un tel service soi-disant anonyme où le fait de payer électroniquement pour l'utiliser revient quelque part pour l'utilisateur à s'identifier officiellement…[226]

- Concernant l'échange de fichiers, les choses ont aussi beaucoup évoluées depuis quelques années. Avec l'émergence en 1999 du premier logiciel peer to peer d'envergure dénommé Napster, puis de l'époque Kazaa et e-Donkey/e-Mule, ceux-ci se sont perfectionnés et affinés pour permettre des téléchargements aux internautes toujours plus rapides et plus sûres juridiquement après toutes les affaires et procès, menés notamment par les maisons de disques. D'après Wikipédia[227] « les actuelles lois sur le peer-to-peer et la copie privée ne font qu'accélérer une évolution technique naturelle des réseaux et clients p2p (peer to peer). Une nouvelle génération est née, dont l'année 2006 aura été la charnière : le p2p crypté et anonyme. Premièrement, les données transitant sur le réseau sont cryptées. Il est impossible de connaître le nom, le contenu et la nature de ces données. Deuxièmement, les utilisateurs sont anonymes. Ce mot n'est pas très juste, car personne ne peut être totalement anonyme quand son ordinateur est connecté à un réseau. Cependant, ce p2p nouvelle génération garantit un anonymat maximal bien que techniquement impossible à couvrir totalement. L'anonymat est d'abord garanti par la décentralisation du réseau. Il n'y a aucune connexion sur un serveur. Dans la majorité des clients peer-to-peer nouvelle génération, un système de cache et de routage des données est utilisé. Il est ainsi impossible de savoir qui possède un fichier en entier et qui l'a uploadé (=transmis) sur le réseau. Les fichiers sont divisés en fragments cryptés qui sont diffusés dans le cache de nombreux utilisateurs, dont la plupart n'ont pas demandé ce fragment. Le cache est un lieu de transit de données incontrôlable par l'utilisateur. Cela peut poser des problèmes éthiques et juridiques (comment inculper un utilisateur d'avoir uploadé un fragment de fichier sous copyright alors qu'il ne le savait même pas ?) mais garantit une sécurité maximale. Cette nouvelle génération de clients et réseaux peer-to-peer cryptés et anonymes, terre d'accueil sécurisée pour les internautes, est techniquement quasi-impossible à filtrer et à contrôler. Le plus connu de cette génération de peer-to-peer est certainement Share, dont beaucoup voient en lui le futur du partage de fichiers. Le plus attendu de cette génération est Kameleon, idée de client p2p idéal qui naquit sur le forum du célèbre site Ratiatum. Voici quelques exemples de p2p cryptés et anonymes : Share, Mute, Ants, GNUnet, Kameleon ».

- Abordons également le cas des moteurs de recherche qui sont nos portes d'entrées, nos sésames vers l'univers de la « toile ». C'est un fait désormais dans l'actualité Internet : des données que l'on croyait personnelles se voient de plus en plus souvent rendues publiques. La publication par erreur de données d'AOL a suscité de nouvelles craintes face à l'usage de la masse d'informations que garde un moteur sur ses visiteurs. Début août 2006 en effet, Aol se confondait en excuses pour avoir « malencontreusement » fait

[226] www.01net.com 17/08/2006
[227] Wikipédia sur la référence « Poste à poste »

circuler sur le net quelque 20 millions de données[228] concernant les requêtes d'internautes sur son moteur de recherche[229]. Face à l'émotion et l'inquiétude suscitées, **le métamoteur de recherche Ixquick**[230] a décidé de miser sur la protection de la vie privée pour rassurer ses utilisateurs. Son porte parole M. Alex Van Eesteren avoue que « beaucoup de moteurs de recherche utilisent ces données (personnelles) à des fins commerciales. **Qu'on en face un usage abusif n'est qu'une question de temps** ». Le rôle d'Ixquick consiste à agréger les réponses générées par 12 des principaux moteurs de recherche (Yahoo, Msn…) sur une même requête et à les présenter à ses visiteurs. Or la société, basée aux Pays Bas, a décidé d'effacer de ses fichiers les fameuses adresses IP des utilisateurs ainsi que tout paramètre unique d'identification ! **Une initiative qui mérite d'être soulignée et utilisée sans ménagement.** A la base, le moteur enregistre comme ses concurrents ces informations, notamment à des fins de statistiques et de sécurité, explique Robert Beens, le directeur exécutif d'Ixquick. « Mais toute donnée permettant l'identification est effacée par un logiciel spécifique qui repère les adresses IP dans les fichiers de logs, et les détruit automatiquement. Par ailleurs, le moteur promet de n'utiliser aucun cookie permanent avec numéro d'identification. » « Contrairement à la plupart de nos concurrents, nous sommes une société indépendante, incapable de croiser les données de nos utilisateurs avec les autres services que nous proposons », assure le directeur. En tant que société européenne, ajoute-t-il, Ixquick doit respecter une législation beaucoup plus stricte au regard de la protection de la vie privée de ses utilisateurs. Ce qui permet au moteur de recherche de se placer en alternative face à ses concurrents Msn ou Yahoo, tout en utilisant leurs propres résultats de requêtes[231]. En conclusion, M. Van Eesteren affirme que « de la sorte, tout internaute pourra utiliser Ixquick en accédant à la série des meilleurs moteurs de recherche sans exposer aucunement sa vie privée. »

- Par ailleurs, des solutions commerciales d'anonymat, comme avec les produits de la société allemande Steganos, voient également le jour. Dernièrement, cette entreprise à lancé « Internet Anonym VPN » sur le marché. De cette manière, l'internaute reste invisible aux yeux des sites visités qui ne "voient" que l'adresse IP (le numéro d'identifiant de la machine connectée à Internet) des serveurs de Steganos, et non celle de son ordinateur propre. Même son fournisseur d'accès, n'est pas en mesure de "surveiller" le trafic de son abonné puisque les données échangées y sont cryptées. Mais bien évidemment, les autorités et la loi ont le dernier mot et font bien souvent de l'anonymat un secret de polichinelle. Lancé en Allemagne (où sont installés le siège et les serveurs de la société), Internet Anonym VPN a été exploité très vite par des spammeurs. Alerté, Steganos a évidemment bloqué l'accès aux profiteurs et cassé leur contrat de licence. La société déclare par ailleurs volontairement collaborer avec les autorités

[228] Pour avoir une idée de ce qui est en jeu, et comprendre pourquoi les moteurs de recherche en savent beaucoup sur nous, vous pouvez aller sur www.aolsearchdatabase.com. En rentrant par exemple l'ID (numéro d'identifiant d'un client Aol) n° 14162375 (ou un autre) vous pouvez vous rendre compte plus concrètement de l'intrusion possible dans nos intimités.
[229] www.zdnet.fr 08/08/2006
[230] Pour la France, à l'adresse : http://eu.ixquick.com/fra/
[231] www.zdnet.fr 9/06/2006

judiciaires et policières allemandes dans le cadre d'enquêtes et, au besoin, déverrouiller le chiffrement des données. En France, le service d'anonymat de Steganos est par ailleurs soumis à la loi sur la Confiance dans l'économie numérique qui oblige également de conserver les données de connexion (un an, rappelons-le, pour la rétention des logs). "Dans la mesure où le service est commercialisé en France, il est soumis aux lois françaises", rappelle David Melison, juriste pour le Forum des droits sur l'Internet,"si le prestataire ne se plie pas à ces règles, il engage sa responsabilité." Pourtant, dans sa communication à la presse, Steganos déclare n'enregistrer aucun des sites visités, ni aucune autre donnée à l'exception du volume des octets transférés. Et sur son site, on peut lire que "la question n'est pas de savoir si vous avez ou non quelque chose à cacher. Vous avez droit à une vie privée et ne devez en aucun cas vous justifier." Info ou intox ? Pour David Melison, "ce n'est pas parce qu'on utilise le service de Steganos qu'on peut faire n'importe quoi"[232].

- Les requêtes effectuées sur le Web par un internaute, via les moteurs de recherche, on l'a vu, laissant forcément des indications permettant de se faire une idée assez précise de ses centres d'intérêt, la société Unspam Technologies propose un outil gratuit, intitulé « Lost in the crowd »[233] pour brouiller les pistes. Il s'agit d'installer, en quelques clics, un favori dans son navigateur pour tel ou tel moteur de recherche. Le favori envoie alors régulièrement vers ledit moteur une requête aléatoire. On peut supposer qu'ensuite, pour Google ou d'autres qui guettent les habitudes des internautes, il devienne difficile de récolter des données vraiment cohérentes.[234]

Bien sûr, si vous avez à rechercher ou à publier des informations sur le web en gardant votre anonymat, le travail depuis un cybercafé, tant que l'identifiant biométrique n'est pas en place sur le réseau, reste une solution intéressante.

D'autres solutions, comme Torbird que nous avons évoqué précédemment en parlant du réseau Tor, sont disponibles pour les e-mails. Autre exemple, une start-up américaine vient de proposer sur le marché des entreprises et des particuliers un système de messagerie électronique qui ne laisse pas de traces. Ce système, dénommé VaporStream est assez simple à comprendre : Alice veut par exemple discuter d'une affaire privée avec Bob. Elle ouvre une page Web VaporStream cryptée et sélectionne ensuite Bob sur une liste de correspondants. Une fenêtre s'ouvre, où elle peut taper un message. Son nom et celui de Bob n'apparaissent nulle part à ce stade et les messages individuels ne peuvent être copiés ou collés dans d'autres programmes. Après son envoi, le message n'est plus visible sur l'ordinateur de l'expéditrice. Il est transmis à un serveur géré par VaporStream, où il est conservé temporairement en mémoire. Lorsque Bob ouvre sa page Web VaporStream, il peut voir qu'il a un message d'Alice et n'a qu'à cliquer pour le lire. Une fois transmis au destinataire, le message quitte définitivement le serveur de

[232] www.vnunet.fr 05/07/206
[233] www.lostinthecrowd.com
[234] www.01net.com 28/08/2006

VaporStream. Lorsque Bob répond, le message original d'Alice disparaît de son ordinateur. Les deux parties poursuivent le dialogue selon le même principe que dans une conversation où chacun doit se souvenir des derniers messages pour ne pas perdre le fil. «L'expéditeur et le destinataire n'ont pas de copie» des messages, souligne Amit Shah, co-fondateur du système avec Joseph Collins[235].

Déjà des choses sont en train d'apparaître pour la téléphonie, et nul doute qu'un véritable marché de l'anonymat est en train d'émerger. Encore une fois, et nous le répétons, il ne pourra y avoir de véritable « anonymat » par ces méthodes individuelles seulement si une majorité d'Internautes utilise ces logiciels et techniques. En effet, si seulement une très petite communauté en fait usage, elle sera de fait mise plus facilement en relief.

Mais ne nous leurrons pas : les terroristes auront toujours les moyens de détourner le système, et **croire que la matérialisation d'un Internet ultra sécurisé pourra lutter contre ce fléau n'est purement et simplement qu'un mensonge.**
Mais la véritable question n'est elle pas plutôt celle ci : **est-ce vraiment d'une telle société que nous voulons ériger** pour nous et léguer à nos enfants, **où l'anonymat soit devenu un marché** et **où il faille se dissimuler derrière des astuces techniques pour se croire un semblant libre ?**
Toutes les solutions, valables un temps, distillées dans ce chapitre ne sont-elles pas en fait qu'une **illusion destinée** à des James Bond en herbe **à remettre toujours au lendemain la création d'un nouveau paradigme** où la vie de l'être humain, conscient de ses responsabilités, pourrait, enfin, réellement prendre tout son sens ? Et où, qui sait, l'amour universel saura se manifester, loin des jugements inhérents à la « matière dense » du réseau.

5-6 L'amour de soi, l'amour des autres

« Je ne connais qu'un seul devoir, c'est celui d'aimer »
Albert Camus

Apparu entre le IIe et IIIe siècle après J.-C., le courant Gnostique professe que la gnose (la connaissance) apporte le salut. Hérétique aux yeux de l'Eglise, la gnosticisme à de nos jours de nombreux adeptes.
Or, on peut en effet considérer aujourd'hui qu'Internet, n'est rien d'autre qu'une matérialisation de la connaissance, une matérialisation de la gnose à l'échelle planétaire. Et l'on peut aller même plus loin avec l'apparition du Wi-fi et des technologies sans fil de l'Internet à grande vitesse : ainsi, **la connaissance est en train de circuler par les « airs », « librement », presque jusque dans le moindre atome composant nos espaces de vie**. Mais après notre exposé, peut-on encore dire qu'Internet dans un futur hypothétique sera toujours aussi libre qu'aujourd'hui, si

[235] www.canoe.com du 26/09/2006

nous n'agissons pas, par la voie qu'aimeraient lui faire prendre certains de nos gouvernants ?
Ainsi la connaissance va se déplacer, probablement à des débits vertigineux (>20Mgbits/s), dans tous les espaces où nous nous situerons. Elle viendra « librement » à nous, presque sans effort, puisqu'il suffira d'un émetteur/récepteur (type téléphone portable Wap) pour pouvoir la capter. Le rêve des gnostiques est en train de se matérialiser. Mais avaient-ils vu juste à l'époque ?

Les derniers prophètes apparus sur la planète avaient un discours, **ne niant cependant pas l'importance de la connaissance**, axé sur **l'amour de soi et l'amour de son prochain.** En effet, tout le monde n'est pas capable d'accéder à la connaissance. Il faut disposer de prédispositions intellectuelles inégalement réparties, et avoir un âge mur pour avoir pu en acquérir suffisamment. Or le « Royaume » annoncé par certains prophètes n'est-il pas accessible « au plus petit » d'entre nous, aux plus humbles et aux enfants ?

Il y a 70.000 ans *l'homo erectus* dut affronter la dernière glaciation. Seuls ceux qui avaient développé un gros cortex cérébral purent s'adapter et survivre. **La connaissance fut le vecteur d'adaptation**, pour ceux qu'on nommera plus tard **« homo sapiens ».** Ils purent effectivement par ce biais là **s'adapter à leur nouvel environnement par des technologies** qu'ils mirent au point (en particulier la fabrication de vêtements) et finalement survivre en perpétuant l'espèce humaine.
Aujourd'hui, et Internet en est la métaphore, **la Connaissance est en passe de remplir le moindre espace physique dans lequel nous nous situons**. Elle devient littéralement omniprésente. Nous sommes, à vrai dire, comme « baignés dedans ». C'est la supériorité en apparence d'homo sapiens qui est arrivé au bout de sa logique : **survivre à tout prix grâce à la connaissance et à son allié, la technologie**. Mais cet homme de « raison » détient-il le monopole de la vérité comme il voudrait nous le faire croire ? Est-ce que toutes ces connaissances accumulées vont servir à l'homme pour se sortir du scénario actuel que beaucoup vivent comme un drame ?
Le successeur d'homo sapiens est peut-être déjà là : il s'agirait d'**homo passiens** et on peut supposer qu'il survivra aux nouvelles conditions de vie socio-ecologique sur la planète. Pour passer ce nouveau cap, **le vecteur adaptatif sera peut être l'amour** universel et inconditionnel (c'est-à-dire que je ne me pose pas de « conditions » pour t'aimer, trop comme ci ou pas assez comme ça : je t'aime tel que tu es. Mais c'est probablement aussi bien d'autres choses : à vous d'expérimenter !). En effet, aimer réellement, c'est se donner le droit d'être, et de donner aux autres le droit d'être et d'en retirer diverses expériences. En donnant le droit à tout ce qui est vivant de vivre des expériences, on accepte le fait que tout ce qui vit est ici sur terre dans le seul but de grandir en sagesse à travers ces expériences. Pour le dire encore autrement, on peut dire qu'aimer c'est respecter son propre espace et celui de l'autre, c'est-à-dire se donner le droit d'avoir des besoins, des désirs, des limites ou des peurs. C'est reconnaître que l'action qu'on a posée, on l'a posée au meilleur de ses ressources du moment : comme tout être en évolution, on apprend aussi par ses erreurs. Parvenir à ne plus juger ni condamner fait partie de notre raison d'être ici : si l'on prend par exemple une personne que vous critiquez sous tel ou tel point de vue, êtes-vous sur que si vous étiez né dans les mêmes conditions spatio-temporelles, dans la même famille, avec le même physique, avec la même éducation… vous seriez vraiment différent d'elle ?

En tout cas, **l'homo Passiens sera probablement complice de la nature**, en harmonie avec elle, en choisissant (sélection) d'aimer seulement ceux qui s'abandonneront à son amour, c'est-à-dire ceux qui seront capables d'être aimés. Ceux-ci auront préalablement appris à s'aimer eux-mêmes et à aimer les autres. L'homo passiens est un homme de partage, d'échange, de réciprocité et toutes ses capacités feront qu'il pourra s'adapter aux nouvelles conditions de vie sur terre. Peut être que la **raison** ne dictera plus sa loi sur terre. Certes elle ne disparaîtra pas mais **sera subordonnée à l'amour**. L'amour sera tout simplement le trait culturel dominant de demain pour l'ensemble de l'humanité.
Depuis des millénaires **nos civilisations se sont bâties sur le mode de la « pensée ».** Certaines Traditions l'ont d'ailleurs relevé quand elles rapportent : « Et le Verbe s'est fait Chair ». Mais n'arrivons-nous pas au bout de cette logique de **la toute puissance de la pensée comme fondement de nos sociétés**, tant les déséquilibres au niveau planétaire paraissent aujourd'hui sans communes mesures ? Internet n'est-il pas l'apogée de ce mode de fonctionnement ? En effet, n'importe quelle pensée émise sur le réseau (sur un moteur de recherche par exemple) se donne chair à la vitesse de l'éclair dans la matière (technologique)[236] la plus dense. Dés que l'on pense à quelque chose, on peut obtenir des réponses quasi instantanément. Comme si la seule manière de voir les choses dans notre monde relevait forcément de l'ordre du mental et de la matière.
Pourtant **c'est peut être l'arbre qui cache la forêt**. En effet, et si maintenant les hommes décidaient que l'amour dans ses multiples déclinaisons pouvait lui aussi se faire chair ? Et si le cerveau de l'amour était véritablement dans le cœur, et celui de la peur et de la survie dans la tête ? Et si un nouveau départ sur des bases saines et équilibrées était désormais possible ?

Connu pour sa théorie de la relativité – alors qu'il n'avait que 26 ans – Albert Enstein est sans doute l'un des plus grand scientifique de tous les temps. A la fin de sa vie, on raconte qu'il a décroché de ses murs les portraits de Maxwell et Newton, deux de ses illustres pairs. Lorsque ses collègues s'en sont aperçus et ont voulu connaître ses motivations, il a simplement répondu : « Il est temps d'enlever les symboles de la science et de les remplacer par ceux du service. » Apparemment, Enstein avait fini par comprendre que **le pouvoir de l'amour dépasse celui de la science.** Il avait d'ailleurs touché très précocement cette idée alors qu'il n'était qu'étudiant :
« Un professeur universitaire défia ses étudiants avec cette question :
Est-ce que Dieu a créé tout ce qui existe ?
Un étudiant répondit bravement, "oui, Il l'a fait !"
Le professeur dit, "Dieu a tout créé ?"
"Oui, monsieur", répliqua l'étudiant.
Le professeur répondit, "si Dieu a tout créé, Il a donc aussi créé le mal puisque le mal existe et selon le principe de nos travaux qui définissent ce que nous sommes, alors Dieu est mauvais."
L'étudiant fut silencieux devant une telle réponse.
Le professeur était tout à fait heureux de lui-même et il se vantait aux étudiants qu'il avait prouvé encore une fois que la foi chrétienne était un mythe.
Un autre étudiant leva sa main et dit, "Puis-je vous poser une question professeur ?"
"Bien sûr", répondit le professeur.
L'étudiant répliqua, "Professeur, le froid existe-t-il ?"
"Quel genre de question est-ce, cela ? Bien sûr qu'il existe. Vous n'avez jamais eu

[236] Cf paragraphe sur « Le droit à l'oubli »

froid ?" dit le professeur.
Le jeune homme dit, "En fait monsieur, le froid n'existe pas. Selon la loi de physique, ce que nous considérons le froid, est en réalité l'absence de chaleur. Tout individu ou tout objet possède ou transmet de l'énergie. La chaleur est produite par un corps ou par une matière qui transmet de l'énergie. Le zéro Absolu (-460°F) est l'absence totale de chaleur ; toute la matière devient inerte et incapable de réagir à cette température. Le froid n'existe pas. Nous avons créé ce mot pour décrire ce que nous ressentons si nous n'avons aucune chaleur."
L'étudiant continua. "Professeur, l'obscurité existe-t-elle ?"
Le professeur répondit, "Bien sûr qu'elle existe !"
L'étudiant : "Vous avez encore tort Monsieur, l'obscurité n'existe pas non plus.
L'obscurité est en réalité l'absence de lumière. Nous pouvons étudier la lumière, mais pas l'obscurité. En fait, nous pouvons utiliser le prisme de Newton pour fragmenter la lumière blanche en plusieurs couleurs et étudier les diverses longueurs d'onde de chaque couleur. Vous ne pouvez pas mesurer l'obscurité. Un simple rayon de lumière peut faire irruption dans un monde d'obscurité et l'illuminer. Comment pouvez-vous savoir l'espace qu'occupe l'obscurité ? Vous mesurez la quantité de lumière présente. N'est-ce pas vrai ? L'obscurité est un terme utilisé par l'homme pour décrire ce qui arrive quand il n'y a pas de lumière."
Finalement, le jeune homme demanda au professeur, "Monsieur, le mal existe-t-il ?"
Maintenant incertain, le professeur répondit, "Bien sûr comme je l'ai déjà dit. Nous le voyons chaque jour. C'est dans les exemples quotidiens de l'inhumanité de l'homme envers l'homme. C'est dans la multitude des crimes et des violences partout dans le monde. Ces manifestations ne sont rien d'autre que du mal !"
L'étudiant répondit, "Le Mal n'existe pas Monsieur, ou au moins il n'existe pas de lui-même. Le Mal est simplement l'absence de Dieu. Il est comme l'obscurité et le froid, un mot que l'homme a créé pour décrire l'absence de Dieu. Dieu n'a pas créé le mal. Le Mal n'est pas comme la foi, ou l'amour qui existe tout comme la lumière et la chaleur. Le Mal est le résultat de ce qui arrive quand l'homme n'a pas l'amour de Dieu dans son coeur. Il est comme le froid qui vient quand il n'y a aucune chaleur ou l'obscurité qui vient quand il n'y a aucune lumière."
Le professeur s'assis abasourdit d'une telle réponse.

Le nom du jeune étudiant ? Albert Einstein »

Comme notre époque est aussi celle de la grande parodie, on peut tout à fait imaginer l'arrivée de nouveaux gourous sur le « marché de l'amour » qui prophétisent pourquoi, comment, quand et qui aimer. Or il faut bien voir que, malgré les croyances, l'amour universel et inconditionnel est une chose assez nouvelle à expérimenter pour les hommes, loin des jalousies, attachements ou autres déclinaisons. Ce n'est pas non plus un amour « béat » qui **bannirait tout discernement** et conduirait à suivre n'importe qui. **Seule l'expérience individuelle, dans la diversité et loin de tout sectarisme** est de mise pour approcher cette fabuleuse opportunité d'évolution, et peut être enfin, de bonheur.

5-7 Un nouveau paradigme[237]

La façon la plus efficace de combattre un système qui ne nous convient plus n'est pas de lutter contre lui, mais de s'en désintéresser et de ne plus l'alimenter.

www.onpeutlefaire.com

Adolescent, j'étais[238] passionné, comme la plupart de mes camarades, de jeux vidéo. Je rêvais secrètement d'un jeu qui permette à mon personnage de se déplacer là où il veut, de conduire une voiture ou piloter un avion s'il le désire ou même de discuter avec d'autres acteurs. A cette époque pas si éloignée où Internet n'existait pas encore et où le graphisme était encore assez éloigné de notre réalité quotidienne, ce rêve n'était alors que pure spéculation.
Pourtant devenu adulte, un jour un petit cousin m'a fait découvrir son nouveau jeu vidéo. Il s'agissait, pour les experts, de GTA (Grand Theft Auto) sur Playstation. Et là j'ai réalisé que le rêve était devenu réalité[239] : on pouvait tout faire ou presque dans ce jeu. La liberté de mouvement et d'action des personnages, dans des villes recrées sur mesure, était presque sans limite (on pourrait tout aussi bien parler aujourd'hui du site Internet de réalité virtuelle « Second life » qui compte déjà plusieurs millions d'adeptes.)
Encore un peu plus tard, j'assistai alors à un enterrement lorsqu'un proche du défunt lut un texte de Mère Teresa, où notamment elle disait : « la vie est un jeu, joue-le ». Et c'est à ce moment là que qu'une intuition folle m'est venue. **Et si le plus grand terrain de jeu et d'expérience au monde n'était pas le monde lui-même !** Et bien plus prenant et enthousiasmant que la plupart de nos créations virtuelles. Avec toutes la palette et les nuances des plans physiques, émotionnels, mentaux et spirituels à la fois ce qui ne fait pas seulement des millions de possibilités, mais véritablement une infinité. Les bouddhistes ont leur vocabulaire pour définir cette réalité du monde : ils parlent alors d'**impermanence**. Chaque seconde est unique : on ne pourra jamais reproduire un moment vécu une seconde fois dans toute sa singularité. C'est tout le merveilleux de la vie. Marcher, respirer, profiter de nos cinq sens pour **apprécier notre environnement naturel à sa juste valeur**, voilà **des choses très simples** qui mériteraient notre attention. La Création est tellement belle et puissante qu'elle ne nous laisse jamais dans la routine et se recrée en permanence, pour qui veut bien l'écouter, l'accueillir, l'admirer, et agir dans son cadre infini. Déjà, beaucoup de jeunes occidentaux, élevés dans un environnement quasi uniquement technologique n'ont bien souvent jamais « mis les mains dans la terre » (pour s'amuser, pour jardiner, etc.) et la trouve « sale », contrairement à la « pureté » de leur « nouvel environnement » mis aujourd'hui à leur disposition. C'est assez consternant de voir ainsi notre planète, une fois de plus, mise à l'écart.
Il faut donc voir la virtualité seulement comme un aspect de la réalité du monde, mais ne pas inverser les choses et la prendre comme la réalité ultime. On pourrait y être

[237] Un paradigme est une représentation du monde, une manière de voir les choses, un modèle cohérent de vision du monde qui repose sur une base définie. (Source : Wikipédia)
[238] Tiré d'une expérience d'un des auteurs
[239] On trouve aujourd'hui aussi directement sur le web des jeux en réalité virtuelle très poussé comme « Second life »qui attire des centaines de milliers de joueurs.

tenté aujourd'hui. On le sera encore plus demain si le réseau devenait tout puissant et s'imposait à tous. La vie est plus que ça, mais surtout la vie est mieux que ça. Là est peut-être **l'ultime vanité de l'homme, croire qu'il peut s'affranchir de la Création pour vivre dans sa propre création**. Délire autistique et prétention ultime ?

Nous avons essayé d'esquisser dans ce livre des trajectoires possibles pour la planète et son humanité, certes en forçant un peu le trait, mais cela était nécessaire à la prise de conscience de ce à quoi pourrait contribuer, si nous y consentons, nos « joujous » technologiques, c'est-à-dire peut être à nous asservir durablement. Si ces probabilités se mettaient en place, beaucoup d'entre-nous pourraient se sentir profondément attirés par **l'idée d'un nouveau paradigme**[240], plus juste, plus vrai, plus beau, car nous aurions compris quel scénario catastrophe se cacherait derrière les apparences. **Il ne sert à rien de ressasser à l'infini les scénarios sombres** tels que décrits ici ou ailleurs : on finirait par y perdre toute son énergie sans que cela nous fasse faire un pas en avant. Certes il faut en avoir été conscient à un moment de sa vie, mais ensuite réussir à les dépasser pour véritablement **se focaliser sur les solutions d'un nouveau paradigme d'expériences**. Des groupes de « rêveurs » à propos de ce nouveau paradigme pourraient alors se mettre en place et « enclencher » une dynamique de création véritablement nouvelle.
Bâtir une nouvelle théorie, un nouveau paradigme à dit un jour Einstein, n'est pas ériger un gratte ciel à la place d'une vieille baraque, « c'est plutôt comme de gravir une montagne et d'avoir peu à peu une vue différente, plus vaste, de découvrir des relations inattendues entre notre point de départ et son riche environnement. Car le point d'où nous sommes partis existe toujours et reste visible, bien qu'il paraisse plus petit et ne soit plus qu'une faible partie de notre vision élargie… »

5-8 Le choix

« Les deux maux du monde sont l'ordre et le désordre. La pourriture me dégoûte, et la vertu me donne le frisson ».

Mort d'un pourri[241]

Ce livre aurait pu être l'antithèse d'un sujet de philo « Etes vous pour ou contre l'usage des nouvelles technologies aujourd'hui ?» Nous sommes conscients de n'avoir écrit la vision que d'un seul côté du miroir. C'était, nous le croyions, indispensable à une époque où l'on ne se pose pratiquement plus le choix de l'usage de la technologie. La thèse est en fait écrite tous les jours à grand renfort de médias et de publicités interposés, et nous laisse supposer qu'il n'y a plus de choix. C'est évidemment faux.

[240] Pour plus de détails, vous pouvez vous procurer gratuitement « Le manuel pour un nouveau paradigme » sur Internet. Par exemple en allant sur le site http://www.onnouscachetout.com/articles .Il se trouve tout en bas de la page web.
[241] Film de Georges Lautner, 1977, avec Alain Delon et Ornella Muti

Maintenant que vous disposez des deux points de vue, vous pouvez vous **construire votre propre synthèse**. Et arrêter enfin d'opposer forcément l'un à l'autre dans **une logique de conflit perpétuel ou nous pousse irrémédiablement nos sociétés**. Mais plutôt de trouver votre propre solution dans une alchimie intérieure qui ne peut déboucher que sur la paix individuelle et collective, dans le respect, la **confiance** mutuelle et le non jugement de chacun. L'attachement à la « matière » dense dans **notre monde, totalement déséquilibré de ce fait**, par certains de nos contemporains (que certains appelleraient les forces de l'ombre) souvent aveuglés malgré eux, conduit déjà, par retour de balancier, à l'extrême inverse avec l'émergence des forces de l'esprit (ou forces de la Lumière). Faudra t'il donc **choisir exclusivement** entre l'une ou l'autre ? L'homme et la Création ne sont-ils pas de subtils mélanges des deux, à la fois matière ET esprit. Contrairement à beaucoup d'entre-nous qui inversent encore les choses à notre époque, il est important de savoir que c'est bien effectivement la matière qui découle de « l'esprit » : il n'y a donc pas à rejeter l'une pour l'autre mais simplement savoir qu'il existe une hiérarchie dans la manifestation, l'une et l'autre étant seulement des réalités « vibrant » à des niveaux très différents.
Il est vrai que les nouvelles technologies aboutissent à une densification de la matière peut-être jamais obtenue jusqu'alors. Les forces de la matière conduisent peut être notre monde progressivement dans l'impasse et il faut en être conscient, comme à pu partiellement tenter de le montrer cet ouvrage. Mais doit-on du coup basculer à 100% dans le camp opposé ? Encore ne faudrait-il pas assimiler la matière « naturelle » issue de notre environnement qui nous a fait naître et grandir, et celle, plus perverse, provenant de la matérialisation de nos connaissances, dans la technologie. La nature peut nous accueillir à nouveau si nous le désirons, quand bien même si nous nous en étions coupé jusqu'alors.
En réalité nous ne sommes pas encore des désincarnés, de pures esprits. Nos corps et notre monde sont aussi faits en partie de matière. Remettre enfin la prééminence de la spiritualité sur la matière ne fait pas de doute, mais éluder totalement l'une au profit de l'autre reste aussi périlleux que de raisonner en pur matérialiste. Il serait bon, pour l'être humain, placé entre terre et ciel, entre enracinement et ouverture, de retrouver là son **véritable équilibre** en restant toujours tolérant envers « l'autre » qui a le droit légitime à la différence.
Etre avant tout « lumineux », tendance qu'annonce le courant actuel du « bien être », d'accord sans doute car c'est un cap qui permet de nous transcender et qui nous relie à la source même de toute chose. Mais savoir aussi ne pas nier et **refouler constamment notre part d'ombre**[242], inhérente à chacun dans notre condition humaine. Et avant tout si possible, faire la paix avec soi même et avec chacun, en **se désintéressant de toute forme de conflit, de peur ou de vengeance**.
Ne serait-ce pas en effet dans les plans de l'ombre justement **d'amener sournoisement la lumière**, **quitte à se faire passer pour elle, à rentrer dans son jeu de conflits et de luttes acharnées sans fin** pour **dresser les 2 forces l'une contre l'autre, et finalement tout le monde contre son prochain ?** Or, est-ce véritablement dans la nature de la Lumière que de se « battre » ? Ne fait elle pas simplement qu'éclairer le chemin, dans la paix ?
Beaucoup de Traditions l'énoncent d'ailleurs clairement : **seul la paix intérieure amène la paix extérieure.** Les « ennemis » qui se présentent devant nous ne sont en fait que le reflet de conflits internes présents en nous même que nous n'avons

[242] « La lumière sans ombre n'appartient qu'aux anges », citation de Ernst Jünger (1895-1998)

pas encore réglés : la vie essaie simplement de nous en faire prendre conscience. Or nous sommes persuadés que la seule solution est, à tout prix, de « **lutter contre** »[243] ses adversaires pour s'en débarrasser, ce qui ne résout rien, car la même situation se représentera pour nous plus tard. D'où aussi l'intérêt, mais nous ne rentrerons pas dans le sujet, de travailler sur soi, pour permettre l'émergence d'un nouvel équilibre interne où les luttes passées feront place à des prises de conscience plus paisibles et enrichissantes pour évoluer.

Internet n'est qu'un outil recelant en lui une multitude de possibles, dans toute la palette qui va de l'ouverture aux autres la plus totale jusqu'au contrôle des masses le plus intime. Nous sommes libre de ne pas espionner notre propre voisin, de ne pas confier entièrement notre vie au réseau, de ne pas déléguer à d'autres notre propre sécurité, de ne pas foncer dans un délire technologique et le contrôle par les machines… ou de le faire si vous en êtes convaincus. Ou bien encore, peut-être par une certaine intelligence du cœur, de trouver une 3ème voie propre à vous-même. Si 2 prophètes se lèvent avec des idées contradictoires, vous avez bien sur la possibilité de suivre soit l'un soit l'autre. C'est la première attitude, celle de forcément adhérer à un camp ou à son opposé. Mais thèse et antithèse seront toujours éternellement en affrontement. Vous avez aussi le choix de ne suivre ni l'un ni l'autre en poursuivant dans votre propre voie. **Le conflit n'est pas exigé. Etre un artisan de paix est possible. La guerre de l'ombre contre la lumière n'est pas une obligation.** On peut se situer en dehors. Bien sur cela ne signifie pas être passif, bien au contraire.
Ne serait-il pas temps pour l'humanité, enfin, de déposer épées et boucliers ? Malheureusement nos sociétés nous conditionnent à rentrer le plus naturellement du monde dans ces cadres de luttes acharnées et de compétition, via les grands médias, le cinéma, le sport, l'éducation…

On a toujours le choix, même dans les pires moments. C'est ce que découvrit Assagioli, le fondateur de la psychosynthèse, lorsqu'il fut emprisonné en 1938 par les fascistes à cause de ses idées pacifistes : « Je réalisais que j'étais libre d'adopter une attitude parmi plusieurs vis à vis de la situation, de lui accorder une valeur ou une autre, de m'en servir d'une façon ou d'une autre. Je pouvais me révolter intérieurement et maudire la situation ou je pouvais m'y soumettre passivement, végétativement, ou je pouvais m'attarder au plaisir morbide de l'apitoiement et prendre le rôle de martyr, ou je pouvais prendre la situation sportivement et avec sens de l'humour, la considérant comme une expérience nouvelle et intéressante… Je pouvais en faire une cure de repos ou une période de pensée intense, que ce soit sur des questions personnelles – revoir et évaluer ma vie passée – ou sur des problèmes scientifiques et philosophiques ; ou je pouvais tirer profit de la situation pour entreprendre un entraînement psychologique personnel, ou enfin, je pouvais en faire une retraite spirituelle. J'ai eu la perception pure et claire que c'était entièrement ma propre affaire, que j'étais libre de choisir l'une ou plusieurs de ces attitudes et activités, que ce choix aurait des effets inévitables que je pouvais prévoir et dont j'étais pleinement responsable. Il n'y avait aucun doute dans mon esprit quant à ce pouvoir et cette liberté essentiels et à leurs privilèges et responsabilités inhérents. »

[243] www.le-corps-memoire.fr/corps_memoire.htm#textes et cliquer en bas de page sur « Le corps mémoire second volet : Cesser la guerre »

Dans les temps qui arrivent, il se pourrait que chaque être humain à condition qu'il ait su développer sa propre autonomie et son discernement, en pleine conscience, ait à faire certains choix pour **continuer sa route dans la paix et la simplicité**. Et pourquoi pas **loin des planifications faites à sa place**, mais dans le respect de son être le plus profond. La voie de chacun est unique et respectable. Et la page de demain est, quoi qu'on en dise, une page blanche…

Ne suivez pas les routes toutes tracées.
Au contraire, allez là où il n'y a pas de route,
Et commencez à creuser le chemin.
Anonyme