Le 5 avril 2015

UTB Chalon sur Saône
Groupe "Ethique et Société"

Préparation d'un débat relatif à "**Vie Publique, Vie Privée**"

En s'appuyant sur un livre écrit par Jean-Marc MANACH intitulé
"Vie privée, un problème de vieux cons ?"
Editions FYP - 2010.

1) En préambule, quelques renseignements sur l'auteur

Jean-Marc MANACH est né en 1971 (44 ans).

Il s'intéresse depuis plusieurs années à l'impact direct des technologies informatiques sur la vie des hommes en société.

A travers la mise en œuvre de systèmes de surveillance, il appréhende leurs effets sur la liberté et sur la vie privée des hommes d'aujourd'hui.

Il est aussi expert des risques induits par la relative difficulté de sécuriser l'usage de tous nos outils informatiques sédentaires et nomades.

Il développe des outils de journalisme sur internet et fait bénéficier de ses démarches et réflexions les auditeurs de ses conférences qu'il donne dans le cadre des écoles de journalisme (ESJ et CFJ) et à Sciences Politiques.

Il semble être militant engagé.

2) La forme littéraire de l'ouvrage

L'auteur est journaliste et met en œuvre un écrit de style journalistique, utilisant volontiers les exemples trouvés dans le vécu. Il fait aussi de nombreuses fois appel à des travaux de chercheurs de tous horizons, sans vraiment construire son argumentation.

Ce livre n'est pas bâti comme une thèse universitaire, c'est un bon catalogue dans lequel il faut ordonner les différents chapitres pour le rendre pédagogique. Certains passages, très techniques (informatique, juridique et d'histoire politique) nous conduisent cependant à nous prendre au jeu et nous amène à nous questionner.

3) Le plan de l'ouvrage

L'auteur expose son sujet en égrenant neuf chapitres. Les deux premiers chapitres sont consacrés à la perception des jeunes de moins de trente ans et des plus de trente ans, de ce qu'ils entendent par vie privée à l'ère de la grande communication internet. Ensuite, un paquet de quatre chapitres vient nous expliquer comment nous sommes arrivés, en France, à accepter majoritairement d'être mis sous surveillance, fichés très facilement par le Ministère de l'Intérieur, contrôlés par de nombreux moyens afin de donner un relatif sentiment de sécurité à une grande partie de la population. Et tout ceci sans vraiment de résistance.

Puis un dernier paquet de trois chapitres nous ramène les pieds sur terre, en nous montrant que la surveillance et le contrôle sont plus des moyens de répression que des moyens d'exercice de l'entière liberté du citoyen, que les efforts déployés pour, soi-disant, nous sécuriser la vie sont vains. Il nous montre que les moyens étatiques mis en œuvre sont seulement efficaces pour les entreprises sensibles, les start-up et les laboratoires ; et que les hackers criminels, comme les agents des divers cyber-espionnage peuvent toujours entrer dans notre vie privée si l'on n'est pas soi-même capable de les en empêcher par de bons logiciels non marchands, donc gratuits, contrairement à Google et consorts qui jouent de nombreux jeux à notre dépend. En effet, ces derniers vendent tous les renseignements extraits de notre vie privée à beaucoup d'entrepreneurs, comme ils fournissent tout l'historique de nos communications des douze mois passés à première demande aux polices et à la justice française. Monsieur MANACH nous fait constater une notoire perte de nos libertés.

Résumé en mille mots

Le titre de ce livre est pour le moins racoleur, provocateur et restrictif sur le sujet abordé.

En effet, il aborde à la fois la mise en commun de beaucoup de données véhiculables par les médias, démocratisant de facto des aspects de vie privée des uns par la mise sous transparence de parties des intimités, et la réalité des risques auxquels ils s'exposent en utilisant en permanence les moyens de communication électronique interceptables par d'autres qui cherchent à savoir, ou mieux, à nuire. En balayant l'évolution des possibilités d'échange de grosses quantités d'informations entres personnes, gérables et stockables à certains "nœuds", l'auteur nous faire sentir que, malgré l'existence en France de la CNIL, nous ne sommes pas à l'abri d'usages néfastes de nos dires, nos écrits ou de nos comportements avoués, tous classables dans des fichiers, notamment de police, que les pouvoirs des puissants de l'Etat peuvent consulter à leur guise.

La différence de perception de ce risque existant entre la génération des adolescents et celles des adultes (nous dirons plus de 30 ans), vient du vécu par les plus vieux ou de l'avoir entendu relaté par ceux qui ont disparu pour les autres alors que les jeunes ont toujours vécu sous surveillance, sans crises graves. Les plus âgés se souviennent qu'à certaines périodes, mieux valait ne pas être au-devant de la scène, ne serait-ce que dans un fichier !

Les jeunes utilisent globalement mieux que les plus anciens, les réseaux sociaux et ne mettent à disposition de leurs amis que les informations choisies, les valorisant au moment de l'édition, mais ne pensent pas à leur devenir.

Cependant, avec tous les "bidouillages" possibles par des tiers et notamment certains "hackers", mais aussi pourquoi pas, les services secrets, toutes les informations sources peuvent être volées, modifiées ou dupliquées pour faire de faux papiers d'identité par exemple. Les faussaires savent produire de faux passeports (malgré le traçage de ce produit), comme vous soutirer de l'argent de votre compte bancaire en ayant pu lire une fois vos codes RFID de la puce de votre carte bleue, alors que cette dernière était dans votre portefeuille quand vous faisiez "la queue" pour entrer au Musée du Louvre.

Les disques durs de nos ordinateurs sont aussi facilement visitables par quiconque sait ouvrir leur porte. Des étrangers peuvent ainsi récupérer vos informations à "l'insu de votre plein gré" et sans les faire ni disparaître, ni même les modifier, ce qui se fait aussi.

Alors oui, la vie privée démocratisée a de bons côtés. Tout est public, on prétend ne rien cacher. Cela n'évite pas le piratage. Et les vieux, comme les jeunes s'accordent pour se montrer nus, mais pas à tout le monde de la même manière … et surtout pas à leur insu.

L'Etat français aide à protéger les informations des champs d'activité économique dits sensibles. Seules les entreprises dites stratégiques, les "startups" scientifiques de pointe ou les laboratoires sont éligibles à leurs services. Les individus, constituant le plus grand nombre, ne sont pas l'objet de protection. Par contre, nous sommes tous vidéosurveillés, souvent sur le domaine public, fichables par les polices et même traçables par nos téléphones portables. Nous sommes traités comme des ennemis de l'intérieur. Si nous sommes repérés, c'est à nous de prouver notre innocence, face à une inculpation par exemple … d'excès de vitesse.

On constate qu'il y a deux poids, deux mesures. Les uns sont aidés contre les attaques externes, les autres non ; ils sont au contraire contrôlés et surveillés comme de supposés délinquants en puissance auxquels il revient d'apporter la preuve de leur innocence.

Le rôle de la CNIL est mal assuré en matière de liberté individuelle ; cela vient de la partialité de ses hauts commissaires.

Alors encore une fois, les jeunes, comme les vieux, ont bien compris. La vie privée, d'un commun accord, n'est pas un problème lié à l'âge que l'on a.

Même si les jeunes sont moins sensibles aux risques potentiels que les vieux, ils savent, lorsqu'ils l'estiment nécessaire, s'y soustraire.

Les jeunes, comme les moins jeunes, ne sont pas des pigeons et n'acceptent pas d'être sous contrôle permanent. Un peu de surveillance, pourquoi pas … surtout si cela peut en rassurer certains. Mais au-delà d'une certaine limite, tous s'accordent pour reconnaître que les libertés individuelles s'en trouveraient bafouées.

Nombreux sont les Français qui refusent le glissement de l'état de droit vers une forme d'autoritarisme, sans vie privée et toujours transparent. Le contenu de fichiers de police, non à jour est inadmissible ; leur exploitation par le pouvoir est délétère. C'est pourtant ce que certaines personnes aimeraient voir venir alors qu'elles entretiennent les sentiments d'insécurité à travers leurs propos appelant à plus de fermeté vis-à-vis de communautés bien ciblées, cherchant par ce biais l'adhésion du plus grand nombre.

Sur la fin du livre, l'auteur explique quelques techniques pour protéger l'émission des données en les rendant non lisibles aux voyeurs, et nous protéger des assaillants de nos disques durs sur internet. L'emploi de la cryptographie comme de la stéganographie et les logiciels libres, sont abordés.

Globalement, il me semble que la lecture de ce livre va dans le sens de rassurer ceux qui ont peur d'utiliser internet et nous fait aussi réfléchir sur les risques de diminution de nos libertés individuelles à partir du moment où nous sommes

régulièrement filmés, fichés et comparables à un individu standard ne faisant pas de vagues.

Contenu du livre matière à débat

1. En un premiers temps, voyons quelle perception ont les jeunes de moins de trente ans et les autres de plus de trente ans, de ce qu'ils entendent par vie privée lorsqu'ils utilisent les moyens de communications électroniques.

11- Le partage des données par les utilisateurs des réseaux communautaires et sociaux de type web sont qualifiés de très bénéfiques par les individus et pour les communautés de travail. En effet, beaucoup de gens mettent en ligne beaucoup d'informations de toute nature, sans complexe.

La NSA (National Security Agency), voit d'un très bon œil ce courant d'émancipation que certains comparent à la libération sexuelle que l'on a tous bien connue dans les années 60-70.

L'auteur nous dit que certains jeunes livrent volontiers des indiscrétions les concernant, mais que d'autres sont très soupçonneux et méfiants. Ces derniers ne mettent en ligne que ce qu'ils veulent bien.

La géolocalisation aussi a des avantages, comme des inconvénients. Ici encore, si l'on veut rester libre de ses mouvements, il faut repérer la norme et gérer la marge de liberté que l'on peut justifier vis-à-vis de cette dernière. C'est de l'autocensure.

Olivier AUBER, chercheur indépendant, a lancé l'idée d'un "Club des naturistes numériques sur Facebook". Ce naturisme est salutaire lorsqu'il est partagé par ses adeptes. Il est déplacé lorsqu'interviennent dans le jeu, des voyeurs ; en effet, ces derniers ne cherchent pas la même chose. Le surplus d'informations possibles rend difficile la lecture et sa saine interprétation. Mais on peut se faire expliquer.

Ceux qui adoptent à grande échelle l'usage des nouvelles technologies, sont nos enfants et nos petits-enfants ; ils ont beaucoup à apprendre à ceux qui redoutent de voir leurs habitudes connues (qu'elles soient alimentaires, sociales ou organisationnelles). En effet, ils trouvent rapidement bon nombre d'idées pour résoudre leurs problèmes, quels qu'ils soient. Malheur à celui qui restera hors du système dans le futur, il risquera de reculer, plutôt que d'évoluer.

A contrario, trop se découvrir sur le net donne aux fichiers de police comme EDVIGE des arguments pour mieux nous classer dans des catégories en le reliant avec FACEBOOK, qui pourraient un jour nous être néfastes selon le type de régime politique.

Notre vie privée est effectivement moins mystérieuse lorsque l'on est mieux connu par beaucoup plus d'individus. Pour autant, avons-nous perdu notre liberté ? Non ! Sauf en régime totalitaire.

Antoinette ROUVROY rappelle que "la vie privée n'est pas un droit fondamental", elle est la condition nécessaire à l'exercice des libertés fondamentales et que "le droit à la protection de la vie privée est à comparer à un système immunitaire".

Pour terminer ce chapitre, à l'époque des réseaux, l'auteur compare la vie privée à une citadelle bien défendue, assiégée de rapaces avec lesquels il serait bon de composer en acceptant progressivement des changements environnementaux négociés et des pratiques mieux encadrées selon les aspirations des protagonistes. Ainsi est approché le concept de vie privée par les citoyens de plus de trente ans.

12-Voyons maintenant l'analyse que MANACH nous propose de la perception de ce concept de vie privée par les plus jeunes.

Au-delà des inhibitions des vieux "cons", la génération du net ne sait pas vraiment ce qu'est la vie privée. MANACH appelle cette génération, celle des transparents.

Danah BOYD rappelle que la vie privée est un "privilège" qui remonte à la déclaration des droits de l'homme, article 12, avec : "Nul ne sera fait objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation".

Cela s'applique en fait peu aux enfants ; en 1946, c'était surtout une affaire d'adultes. Les parents sont perçus surveillant trop leurs enfants, pour les sur"protéger" de tout, et beaucoup de ces jeunes mineurs préfèrent communiquer par SMS au lieu d'être entendus par les parents, en face à face.

Les enfants aiment pourtant les espaces de socialisation, physiques plutôt que virtuels … mais sans le contrôle parental.

Les technologies nouvelles ne sont pas particulièrement plus faciles d'accès aux enfants. C'est cependant en apprenant à s'en servir qu'ils se socialisent et ainsi récupèrent des libertés multiples (celles qui angoissent les parents et les adultes en général).

Emily NUSSBAUM a fait, en 2007, un portrait des enfants du numérique et analysé leur approche de la vie privée. "Les enfants n'ont aucune pudeur, de sentiment de honte, ni de vie privée. Ce sont des frimeurs, des "putains" de la célébrité, de petits coquins de la pornographie qui mettent en ligne toutes sortes de messages pour des amis virtuels ou réels. Ils ne s'intéressent qu'à l'attention qu'ils suscitent". Leur terrain de jeu est de facto, bien plus vaste que celui qu'avaient leurs parents à leur âge,

alors qu'eux-mêmes ont aujourd'hui trente-cinq ans. Si ces derniers n'agissaient pas de même manière en leur temps, c'est simplement parce que cela n'existait pas, technologiquement.

Les enfants d'aujourd'hui sont préparés dès leur plus jeune âge en étant filmés à leur insu. Que ce soit avant de naître, par échographie de leur fœtus, par la vidéosurveillance en maternité, à l'entrée de leur école, dans la cour du lycée ou sur certaines places urbaines où ils sont tracés. Puis la carte bancaire ou le téléphone portable qui les géolocalisent. En conséquence, ils ne sont pas gênés pour se répandre sur le net, pourvu qu'ils montrent ce qu'ils pensent de mieux, ici et maintenant. Pour eux, la vie privée ne veut pas dire grand-chose. Ils aiment faire savoir … mais avec cependant une carapace à leur mesure.

Cela ne les empêche pas d'être sentimentaux … et de garder leurs secrets aussi longtemps qu'ils le décident.

A propose de "sexting", pour certains, c'est normal ; ils sont décomplexés tout en restant cependant plus ou moins conscients de certaines conséquences. Ils sont très conscients que la jeunesse est belle. En se mettant en ligne, ils sont confrontés aux mêmes problèmes que les hommes et femmes politiques. Ils sont devenus des personnages publics, et pour cela ils contrôlent au mieux leur communication. Des dérapages font cependant réfléchir, tel que le petit ami éconduit peut se venger en envoyant à tous les camarades de classe un petit film de ses ébats amoureux avec son ex partenaire et dégrader l'image de l'autre. Mais cela semble fonctionner dans les deux sens.

Pour la plupart des adultes parents, le jeu est risqué ; la rencontre d'un pervers aguerri peut être dangereuse. Les adolescents en sont conscients et très rares sont ceux qui s'y font attraper. C'est la principale raison qui leur fait quelquefois dire que ceux qui pensent qu'ils ne font que du sexting sur le net sont "des vieux cons". Surtout qu'en réalité, nombre d'enfants subissent toujours, aujourd'hui, des violences familiales du ressort de la "Justice des Enfants" ou de l'ASE.

La sexualité a toujours "travaillé" les enfants ; même grands, certains consomment des revues spécialisées. C'est donc un réel sujet de la vie. Pourquoi pas sur internet !

Cependant, l'humain a toujours eu besoin de vie privée pour s'épanouir.

Pour les jeunes, la notion de vie privée renvoie à la faculté de contrôler l'image que l'on donne de soi sur le net. Ce contrôle induit la possibilité de corriger ce qui circule publiquement pour mieux affirmer les limites du sens donné aux messages.

Internet permet à tout le monde de devenir un personnage public. Mais à chacun de trouver la possibilité de quérir le moyen de protéger sa vie privée.

Sur FACEBOOK, il n'y a point de vie privée, tout est rendu public, c'est leur fonds de commerce. A partir de l'instant où l'on va sur ce réseau, on sait qu'il faut assumer. Dès lors, toute information privée peut être exploitée par quiconque y voit un intérêt, dont celui de nous surveiller.

Celui qui a le pouvoir est celui qui regarde, comme dans le panoptique de Jérémy BENTHAM où le surveillant de prison pouvait voir beaucoup de prisonniers sans être vu. Dans le cas du net, on peut dire qu'en plus, tout le monde échange avec tout le monde, en plus d'être vu par ceux qu'on intéresse. Chacun peut donc se préparer à se montrer et à répandre.

La comparaison des deux situations est évidente ; dans le cas du panoptique de 1875, les surveillants pouvaient exercer une autorité absolue et silencieuse, alors que sur le net, chacun des participants est à rigoureuse égalité avec tous les autres.

Le net à ce stade, aide à promouvoir sa vie privée et s'y faire connaître, sans s'en méfier et sans cacher ce que l'on veut montrer.

Andy WARHOL disait que chacun aura ses quinze minutes de célébrité dans sa vie. Aujourd'hui, nous dirions plutôt que nous cherchons notre quart d'heure d'anonymat.

Les gens aspirent toutefois de plus en plus à reprendre le contrôle de leur vie privée, même si nous sommes filmés régulièrement et tracés tous les jours.

Aussi, de même la libération sexuelle des années 68 à décoincé beaucoup de gens, elle n'a pas fait que des dépravés ; il est plus facile aujourd'hui qu'hier d'être un personnage public en contrôlant les images de sa vie privée mises en circulation. Toujours à la suite de 68, la sexualité, le féminisme et le droit des homosexuels ont évolué et le patriarcat devient moins pesant. Ce n'est pas parce que beaucoup d'utilisateurs du net mènent une vie publique que tous doivent en faire de même. Voici comment les jeunes perçoivent leur vie privée.

2. A ce niveau de lecture du livre de Monsieur MANACH, nous avons la perception première du concept de vie privée de nos contemporains. Il va maintenant tenter de nous livrer des arguments pour analyser l'apport de l'utilisation des nouvelles technologies, confrontées aux tendances politiques des gouvernants, afin de mieux comprendre les risques sociétaux. Il commence par nous expliquer les difficultés que le Président de la CNIL a rencontrées auprès de nombreux députés lorsqu'il essayait de leur faire comprendre les risques générés par ce type de communication. En effet, le "net" devenait le gisement potentiel de renseignements utilisables dans des fichiers de police.

21-A la suite du constat caricatural de l'utilisation d'internet par les adolescents, l'auteur nous explique **l'évolution des moyens législatifs encadrant l'usage de cette nouvelle technologie**. D'abord, il se réfère au vécu en Allemagne de l'Est, sous le contrôle de la STASI en nous disant, un peu ironiquement, que sous ce régime communiste, les

allemands de l'est, habitués à la surveillance, la supportaient bien, car ils avaient même un droit à l'insurrection. Mais peu l'utilisèrent, et pour cause ! L'invention du fichier EDVIGE en 2008 en France suscita beaucoup d'inquiétudes. Les parlementaires auditionnant en 2009 le Président de la CNIL au sujet de l'évolution de la Loi Informatique et Libertés, Monsieur Alex TURK, venu leur présenter le nouveau droit à l'oubli, s'est entendu qualifier les internautes comme la "chienlit de l'époque". Nous mesurons ici le chemin à parcourir pour faire avancer l'informatisation de la société française.

Il est vrai que nous pouvons doublement être tracés par un Big Brother, physiquement par les vidéo surveillances, géo localisés avec nos téléphones portables et temporellement repérables sur les réseaux sociaux par les moteurs de recherche.

En réalité, l'exploitation croisée de ces deux types d'informations est réservée aux délinquants et aux déviants dans le collimateur des surveillants. Nous pouvons cependant toujours craindre le pire. Les internautes plutôt jeunes écrivent sous leur responsabilité en toute liberté, sans opposition de génération avec les plus âgés. Contrairement à ceux qui étaient jeunes entre 1960 et 1970 qui défiaient à leur manière le conservatisme de leurs aînés, ceux d'aujourd'hui ne tiennent pas compte des vieux, alors que lesdits "vieux", acceptent mal l'attitude des jeunes qu'ils qualifient de "petits internautes inconscients". En constatant l'aspect diffusion des logiciels libres et la mise en "ligne sauvage" d'œuvres culturelles, l'auteur explique que les petits génies de l'informatique font bouger les mentalités.

Pour permettre la culture au plus grand nombre, tout en protégeant l'artiste, il faut pouvoir diffuser des œuvres en limitant la surveillance et les contrôles des individus sur internet en faisant le pari de la rétribution du créateur par d'autres circuits.

22-Les internautes jeunes sont de plus en plus à l'origine des sources de nouvelles réglementations et obligent à continuer de légiférer afin de construire des règles de fonctionnement sur internet. Les adultes bien évidemment utilisent internet et y trouvent de plus en plus ce qu'ils y cherchent. Par contre, il faut toujours penser à ce que peuvent faire ceux qui piochent dans les informations mises en ligne et éviter que ces derniers viennent nous nuire. A partir de l'instant où l'on a mis en ligne des points précis de sa vie privée, cette dernière devient une information publique disponible. Alors comment contrôler les usages qui peuvent être faits de tous ces renseignements ? C'est là tout le problème de ceux qui veulent démocratiser leur vie privée. Tous les moyens de communication d'aujourd'hui ne font que rapprocher vie publique, vie privée, ne serait-ce que par la simple possibilité de rapporter du travail faisable à la maison par un cadre, ou être joignable par téléphone mobile partout. Comme toutes nos communications passent par internet, les moteurs de recherche que nous utilisons nous connaissent et peuvent vendre nos informations de vie privée à leurs clients. Le souci de la CNIL est de veiller à faire en sorte que le temps de conservation de nos données en mémoire ne soit pas trop long. Nous sommes théoriquement loin de l'utilisation fallacieuse de nos données par des régimes fascistes, dictatoriaux et autres formes de totalitarisme**.**

Malheureusement, on ne peut pas totalement faire confiance aux prestataires informatiques. En effet, les services secrets des pays piochent en permanence dans les banques de données qui leurs sont accessibles. Toutes les atteintes ressenties à nos libertés constatées doivent être dénoncées et combattues.

Depuis 2002, les prestataires respectent les consignes et livrent peu de fichiers. Cependant, des entreprises et des administrations perdent ou subissent des vols ou des copies de certains fichiers par "hackage".

Il est relaté aussi que beaucoup de fuites constatées proviennent directement des utilisateurs eux-mêmes qui font des erreurs, par exemple, d'adressage d'envoi groupé, ou simplement subissent une agression à la suite de non mise en arrêt de leur ordinateur le soir, après le travail. Ce dernier dysfonctionnement permettant à certaines personnes l'usurpation d'identité du titulaire de l'ordinateur. Dès lors, ce dernier est vulnérable.

23-La société de surveillance est-elle devenue une réalité ?

Sommes-nous énormément surveillés ? Arrivons-nous à contrôler partiellement notre vie privée, notre liberté ? Rien n'en est moins sûr. Depuis plusieurs années, Alex TURK (CNIL), nous dit que progressivement, nous sommes arrivés à la société de surveillance. Nous sous estimons sa réalité depuis le 11 septembre 2001, car à l'avis du profane, cet évènement aurait dû être évité. Nous savons que le coût du travail de surveillance des personnes dangereuses, des terrorismes, d'espionnages militaires, d'espionnages économique a été calculés à plus de 1000 milliards de dollars pour l'année 2002 pour les pays de l'OCDE (ramené au PIB mondial de 28470 et de la France 1303, soit 3.5 % du PIB mondial).

Les missions de surveillance sont nombreuses à être confiées à des entreprises privées. Pour montrer le pressant besoin de mise en œuvre de ces industries, il est beaucoup montré d'images de catastrophes attribuables à la criminalité ou au terrorisme. En parallèle, les pouvoirs publics toujours soucieux des prochaines élections mettent de plus en plus l'accent sur la sécurité, en contrepartie d'une surveillance sociale générale accrue qui est finalement le résultat d'une demande des peuples. Nous sommes loin du temps où l'action politique était portée par des idéaux d'égalité et de liberté (sans parler de fraternité). Si les politiques ne freinent pas la spirale infernale de la prolifération des vigiles partout, nos démocraties finiront par en pâtir.

En effet, il ne faut pas confondre garantir la sécurité publique avec lutter contre le sentiment d'insécurité qu'entretiennent certains lobbies.

Un sentiment est irrationnel, il peut être discriminatoire et la société dans laquelle nous vivons pourrait passer aisément de surveillée à contrôlée, si cela devenait le choix des politiques au plus haut niveau (pour ma part, je ne le souhaite pas).

Concrètement, la sécurité c'est, la porte blindée de l'appartement, le code secret de la carte bleue ou de l'ordinateur, la ceinture de l'automobiliste ou le casque du motard. Ils apportent un niveau de confiance alors que rouler en voiture avec un mouchard, avoir une caméra cachée dans le hall d'entrée de l'immeuble ou un mouchard sur les téléphones portables des employés comme de nos enfants brise le contrat de confiance que les individus peuvent avoir entre eux et vient accroître l'insécurité chez ceux qui sont tracés. A ce niveau de raisonnement, le choix est politique en ce qui concerne les mises en œuvre sur la voie publique.

Le fichage génétique avait été institué pour les seuls délinquants sexuels récidivistes jusqu'à il y a peu de temps en arrière. Aujourd'hui, presque toutes les affaires de police judiciaire font appel à ce fichage. Ici encore, se pose le problème de libertés.

C'est le Président de la CNIL qui tire la sonnette d'alarme : peu de gens se révoltent contre ces décisions qui sont des atteintes aux libertés et dit qu'il faudra défendre le droit des individus "malgré eux" en rédigeant un droit individuel à la protection des données et à la vie privée.

De nos jours, si l'on demande un accès aux divers fichiers pour procéder à une rectification de données, on a de grandes chances d'avoir raison, si l'on se sait être fiché. Il est avéré que :

- l'ex STIC comportait cinq millions de Français suspects et vingt-huit millions de victimes. Ce fichier ne fut légalisé qu'en 2001, soit dix ans après sa création.
- L'ex JUDEX comportait trois millions de suspects, qu'il existait depuis longtemps, et ne fut légalisé qu'en 2006. Pour plus de 25% d'entre eux, de grosses erreurs existent toujours dans les renseignements de police.

Aujourd'hui, ces deux fichiers n'en constituent qu'un seul qui s'appelle ARIANE contenant toujours un fort taux d'indications erronées. Tous les gens ainsi fichés le sont souvent à tort.

Un gros travail d'analyse fut fait en 2008 :*

- 66 % des fiches contrôlées ont été modifiées,
- 17 % des fiches contrôlées ont été supprimées.

Seulement 17 % étaient exactes… pour 83 % de partiellement ou totalement fausses. C'est grave !

Les policiers gestionnaires de fichiers imputent ces erreurs au non-retour des informations des Procureurs en cas d'affaires classées sans suite, en cas de relaxe, d'acquittement et de non-lieu. Tous les individus concernés étaient 1 084 228 personnes en 2010 toujours suspectes avant ce tri.

Un exemple de durée de garde d'informations : homosexuel 40 ans.

Avant 2010, les gouvernements ont préféré construire des prisons neuves (même privées), plutôt que se construire un gros outil informatique de gestion de ces informations entre les polices et la justice. Nous souffrons de la guerre entre le Ministère de la Justice et celui de l'Intérieur.

Les mauvaises informations contenues dans les fichiers de police peuvent porter préjudice aux individus. Ainsi en 2009, plus d'un million de postulants à des emplois publics ont eu à satisfaire aux enquêtes administratives de moralité. Ces enquêtes sont régulièrement renouvelées pour certains emplois en poste pourvu. Ainsi en 2005 et 2006, plus de trois mille cinq cents personnes travaillant en zone sensible à Roissy ont perdu leur emploi à la suite de l'ouverture de leur "casier". C'est à se demander sur quels critères ils avaient été recrutés ou si les règles de maintien dans l'emploi n'ont pas évolué ? De nombreux recours eurent lieu pour des agents pour lesquels il était flagrant qu'ils subissaient une injustice.

En 2009, le Ministre HORTEFEUX supprime le fichier EDVIGE pour le remplacer par CRISTINA qui était l'addition de celui de la DST et celui d'EDVIGE. D'où retour à la case départ, mais avec une seule police au lieu de deux. Dès ce jour, il n'y eut plus d'opposition alors que la nouvelle mission de ce fichier fut classifiée "secret défense" ; ce qui permet presque tout.

Dès lors, la France s'est découvert beaucoup d'ennemis intérieurs tels que gauchistes, contestataires, hooligans, nombre de groupuscules d'extrême droite et d'autres …, même des retraités en colère sont fichés, comme les bandes d'adolescents.

Le fichier PASP (Prévention des Atteintes à la Sécurité Publique) est le premier et vise même nos enfants jusqu'à 13 ans ; le second fichier a pour acronyme EALSP (Enquêtes Administratives Liées à la Sécurité Publique), visant tous les individus de plus de 16 ans dont il convient de jauger la moralité. La conséquence de ces moyens mis en œuvre est le fichage policier de beaucoup de gens qui ne sont pas des délinquants.

A ce stade, il n'était plus question de mettre en fiches les gens selon leur vie sexuelle ni leur santé, pas plus que leurs opinions mais plutôt leurs "activités publiques" et leur comportement. Tout ceci est bien flou.

Mais on y avait recensé des mineurs, des militants de n'importe quoi et leurs relations. Ici il y a un gros problème pour les défenseurs de droits de l'homme et des libertés.

Malgré la position anti fichier de la commission des lois présidée par un UMP, avec l'accord de l'opposition du moment dans cette commission, le Ministre n'a fait qu'imposer ce qu'il voulait et fit modifier certains alinéas de contrôle de la CNIL pour la stériliser sur cette question.

La CNIL, pionnière mondiale des autorités indépendantes de protection de la vie privée, est souvent perçue comme l'ultime rempart contre tout fichage. En réalité, elle est très souvent stérilisée. Nous avons eu la preuve dans un autre domaine lors de la discussion du projet de loi Création et Internet. D'où l'invention de la Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet (HADOPI) et défendue de haut vol par un des commissaires importants de la CNIL, alors que cette loi est considérée comme liberticide. En effet, si l'on est accusé d'avoir sur internet, agi de manière jugée incorrecte, c'est à nous de prouver notre innocence d'un usage non marchand. La loi était censée protéger les industriels et les artisans, voilà qu'elle suspecte tous les intervenants.

Mais la CNIL surveille, elle ne dénonce pas.

Elle a reçu 33 000 plaintes en vingt ans et délivré 47 avertissements pour 16 dénonciations au Parquet. Alors que pour année, en Grande-Bretagne, on peut dénombrer 145 instructions de dossier pour 130 condamnations, en France, la CNIL agit tout en nuance et propose aux contrevenants des actions correctives qui sont respectées dans 90 % des cas. Les résultats ne sont pas publiés. Ainsi, nous ne sommes pas au courant des problèmes afférant à la protection de notre vie privée sur les moyens informatiques que nous utilisons. Cela pourrait ne pas être très rassurant.

Le monde entier enterre t'il la vie privée ? Non bien sûr mais le 28 janvier 2010 eut lieu la 4ème Journée de la Protection des Données Personnelles initiée par la CE. Le seul problème duquel il fut discuté fut celui de ceux qui relatent la physionomie de leurs fesses sur FACEBOOK.

Les recruteurs du monde entier consultent sur ordinateur les informations mises en ligne par les candidats de quelque nature qu'elles soient. Les statistiques montrent que la plupart des candidats y trouvent leur compte. Les images de fesses ne semblent gêner personne.

3. Alors, la vie privée des individus est-elle soluble dans le Web, comme à chaque lieu de vie ?

> **31-La CNIL, en France,** bien que peu efficace, essaie de faire réfléchir les jeunes de 12 à 16 ans sur la relation privée et internet, sur les messages coquins et plus ou moins documentés de photos intimes. Ce genre d'action semble peu les faire réagir alors que le droit à l'oubli sur les réseaux n'est pas encore acquis. Selon les messages mis en ligne, ceux-ci sont consultables entre 1 et 40 ans. La vie privée de beaucoup de gens est durablement livrée à la vindicte populaire comme policière**.**

Quand on sait que 25 % des fichiers policiers sont hors la loi, que leur nombre progresse très rapidement (+ 10 % par an) et que 1.2 million de gens sont génétiquement identifiés, que 75 % d'entre eux sont présumés innocents, on doit se reposer politiquement la question de savoir ce que l'on veut que devienne notre vie privée.

Les histoires de fesses invoquées par la CNIL et la CE sont un détail grivois qui cache le gros de l'iceberg : la liberté des individus à avoir une vie privée dans un système démocratique.

> **32-Une autre atteinte à la vie privée pourrait voir le jour,** suite à la découverte aux USA d'un jeune homme avec un slip rempli d'explosif dans un avion0 heureusement, l'explosion n'eut pas lieu**.**

Pour remédier à cela, certains pensent s'équiper de scanners portiques spéciaux pour tous ; mais ces derniers montreraient les anomalies corporelles corrigées par prothèse ; ce qui n'est pas pensable aux yeux de nombre de personnes. Alors, nous continuons à avoir peur des attentats. Et ainsi le terrorisme aura encore une fois gagné, renforçant un peu plus le rôle des entreprises de contrôle … D'autant plus que le terrorisme trouvera toujours de nouvelles solutions pour déjouer les contrôles installés, quels qu'ils soient.

Une attaque ennemie ne peut pas détruire notre mode de vie. Nos réactions sécuritaires et les discours anxiogènes de nos dirigeants sont beaucoup plus graves et incitent les terroristes à devenir de plus en plus inventifs.

> **33-En réaction à ces idéologies sécuritaires,** 10 % des lycées anglais surveillent les élèves par caméras. Les caméras sont installées en salles de classe, dans les couloirs, dans la cour et dans les toilettes. Quelques soient les motifs invoqués, un tel système de surveillance est plus un conditionnement à la perte d'initiative, à l'apprentissage du respect du plus fort et à l'application des codes moraux prônés dans ce type d'établissement qu'à l'apprentissage du "grandir". Nombre d'enseignants en sont conscients, mais semblent minoritaires et impuissants. Ils disent qu'avec tous ces appareillages, ils risquent bien de passer à côté de leur devoir d'éveil et d'ouverture de la jeunesse au questionnement en respectant leurs singularités tout en les protégeant. Cet univers quasiment carcéral, au nom de convenances administratives, prive les jeunes de l'expression de leurs réactions interpersonnelles et semble contraire à une bonne acquisition d'autonomie (contraire à l'aide à grandir).

En France aussi, il se développe dans certains établissements des installations de vidéosurveillance à l'entrée de l'enceinte, dans les couloirs, à l'accès des cantines, dans les infirmeries et dans les salles des toilettes ainsi qu'au passage à l'entrée de chacun des WC. Dans les dortoirs, des haut-parleurs diffusent de la musique le matin pour le réveil et quelques institutions ont installé des micros pour limiter les discussions le soir après le couvre-feu. La technologie remplace le surveillant d'internat ; c'est le préfet des disciplines qui sermonne les récalcitrants. Dommage d'en arriver là !

> 34-Aux dires de certains, **la surveillance ne doit pas gêner ceux qui n'ont rien à se reprocher,** rien à cacher. Rien n'est moins sûr !

Le cardinal de Richelieu avait dit : "Apportez-moi deux lignes du plus honnête homme et j'y découvrirai de quoi le faire pendre".

Telle est la phrase sur laquelle nous pouvons méditer. En effet, quand on cherche, on trouve. Il est facile de relater une cause pour discréditer un individu et le priver de liberté. Ce n'est qu'une question de dialectique et d'arguments bien manipulés.

Aujourd'hui, le problème vient du voyeur et non pas de celui qui est surveillé, de celui dont la vie privée est violée. Les paranoïaques ne sont pas ceux qui s'étonnent d'être surveillés, mais ceux qui veulent surveiller tout le monde "à l'insu de leur plein gré". La question n'est pas de savoir si ceux qui sont filmés ont quelque chose à cacher, mais de savoir ce que veulent protéger ceux qui nous surveillent, sans notre accord.

En démocratie, l'accusation apporte la preuve de ce qu'elle avance ; ce n'est pas aux accusés de prouver leur innocence. Le problème des atteintes à la vie privée est idéologique, les "people" en usent, mais beaucoup en souffrent.

Quand on cherche, on trouve. Par exemple, les Français nés à l'étranger … qui durent en 2009, apporter plusieurs documents prouvant qu'ils étaient bien Français ou des SDF qui se sont vus refuser le RSA au motif qu'ils étaient trop propres.

Aujourd'hui, avec tous ces voyeurismes, ce n'est pas parce que vous n'avez rien à cacher, que jamais rien ne vous sera reproché. Quand on veut chercher une faille, on trouve toujours.

C'est du KAKFA,

Dans la société de surveillance, de contrôle, de suspicion, le problème est la disparition de la valeur sociale de la vie privée. Le problème n'est pas tant la surveillance des données mais l'utilisation qui est faite de ces données, sans inclure la personne concernée au procès qu'on lui intente ou à l'interprétation du croisement de ces données à but marketing. Tout ceci correspond à la mise en œuvre d'un monstre froid bureaucratique qui affecte les relations des individus avec l'Etat … ou avec les clients de GOOGLE.

La surveillance généralisée risque de nous faire aller vers une société opprimante, avec perte de libertés certes, mais surtout avec la destruction de la confiance sociale ; on n'osera plus inventer, ni plaisanter, ni critiquer … de peur qu'un jour on nous le reproche pour de mystérieuses raisons.

La vie privée va bien plus loin que ce que l'on fait chez soi. Elle inclut notre façon d'être dans la société. L'auteur, à ce stade, nous dit qu'il espère que nos gouvernants dans notre actuelle démocratie, feront preuve de bon sens et mettront rapidement un terme à leur actuelle paranoïa sécuritaire (le livre a été rédigé de 2009 à 2010).

En poussant plus loin le raisonnement, si vous n'avez rien à vous reprocher, vous n'avez pas à avoir peur d'être filmé au lit. Pour application, lorsque l'on soupçonne des parents délinquants avec leurs enfants, on pourrait supposer les surveiller dans leur lit puisque chaque viol d'enfant par un parent est fait dans la chambre du parent ; et la fréquence est plus grande que l'on croit. Mais non, il est impossible de le faire et ce n'est pas parce que le juge ne l'impose pas qu'il cache personnellement aux autres quelque chose. A ce stade du raisonnement, on se rend compte que ce n'est pas le refus d'imposer aux autres une surveillance qui laisser soupçonner que nous serons de bons candidats à ladite surveillance.

Certains prétendent que les caméras sont dissuasives. Oui, devant elles, mais pas hors champ. Par ailleurs, la caméra n'empêchera jamais la crise chez un individu agissant de manière pulsionnelle. Par contre, les caméras diminuent le sentiment d'insécurité des autres ; à vrai dire, elle rapporte des voix lors de la plus proche élection politique à celui qui les a initiées.

La vidéosurveillance est un cautère sur une jambe de bois ; ce n'est pas par ce procédé qu'on empêchera la délinquance de s'exprimer.

Depuis 2001, tous les Français équipés d'ordinateur et d'accès internet sont tracés et leurs communications sont stockées pendant un an par leur fournisseur d'accès, afin de les restituer à la justice française en cas de suspicion quelconque, sur simple demande.

Cette disposition est la première mise en œuvre par n'importe quelle dictature ; cela s'appelle abolir la vie privée, la liberté d'expression, la liberté d'opinion et de circulation, cela généralise la suspicion en mettant tous les citoyens sous surveillance.

A contrario, un régime démocratique fait confiance aux citoyens et considère que seulement une petite partie de la population viole les lois. La présomption d'innocence est la règle. C'est à l'accusation de démontrer la culpabilité des suspects et non l'inverse. C'est ce qu'on appelle l'état de droit. En France, la CNIL a pour rôle de donner son avis sur tout système d'identification, de fichage et de surveillance. C'est pour cela que le pouvoir politique, avant 2010, a agi pour limiter son action et son pouvoir avec en son sein, des administrateurs acquis à la bonne cause du moment.

Trop de vidéosurveillance montre que le pouvoir politique à certains moments, sombre dans l'hystérie et la paranoïa sécuritaire ; ce qui revient à considérer que le terrorisme est le grand gagnant et qu'il faut en avoir peur.

Tous ceux qui veulent culpabiliser les gens, de sorte qu'ils acceptent la surveillance, sont très souvent ceux qui ne veulent pas être transparents. Nous en avons souvent des exemples parmi les politiciens.

Certes, pour certains, la vidéosurveillance ne leur pose pas de problème. L'auteur cite ici le travail fait au CNAM par François EWALD qui chercha à comprendre ce pourquoi la vie privée n'est pas un problème de "vieux cons" et ce pourquoi les "petits

cons" aujourd'hui qui ont grandi constamment surveillés, ont de fait appris à jouer de cette surveillance et à se mettre en scène plutôt que d'être passivement observés à leur insu.

Un expert de sécurité informatique américain expliquait que s'il y avait eu, il y a cent ans, des caméras dans les chambres de nos grands-parents, il y aurait eu de moins en moins de bébés car les gens ne feraient plus l'amour et nous ne serions peut-être pas là !

En réalité, la notion de vie privée nous protège de ceux qui ont le pouvoir, qu'il soit tyrannique ou provienne de menaces physiques extérieures ou encore d'une surveillance constante par une autorité locale. La liberté est la sécurité sans l'intrusion dans la vie privée.

Une surveillance omniprésente par des polices n'existe que dans des Etats policiers. C'est pour cela qu'il faut soutenir haut et fort le respect de la vie privée même si l'on n'a rien à cacher.

> **35-L'Histoire, de 1789 à aujourd'hui, est cependant riche d'enseignement en matière de liberté.** Quand de nombreuses personnes ne s'étonnent pas du traçage, on est entrés dans un monde sans souvenirs**.**

En effet, en démocratie, le problème est le voyeur, le violeur, mais pas la victime, même si certaines filles montrent leurs seins à la plage. Le féminisme a permis de renverser la charge de la preuve et c'est bien.

Traiter tous les gens comme de potentiels délinquants est contraire à nos principes démocratiques ; c'est un retour en arrière de notre mentalité d'enfants des "lumières".

La loi Informatique et Libertés a été adoptée par les gens de gauche comme de droite qui se rappelaient de l'utilisation faite des fichiers. Cette loi démocratiquement votée rappelle qu'on ne peut pas ficher, surveiller n'importe qui, n'importe où, n'importe quand. Hors de cas précis, la vidéosurveillance doit être proscrite.

Cette loi est d'autant plus importante, dans nos démocraties occidentales, que lorsqu'un régime policier a un individu dans son viseur, il est présumé suspect, il doit apporter la preuve de son innocence. L'absence de mobile, comme par exemple ne pas pouvoir préciser le contenu exact d'une conversation téléphonique sur terminal fixe ou ne pas toujours être traçable physiquement par son téléphone mobile, est devenu à charge. C'est du KAFKA, c'est le monde à l'envers.

4. Nous venons de voir que l'on doit toujours être prêt à se défendre face à toute accusation de police. Mais, que fait l'Etat pour nous protéger de l'ennemi extérieur ?

Certains services de l'Etat (DST) aident les industriels, les laboratoires, les "startups" à se protéger de la piraterie sur internet. Par contre, il ne fait rien pour tous les autres, les particuliers ; au contraire il se sert dans leurs données si cela l'arrange.

> **41-Heureusement, il existe des hackers. Les hackers sont souvent considérés comme des pirates, alors qu'au contraire, ce sont de très bons utilisateurs, bricoleurs, débrouillards. Ils sont aussi développeurs de logiciels (libres de préférence) mais doivent rester dans l'ombre pour garder leur liberté. Certains vivent de leurs compétences en devenant prestataires informaticiens.**

Deux types de hackers existent : ceux qui nagent réellement dans la piraterie en utilisant leurs compétences pour nuire aux autres et ceux qui développent des sécurités pour des clients. Ils sont tous repérés par la DST et sont souvent sans complexes. Ils arrivent à trouver tout ce que vous n'osez pas demander sur internet.

Mais les barrières aux non-connaisseurs sont nombreuses. En effet, la technologie informatique utilise de plus en plus les puces dites RFID (Radio Fréquence d'Identification). Or, ces petits objets, placés sur un passeport, sur une carte de santé, ou implantés sous la peau pour certaines personnes, sont facilement lisibles et modifiables par des informaticiens électroniciens zélés et compétents. La CNIL en France, s'est élevée contre ce moyen de traçage des personnes … en relatant surtout les risques de se faire voler des données très personnelles ou même dans certains cas, se les faire modifier. La modification peut être lourde de conséquences au moment, par exemple, d'embarquer dans un avion américain. C'est ce qui est arrivé à Ted KENNEDY alors Sénateur américain.

L'auteur nous dit qu'il préfère que les individus renseignent tous ceux qui veulent savoir (quoique que ce soit à leur sujet), sur internet, plutôt que ces derniers soient tracés par un système quelconque, que des individus mal intentionnés peuvent lire et surtout modifier ou enlever des données pour s'en servir à d'autres usages (exemple : fabrique de vrais faux papiers avec tous les identifiants d'un tiers sans que ce dernier ne le soupçonne).

Il en est de même pour nos ordinateurs. Ces moyens de communication sont tellement sujets à agression, qu'il est prouvé que sans protection, ils avaient une durée de fonctionnement normal de quarante minutes en 2003, vingt minutes en 2004 et trois minutes en 2010. Aujourd'hui, le délai est descendu à quelques secondes.

C'est pour cela qu'il est recommandé d'utiliser une bonne protection contre les virus, contre les hébergements clandestins et autres chevaux de Troie.

> **42-Mais alors, comment se protéger de tous ceux qui nous épient** pour le pire et le meilleur par une quelconque cyber surveillance ?

Savoir protéger son ordinateur, c'est bien ! Rester maître des données qu'on partage sur le net, c'est mieux.

Nous sommes en France tous surveillés à travers les usages que l'on fait d'internet, (c'est le fournisseur d'accès qui répond aux demandes de polices, -stockage pendant un an-). Pour savoir comment protéger sa vie privée, l'auteur nous commente d'abord pourquoi la France a décidé de placer tous les internautes sous surveillance puis comment se protéger des pouvoirs.

La cyber surveillance qui nous concerne tous, nous les internautes, est celle que pratique l'Etat vis-à-vis de nous.

Suite aux attentats du 11 septembre 2001, les Etats-Unis ont renforcé les procédures de surveillance de contenu des messages transmis par internet. En réaction à cet état de fait, de nombreux individus et entreprises ont appris à cacher encore mieux leur contenu de courrier par stéganographie ou par cryptographie. Ces dernières méthodes sont devenues prohibées ; la France a pris la même règlementation que les USA. Aujourd'hui, seulement, les entreprises dites sensibles, dont les critères de classification sont toujours évolutifs et les organismes classificateurs, sont autorisés à se protéger par cryptographie. Mais il est nécessaire de donner à la DST en France ou NSA aux USA, la clé de cassage des programmes de protection pour que ces derniers puissent contrôler à leur guise.

Tout individu non autorisé (politique, commerçant, chercheur, etc.) maquillant ses écrits par cryptographie est suspecté délinquant. Pire encore, si quelqu'un maîtrise un procédé de stéganographie (par essence détectable seulement par les initiés) et que par hasard il soit "vendu" [1] à la DST, il encourt rapidement toutes sortes de contrôles et justifications de son usage d'un tel procédé (tombant sous la loi de novembre 2001 - LSQ : Loi sur la Sécurité Quotidienne). Cette loi fut contestée par la Gauche, mais le Conseil Constitutionnel de France n'en fut même pas saisi, alors qu'elle sort de la légalité républicaine et qu'ainsi, la France n'est plus un état de droit. La Loi LSI (Sécurité Intérieure) de 2003 a entériné la LSQ.

Finalement, l'opinion publique bien préparée à protéger les secrets des industries et laboratoires, a accepté de se laisser tracer la vie privée de tous, essentiellement par peur du terrorisme.

Tous les Français ne sont cependant pas d'accord.

> **43-Comment échapper à la cyber surveillance ?** (de l'Etat en premier). Pour bien protéger sa vie privée, la première condition est de renseigner sur sa personne sous pseudonyme ; ce que très peu de gens font. Ce que nous avons relaté précédemment permet de mettre nos renseignements dans un coffre-fort ou dans des écrits bien maquillés. Encore faut-il ne jamais oublier de fermer la porte du coffre et ne jamais louper à certains moments, de respecter le code de maquillage de nos émissions.

Et finalement, comment se protéger du cyber espionnage ? Aujourd'hui, il est possible de se protéger de la cyber surveillance sur les réseaux mais il est toujours difficile de sécuriser l'ordinateur lui-même de par les actions de son propriétaire.

Tous nos appareils nomades sont susceptibles d'être visités par des intrus si nous n'y prenons pas garde. C'est à nous de respecter les consignes de sécurité que nous enseignent les spécialistes de l'informatique embarquée.

La sécurité est un processus, ce n'est pas un produit. Il n'y a rien d'absolu. Après tout voyage à l'étranger par exemple, il est recommandé de confier nos matériels (ordinateurs, téléphones portables, tablettes, IPhone, etc.) à notre informaticien qui nous videra les mémoires sur des espaces vierges et réinstallera les sécurités utiles en vigueur là où nous nous trouvons. Nous éviterons ainsi les espions émetteurs embarqués sur nous, ramenés de l'étranger, les fauteurs de troubles ou les traçages repérables par quiconque veut savoir à tout moment où nous trouver. Ce raisonnement est valable aussi chez soi vis-à-vis de la DCRI.

En conclusion de ce dernier chapitre, soyons vigilants lors de l'utilisation de nos équipements de communications quels qu'ils soient … et protégeons de notre mieux nos écrits, tout en sachant que les fournisseurs d'accès internet ont le devoir de communiquer à la police et à la justice française tout le flux de communications qui passa par nous les douze derniers mois. Certains logiciels évitent la lisibilité des contenus. Ce ne sont pas ceux du commerce classique, encore faut-il en être équipés.

Notre vie privée n'est sauvegardée que si notre liberté chérie est assurée quitte à être plus rusé que ceux qui veulent toujours nous avoir tout nu, en ne leur permettant pas la propension au contrôle sur nous dont ils sont avides. Le tout sécuritaire est contraire à la concorde démocratique. Le tout sécuritaire est ennemi de la vie privée des citoyens. C'est un leurre qui a pourtant cours dans l'esprit de beaucoup d'humains sur la terre.

Michel CLERC

[1] Pour ceux qui veulent se protéger, aller chercher sur Google à stéganographie et aller sur les commentaires relatifs à "Chiffrement et stéganographie KORBEN".

Petit lexique de termes ou sigles

Immixtion : C'est l'action d'intervenir dans les affaires d'autrui. Synonyme : Ingérence.

Sexting : Mot non répertorié dans le dictionnaire Robert, exprimant une forme de harcèlement téléphonique, de la famille du texto pornographique qui, plus trivialement dit, consiste à envoyer à des interlocuteurs, des images numériques coquines savamment commentées.

A. S. E. **A**ide **S**ociale à l'**E**nfance. C'est un service existant dans tout département français.

Panoptique de BENTHAM : Consiste à installer un surveillant dans une tour centrale, dans un environnement industriel ou carcéral, qui voit tous les surveillés sans être vu d'eux.

C'est l'administration par contrat, à l'opposé de la gestion à la confiance.

EDVIGE : Fichier de police d'**E**xploitation **D**ocumentaire et **V**alorisation de l'**I**nformation **GE**nérale. Créé le 27 juin 2008, (fusion des RG et de la DST), (informatisé).

CNIL : **C**ommission **N**ationale de l'**I**nformatique et des **L**ibertés. C'est une autorité indépendante française, créée le 6 janvier 1978, modifiée le 6 août 2004.

STASI : Staatssicherheit. C'est le Ministère de la Sécurité d'Etat d'Allemagne de l'Est créé en 1950. La STASI avait les missions de service de police politique, de renseignements, d'espionnage et contre-espionnage sous tutelle directe du gouvernement. Elle fut démantelée en 1990. Les dossiers qu'elle a produits pendant 40 ans, non détruits, contiennent tous les noms des suspects, des agents accusateurs, comme ceux des indicateurs dont beaucoup sont encore vivants.

STIC : Fichier de police informatisé du Ministère de l'Intérieur français, regroupant les auteurs d'infractions relevées par la police nationale, créé en août 1985. Veut dire : **S**ystème de **T**raitement des **I**nfractions **C**onstatées. Il est destiné aux zones urbaines.

JUDEX : Fichier de gendarmerie informatisé. Le sigle veut dire : **S**ystème **J**udiciaire de **D**ocumentation et d'**EX**ploitation. Il est détenu par la gendarmerie nationale. Il est destiné aux zones rurales et périurbaines.

ARIANE : En 2010, il fut décidé de fusionner le fichier de police avec le fichier de gendarmerie. Le sigle veut dire : **A**pplication de **R**approchement, d'**I**dentification et d'**AN**alyse pour les **E**nquêteurs.

Ce dernier est devenu le 14 mars 2011, le TAJ qui veut dire : **T**raitement d'**A**ntécédents **J**udiciaires.

Hacker : Se dit d'un individu spécialiste de la sécurité informatique, qui aime comprendre le fonctionnement interne d'un système et particulièrement d'ordinateurs et de réseaux.