Comment contourner les systèmes de traçabilité ?

par Jean-Marc Manach,
journaliste à InternetActu.net et LeMonde.fr,
et membre des Big Brother Awards France.

version originale d'un article publié dans
Hermès n°53, 2009 : "Traçabilité et réseaux"

Résumé :

Brian Gladman est un ancien directeur des communications électroniques stratégiques du ministère de la Défense britannique et de l'OTAN. Ian Brown, un cryptographe anglais membre de l'ONG Privacy International. En l'an 2000, ils rendaient public un texte expliquant comment contourner, en toute légalité, les diverses mesures de "cybersurveillance" adoptées par les législateurs. Ces techniques s'avéreraient en effet "techniquement ineptes et inefficaces à l'encontre des criminels" et risqueraient, a contrario, de "saper le droit à la vie privée et à la sécurité des citoyens et du marché".

Leur démarche est d'autant plus salutaire que les gouvernements se contentent généralement, au mieux, d'expliquer que toute action informatique laisse des traces, et que l'on est de toute façon surveillé (mais sans jamais, étrangement, expliquer comment s'en protéger), au pire, de passer des lois sécuritaires renforçant cette cybersurveillance, contribuant d'autant à créer un climat de peur, loin du climat de confiance nécessaire à toute démocratie.

Mots clefs : internet, vie privée, sécurité, anonymat, pseudonymat, surveillance

Abstract :

How to protect ourselves ? (countermeasures, cryptology and anonymisation)

Brian Gladman has been the Director of Strategic Electronic Communications for the english Minister Of Defense for years. Ian Brown is a cryptographer and a member of the NGO Privacy International. In 2000, they published an article detailing several countermeasures in order to evade, legally, the technical measures governments adopt in order to monitor what users do on the internet. Those techniques are accused to be "technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses".

Their work is precious as governments generally explain how people can be monitored on the internet (without explaining how to protect their privacy, safety and security), and becuse the "oppressive powers introduced by their legislation" creates fear and undermines the confiance which is necessary to maintain the democracy.

Keywords : internet, privacy, security, anonymity, pseudonymity, surveillance

Introduction

En l'an 2000, Brian Gladman, ancien directeur des communications électroniques stratégiques du ministère de la Défense britannique et de l'OTAN, et Ian Brown, un cryptographe anglais membre de l'ONG Privacy International, rendaient public un texte expliquant comment contourner, en toute légalité, la RIP Bill britannique (1). Pour eux, cette loi visant à renforcer les moyens de surveillance et de contrôle des internautes s'avérait "techniquement inepte et inefficace à l'encontre des criminels" et risquait, a contrario, de "saper le droit à la vie privée et à la sécurité des citoyens et du marché".

Partant du constat que les terroristes, et autres criminels, n'ont que faire de respecter la loi, Gladman et Brown avaient ainsi détaillé un certain nombre de moyens visant à aider les citoyens à apprendre à communiquer sur l'internet en toute confidentialité. Leur démarche est d'autant plus salutaire que les gouvernements se contentent généralement, au mieux, d'expliquer que toute action informatique laisse des traces et que l'on est de toute façon surveillé, au pire, de passer des lois sécuritaires renforçant cette cybersurveillance. Etrangement, ils n'expliquent jamais comment, concrètement, protéger sa vie privée sur l'internet, contribuant d'autant à créer un climat de peur, loin du climat de confiance nécessaire à toute démocratie.

Huit ans plus tard, l'analyse de Gladman & Brown n'a rien perdu de sa pertinence. On ne compte plus les mesures sécuritaires substituant la suspicion de culpabilité à la présomption d'innocence. La France a elle aussi légiféré, dans la foulée des attentats de 2001, afin de placer sous surveillance, et "par principe", l'ensemble des internautes. Dans le même temps, de nouveaux outils et logiciels sont également apparus, qui renforcent, et facilitent, les moyens de lutter, en toute légalité, contre ce type d'atteintes à la vie privée.

Surveillance des internautes : vers la présomption de culpabilité

Le 15 septembre 2001, un article de Libération (2) avance que les terroristes auraient communiqué via l'internet en cachant leurs messages secrets dans des photos pornos, rendant impossible leur détection. La technique utilisée mêle stéganographie et cryptographie. Ces deux techniques n'ont rien de propre à l'internet. La première consiste à cacher l'existence même du message. Alfred de Musset et George Sand avaient ainsi pour masquer leurs propos licencieux dans des poèmes d'apparence romantique, et d'innombrables enfants se sont essayés à l'encre invisible.

La cryptographie, elle, consiste à transformer les caractères du message en un amas indéchiffrable, sauf à disposer de la clef de déchiffrement. Elle a servi à nombre de diplomates et espions, depuis des siècles, et a gagné en popularité depuis qu'un mathématicien américain, Phil Zimmermann, a créé Pretty Good Privacy (PGP), un logiciel de cryptographie grand public que les autorités américaines avaient cherché, en vain, au milieu des années 90, à interdire. Dans le monde entier, des internautes s'étaient en effet ligués pour soutenir PGP, car c'est le seul moyen de converser, en tout confidentialité, sur l'internet. Un e-mail y est en effet aussi peu protégé que ne l'est une carte postale.

Mais revenons-en à cette affaire de "porno-terrorisme", qui fut relayée dans nombre de journaux, radios et télévisions (3). Elle émanait d'un journaliste américain qui, dans USA Today, avançait en février 2001 (4) tenir l'information de "sources officielles". Personne ou presque ne releva alors qu'il était improbable que des fondamentalistes musulmans, qui

abhorrent la pornographie, puissent s'en servir pour communiquer, à l'exception des Echos, qui avancèrent que "D'aucuns voient dans ces informations une manipulation des autorités américaines visant à accroître le contrôle de l'information circulant sur le Net au dépend de la liberté d'expression" (5). De fait, dans les jours qui suivirent, le Congrès adopta un amendement facilitant la surveillance électronique des individus, sans mandat judiciaire, ouvrant la voie à de nombreuses lois visant explicitement à généraliser la cybersurveillance des télécommunications, et des individus.

Quelques années plus tard, on découvrit que le journaliste à l'origine de cet article avait bidonné un certain nombre de ses articles (6). Aucune preuve n'est par ailleurs parvenu à étayer le fait que les terroristes du 11 septembre aient communiqué via l'internet, et encore moins au moyen d'outils de stéganographie ou de cryptographie. Mais qu'importe, le message était passé, la stéganographie et la cryptographie avait été diabolisée, et l'opinion publique préparée à accepter de voir réprimer tout ce qui peut permettre aux terroristes de communiquer en toute confidentialité. Quitte, pour cela, à criminaliser le fait, pour tout internaute, de chercher à protéger sa vie privée.

En novembre 2001, le Parlement adoptait la Loi sur la Sécurité Quotidienne (LSQ). Rédigée bien avant les attentats, elle fut modifiée, en urgence, afin d'y ajouter un certain nombre d'articles présentés comme anti-terroristes. Ses mesures les plus liberticides furent qualifiées d'anticonstitutionnelles par plusieurs juristes. Mais le Conseil Constitutionnel n'en fut pas saisi, les parlementaires cherchant surtout rassurer l'opinion publique. Le sénateur socialiste Michel Dreyfus-Schmidt, reconnut d'ailleurs, dans un lapsus lourd de sous-entendus, que la France sortait peu ou prou de l'état de droit : « Il y a des mesures désagréables à prendre en urgence, mais j'espère que nous pourrons revenir à la légalité républicaine avant la fin 2003 » (7). Deux ans plus tard, à l'occasion du vote de la Loi pour la Sécurité Intérieure (LSI), les dispositions les plus critiquées de la LSQ furent prolongées sine die, sans qu'aucun bilan ne soit tiré de leur application, et contrairement à ce que la LSQ précisait pourtant expressément.

La vidéosurveillance a beau se généraliser et se développer, on n'en est pas encore au stade où la loi obligerait tout un chacun à accepter le port d'une caméra filmant ses activités 24h/24. De même, le placement sous surveillance électronique mobile (PSEM), ou « bracelet électronique » GPS ou GSM, est pour l'instant réservé aux seuls délinquants sexuels et violents, ainsi qu'aux personnes faisant l'objet de mesures d'adaptation de leur peine, et ils doivent être consentants. La généralisation, à l'ensemble de la population, de telles mesures serait bien évidemment indigne de notre démocratie, et, sauf à abolir les Droits de l'homme, très certainement contraire à nos principes républicains et constitutionnels.

Sur l'internet, il n'en est rien. La LSQ a érigé en principe la surveillance, a priori, de tous les internautes. Les fournisseurs d'accès à l'internet (FAI) sont en effet tenus de conserver, pendant un an, la trace de leurs activités afin de permettre aux autorités, sur requête judiciaire, de fouiller dans leur passé. Il leur est ainsi possible de savoir ce que les internautes ont fait, quand, pendant combien de temps, à qui ils ont écrit, au sujet de quoi : la liste des traces à conservées (appelés "données de connexion" ou "logs") est un véritable inventaire à la Prévert (8), et couvre à peu près tout ce que l'on peut faire sur l'internet, à l'exception du "contenu" de leurs e-mails et des fichiers consultés ou échangés -ce qui s'apparenterait à une mise sur écoutes personnalisée, ce que la loi n'est pas, puisqu'elle prévoit de surveiller tout le monde, tout le temps. Evoquant le fichage

généralisé de la population par la gendarmerie nationale, Louis-Marie Horeau, journaliste du Canard Enchaîné, évoquait ainsi, en 1981, "la recette bien connue de la chasse aux lions dans le désert : on passe tout le sable au tamis et, à la fin, il reste les lions..."

En somme, et à la manière des bracelets électroniques, il est possible de retracer le parcours des internautes, de savoir où ils sont allés, quels sites ils ont consultés, sur quels serveurs ils se sont connectés et, par triangulation, qui ils y ont rencontrés. A la manière d'une caméra de vidéosurveillance filmant, non pas des lieux comme d'ordinaire, mais les agissements des personnes nomément désignées, il est aussi possible de savoir ce qu'ils y ont fait, s'ils se sont contentés de lire, ou s'ils ont échangés ou publiés des fichiers et, partant, quels fichiers ont ainsi été partagés, avec qui. Si l'on poursuit la logique de Michel Dreyfus-Schmidt, nous ne sommes toujours pas revenu à la "légalité républicaine". Mais personne ou presque n'a réagi, ni au moment de l'adoption de la LSQ, ni lorsque ses mesures "exceptionnelles" ont été prolongées sine die avec la LSI, ni vraiment depuis. Elles renversent pourtant la présomption d'innocence en faisant de tout internaute un suspect en puissance.

La seconde mesure expressément dédiées à l'internet adoptée lors de la LSQ concerne la cryptographie, qui bénéficiait d'une longue tradition législative : jusqu'en 1999, elle était assimilée à une arme de guerre, et son utilisation par le grand public interdit (sauf à utiliser un niveau de protection suffisamment bas pour permettre aux autorités de le "casser"). Las : pour favoriser le développement du commerce électronique, le gouvernement avait été contraint de libéraliser son utilisation. La cryptographie étant le seul moyen de protéger, de façon fiable, la circulation d'information sur l'internet, la France ne pouvait décemment pas se mettre au ban du marché mondial. Au grand dam des intérêts militaires et policiers, qui voyaient d'un mauvais oeil cette légalisation d'un moyen permettant à tout un chacun de communiquer sans qu'ils puissent prendre connaissance des contenus échangés.

La LSQ décida donc que l'utilisation d'outils de cryptographie serait désormais considérée comme une "circonstance aggravante", et que ses utilisateurs seraient passibles de deux ans de prison, et 30 000 euros d'amende, s'ils refusaient de déchiffrer les messages chiffrés échangés. La LSI porta la peine à trois ans de prison, et 45 000 euros d'amende. Qu'importe le fait qu'un terroriste, qui risque la prison à vie, serait plutôt enclin à ne pas révéler le contenu de ses messages et se contenter de ces trois ans de prison.

La loi autorise également les juges à recourir aux "moyens de l'État soumis au secret de la Défense nationale" pour décrypter des informations chiffrées. Les rapports d'expertise sont donc classifiés et ne peuvent faire l'objet d'aucun recours; ce qui avait d'ailleurs été perçu, dans les milieux du renseignement français, comme un excellent moyen de pouvoir fabriquer des preuves sans possibilité, pour l'accuser, de les contester. Une mesure qui, à n'en pas douter, pourrait être dénoncée par la Cour Européenne des Droits de l'Homme, et qui, une fois de plus, s'attaque à la présomption d'innocence. Tout utilisateur d'outils de cryptographie se retrouve en effet, sinon potentiellement suspect, tout du moins placé sous une épée de Damoclès dont il ne pourrait s'extirper si les autorités, pour quelque raison que ce soit, décidaient de s'intéresser à lui. Car la charge de la preuve est désormais inversée : ce n'est plus aux forces de l'ordre d'arriver à prouver la culpabilité d'un quidam, mais à celui-ci d'amener la ou les preuves de son innocence.

On aurait pu craindre une vague de "dommages collatéraux". Il n'en est rien : ces articles

de loi ne sont quasiment pas utilisés, ou n'ont pas entraîné de jurisprudence ou d'"affaires" particulières, pour l'instant tout du moins. Restent que le risque est inscrit dans les tables de loi, et que les menaces, elles, sont multiples. Employeur soupçonneux, collègue indélicat, conjoint jaloux, parents suspicieux... de nombreuses sociétés, notamment aux USA, font commerce d'outils spécifiquement dédiés à la surveillance, sinon à l'espionnage, des internautes. Plusieurs affaires ont révélé que des policiers avaient vendus à des tiers des informations issues des fichiers accessibles aux seuls officiers de police judiciaire. Le secteur de l'intelligence économique, en plein développement, a recruté nombre d'anciens policiers ou membres des services de renseignement qui, pour certains, n'hésitent pas à utiliser des méthodes barbouzardes. Un rapport des Renseignements Généraux estime qu'une entreprise sur quatre est ou a été touchée par l'espionnage industriel (9). Et la DST, depuis des années, fait le tour des PMI-PME afin de leur expliquer qu'en temps de "guerre économique", il convient d'apprendre à se protéger des puissances étrangères et des concurrents malintentionnés. Rien ne saurait donc détourner les citoyens du droit à leur vie privée, et donc des outils et méthodes permettant de se prémunir contre tout type de cybersurveillance.

Des outils contre la cybersurveillance : les couteaux suisses de la vie privée

Les LiveCD

Il est souvent impossible, notamment en entreprise, d'installer de logiciels, au nom d'impératifs de sécurité considérant les utilisateurs comme autant de failles potentielles dans le dispositif de sécurité. En sécurité informatique, l'adage veut en effet que la principale faille de sécurité se trouve entre la chaise et le clavier. De fait, on ne compte plus le nombre de portables "perdus", volés, de virus introduits via l'ordinateur portable d'un employé qui l'avait ramené chez lui et utilisé au mépris des consignes de sécurité. On a aussi vu apparaître, ces dernières années, des logiciels espions spécialement dédiés aux clefs USB : certains, installés sur les PC, permettent de copier furtivement tout ou partie de la clef USB qui vient d'y être insérée, d'autres, a contrario, installés sur des clefs USB, copient certains des fichiers contenus dans le PC dans lequel elles ont été enfichées.

Michel Bouissou fut probablement l'un des tous premiers à proposer "la" solution permettant d'utiliser un ordinateur sans y laisser de trace, et sans risquer d'y être piégé par des logiciels espions ou installés au préalable. Cet informaticien très attaché aux droits de l'homme a créé, en 2003, la Knoppix-MIB (10), un "LiveCD" dédié à la protection de la vie privée. Un LiveCD, ou "CD bootable", est un CD-Rom que l'on insère dans son PC et qui, lorsqu'on redémarre l'ordinateur, permet d'utiliser le système d'exploitation libre GNU/ Linux qui y a été gravé. Conçu pour permettre aux néophytes de découvrir Linux sans rien avoir à installer, il connaît depuis de nombreuses déclinaisons, dont plusieurs orientées sécurité. Certains experts judiciaires s'en servent ainsi pour "autopsier" un ordinateur sans en manipuler les fichiers. En effet, si les LiveCD reposent sur les ressources matérielles des PC sur lesquels ils tournent, ils n'en touchent pas les composantes logicielles, et sont insensibles aux virus informatiques du fait qu'ils tournent sous GNU/Linux, et que l'on ne peut rien installer sur le CD une fois celui-ci gravé.

La Knoppix-MiB permet aussi de se créer un répertoire personnel persistant chiffré sur une clef USB ou encore sur l'ordinateur utilisé afin d'y stocker ses fichiers. Mieux : selon la règle de la "déniabilité plausible", il est possible à l'utilisateur de nier que s'y trouve quoi

que ce soit d'autre qu'une suite de nombres aléatoires non significatifs. Apparu depuis, AnonymOS (11) est lui aussi un LiveCD destiné, comme son nom l'indique, à protéger l'anonymat de son utilisateur, mais basé sur OpenBSD, l'un des systèmes d'exploitation les plus sécurisés qui soient. AnonymOS dispose d'un autre avantage : car si les LiveCD protègent l'utilisateur de ceux qui chercheraient à espionner l'ordinateur utilisé, ils ne le protègent pas de la cybersurveillance effectué par les FAI... sauf à utiliser TOR (voir plus bas), ce qu'AnonymOS propose par défaut.

Contourner la censure, le filtrage et la surveillance du web

C'est probablement la chose la plus facile à faire. Il existe une foultitude d'anonymiseurs permettant d'accéder aux contenus dont l'accès est filtré ou censuré pour les internautes venant de tel ou tel pays, ou de telle ou telle société (12). C'est un sport international aussi bien pratiqué par les étudiants américains dont l'accès internet est filtré que par les internautes chinois ou tunisiens dont le web est censuré. Le principe est de se connecter, de manière sécurisée (le "s" du https) à un anonymiseur et d'y entrer l'URL du site que l'on veut visiter. Le FAI saura, certes, que l'on a consulté l'anonymiseur, mais pas quels sites ont ensuite été visités.

On peut aussi utiliser TOR, un logiciel conçu par l'Electronic Frontier Foundation (13), dont il existe une extension pour le navigateur Firefox. Son principe est similaire, sauf qu'au lieu de passer par "un" anonymiseur, l'internaute passe par l'ordinateur d'un autre utilisateur de TOR, sur le modèle du peer-to-peer, rendant encore plus difficile la cybersurveillance. Concrètement, il suffit de télécharger l'extension TOR pour Firefox et de cliquer sur un petit bouton lorsque l'on veut commencer à protéger sa navigation. Seul inconvénient : la navigation peut s'en trouver quelque peu ralentie...

Sécuriser ses mails, chats et messageries instantanées

Pour se faire, on privilégiera l'utilisation d'un webmail sécurisé "étranger" au courrier électronique de son FAI "bien français". De préférence, on choisira un service qui propose la connexion par webmail sécurisé entre ses serveurs et son ordinateur (tel que hushmail.com, qui propose également de crypter les e-mails), de sorte que les données ne soient pas transmises "en clair", mais chiffrées (reconnaissable au 's' de https ://, ainsi qu'au cadenas fermé dans la barre d'état de votre navigateur) et ne puissent donc être lisibles ni interprétables dans les fichiers logs de son FAI. Plutôt que d'utiliser une messagerie instantanée propriétaire, on utilisera Pidgin, une logiciel « libre » compatible avec ICQ/AIM, Yahoo! et Windows Live Messenger, qui propose un module cryptographique permettant de chiffrer la communication. Il est aussi possible d'utiliser Skype, qui propose lui aussi le chiffrement de la conversation, mais avec un algorithme propriétaire et secret ne permettant pas de savoir jusqu'où il est fiable, ou pas.

Par défaut, on privilégiera les logiciels "libres". En matière de sécurité informatique, et à défaut d'être un informaticien hors pair, on est en effet obligé de faire confiance à l'éditeur de logiciel, et d'être assuré que ce dernier ne contient pas de porte dérobée ("backdoor", en anglais). Or, on ne peut accéder aux codes sources des logiciels propriétaires. Il n'est donc pas possible d'en vérifier l'intégrité, contrairement aux logiciels libres qui, surtout lorsqu'ils traitent de sécurité, font l'objet d'une surveillance constante de la part de la communauté. Le mieux est encore d'installer un système d'exploitation GNU/Linux, une procédure considérablement facilitée ces dernières années, et à la portée de toute

personne ayant déjà installé un logiciel et un tant soit peu familiarisé avec l'informatique.

Crypto, stégano & Co : quand les coffres-forts deviennent virtuels

GnuPG (ou GPG), dont le développement a été financé par le gouvernement allemand, supplante dorénavant PGP en matière de chiffrement des e-mails. Son principe, dit de cryptographie à clefs publiques, repose sur la création d'une paire de clef : une clef publique, que l'on rend accessible à ses correspondants (pour qu'ils puissent vous écrire), et une clef privée, protégée par un mot de passe et que l'on doit précieusement conserver à l'abri de tout regard indiscret (pour que vous puissiez déchiffrer les données cryptées qui vous sont envoyées). En d'autres termes, la clef publique est comme un coffre-fort que l'on laisse ouvert de sorte qu'un tiers puisse y mettre des données, avant que d'en claquer la porte. Seul le détenteur de la clef privée peut ouvrir ledit coffre-fort, une fois fermé.

C'est une évidence qui semble avoir échapper aux législateurs, mais il suffit de changer régulièrement de clef pour pallier, en partie, à l'obligation de déchiffrement. Il est aussi possible de donner une date d'expiration à sa clef : une fois périmée, elle ne pourra plus servir. De même, il est possible de "révoquer" sa clef, ou encore se doter de clefs à usage unique.

Autre évidence, un fichier qui n'existe plus ne peut être déchiffré. Encore faut-il l'effacer définitivement, ce qui n'est pas le cas si l'on se contente de le "jeter à la corbeille". A la manière des destructeurs de documents utilisés en entreprise, il existe des logiciels d'écrasement sécurisé des données, tels qu'Eraser ou Wipe.

La cryptographie ne permet pas, cela dit, de masquer l'existence des données chiffrées. On peut ainsi opter pour des outils de stéganographie, qui permettront de camoufler les fichiers à protéger dans d'autres fichiers plus anodins (images ou sons, par exemple). On pourra aussi créer un coffre-fort électronique afin d'y entreposer les données que l'on voudrait sécuriser, ou encore chiffrer tout ou partie d'une partition de disque dur à cette intention, ce que propose de faire, très facilement, les principales distributions GNU/Linux. Avantage de cette dernière option : elle permet, elle aussi, la "déniabilité plausible". Le chiffrement de tout ou partie d'un disque dur ne peut cela dit se concevoir que dans le cadre d'une politique globale de sécurité.

Conclusion

Bruce Schneier, l'une des personnalités les plus respectées des milieux de la sécurité informatique, n'a de cesse de le répéter : la sécurité est avant tout un processus, pas un produit. Aucune solution n'est fiable à 100% et rien ne sert, par exemple, d'installer une porte blindée si on laisse la fenêtre ouverte. Il convient d'autre part de ne jamais oublier qu'en matière informatique en générale, et sur l'internet en particulier, l'anonymat n'existe pas. Il arrive fatalement un moment où l'on se trahit, où l'on commet une erreur, ou, plus simplement, où l'on tombe sur quelqu'un de plus fort que soi. La sécurité informatique est un métier, elle ne s'improvise pas.

En attendant, on peut raisonnablement espérer garantir un pseudonymat de bon aloi, si tant est que l'on adopte une bonne "hygiène" du mot de passe (14), que l'on mette à jour ses logiciels régulièrement (et son antivirus quotidiennement) et, plus globalement, que l'on se forme aux rudiments de la sécurité informatique. Quelques éléments de bon sens

ne nuiront pas : se doter d'un fonds d'écran protégé par un mot de passe (histoire de se protéger des pauses pipi ou déjeuner), utiliser le "clavier virtuel" de son PC afin d'éviter le risque posé par les keyloggers (enregistreurs des touches tapées au clavier), effectuer des sauvegardes régulièrement (et les entreposer dans un lieu sécurisé), ne pas hésiter à se créer de multiples identités ou encore... de préférer, au courrier électronique, le courrier papier (qui, lui, n'est pas systématiquement surveillé).

Comme le rappelle l'article 1er de la LSQ : "La sécurité est un droit fondamental. Elle est une condition de l'exercice des libertés et de la réduction des inégalités." CQFD.

Notes :

1. "Ways to Defeat the Snooping Provisions in the Regulation of Investigatory Powers Bill", by Ian Brown and Brian Gladman : http://www.fipr.org/rip/RIPcountermeasures.htm. A noter que cet article est aussi adapté d'une version francisée dudit manuel, "LSQ : sortez couvert ! ou Comment passer outre la cybersurveillance et les mesures anti-crypto de la LSQ..." : http://www.bugbrother.com/archives/sortezcouvert.html

2. "Pornoterrorisme : Messages islamistes cryptés sur des sites impies", par Edouard Launet, le 15/09/2001

3. "Terrorisme : les dessous de la filière porno", par Jean Marc Manach, le 27/09/2001 : http://www.lsijolie.net/article.php3?id_article=60

4. "Terror groups hide behind Web encryption", by Jack Kelley, USA Today, le 05/02/2001

5. "L'encre sympathique à l'heure d'Internet", par Emmanuel Paquette, le 24/09/2001

6. « Ex-USA TODAY reporter faked major stories », by Blake Morrison, USA Today (3/19/2004)

7. "L'ère du soupçon", par Bb), lundi 8 juillet 2002 : http://www.lsijolie.net/article.php3?id_article=123

8. « Les opérateurs Internet et télécoms devront conserver plus de données », par Charles de Laubier, Les Echos, le 19/02/2008

9. « Espionnage économique : La France pillée », par Jean-Jacques Manceau, l'Expansion.com, le 25/10/2006

10. Knoppix-MiB : http://www.vie-privee.org/comm173 ou http://www.bouissou.net

11. AnonymOS http://kaos.to/cms/projects/releases/anonym.os-livecd.html

12. cf cette longue liste en anglais : http://www.freeproxy.ru/en/free_proxy/cgi-proxy.htm

13. Tor : Un système de connexion anonyme à Internet, http://www.torproject.org/index.html.fr

14. Hygiène du mot de passe : http://www.bugbrother.com/security.tao.ca/pswdhygn.html