# GUIDE PRATIQUE DU **BLOGGER** ET DU **CYBERDISSIDENT**

## REPORTERS SANS FRONTIÈRES

SEPTEMBRE 2005

reporters sans frontières

www.rsf.org

# GUIDE PRATIQUE DU BLOGGER ET DU CYBERDISSIDENT

## REPORTERS SANS FRONTIÈRES

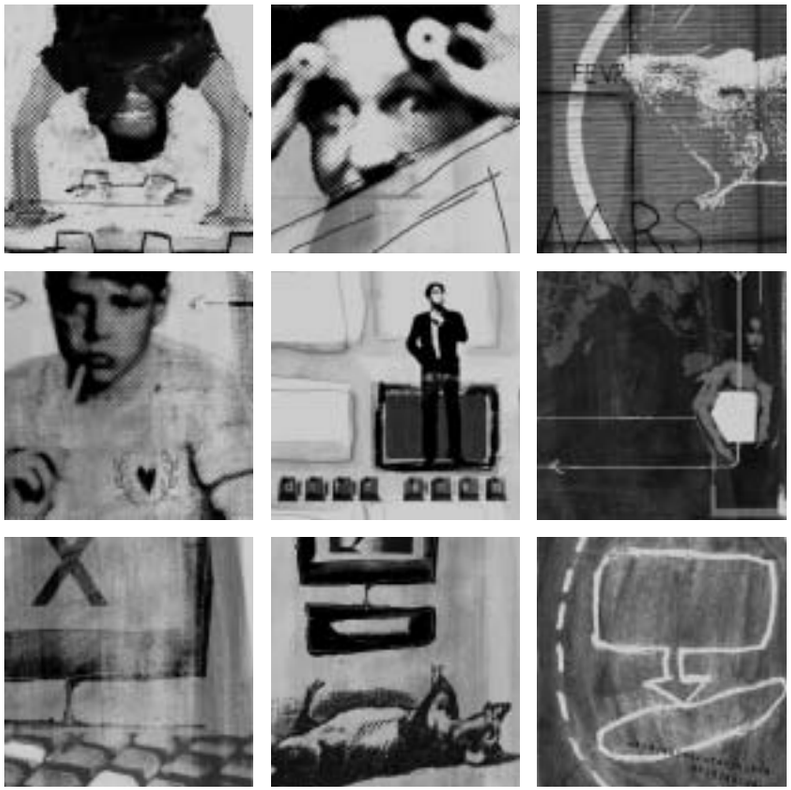
SEPTEMBRE 2005

reporters sans frontières

www.rsf.org

# GUIDE PRATIQUE **DU BLOGGER** ET DU **CYBERDISSIDENT**

# SOMMAIRE



ISBN : 2-915536-35-X




# LES BLOGGERS, **NOUVEAUX HÉRAUTS** DE LA LIBERTE D'EXPRESSION

Les blogs passionnent, inquiètent, dérangent, interpellent. Certains les méprisent, d'autres les tiennent pour les prophètes d'une nouvelle révolution de l'information. Une chose est sûre : les blogs ne laissent plus indifférent. Entre diabolisation et adoration, que penser de ce phénomène qui transforme le paysage médiatique de pays aussi différents que les Etats-Unis, la Chine ou l'Iran ?

Nous manquons encore de recul pour répondre à cette question. Nous sommes lecteurs de presse, auditeurs et téléspectateurs depuis des décennies. Sans même en être conscients, nous disposons de grilles de lecture nous permettant de faire la différence, au premier regard, entre un commentaire et une info, un journal « people » et un magazine sérieux, un programme de divertissement et un documentaire.

Nous n'avons pas de telles références pour déchiffrer les blogs. Or, ces « blocs-notes en ligne » sont encore plus hétéroclites que la presse. Difficile de faire le tri entre les publications d'information, les tribunes personnelles, les vraies enquêtes et les témoignages bidons, difficile de séparer le bon grain de l'ivraie. Il est probable que certains bloggers développent peu à peu leurs propres standards éthiques, pour renforcer leur crédibilité et gagner la confiance de leur lectorat. Mais ne nous cachons pas les yeux, les fausses informations, les insultes et les calomnies fleuriront toujours sur Internet. Le blog donne à chacun, quelles que soient sa formation ou ses compétences techniques, la possibilité de devenir éditeur. Cette liberté ne va pas sans risques et les blogs sans intérêt, voire nauséabonds, vont se développer au même rythme que les publications de qualité.

Malgré cela, reconnaissons que les blogs sont un formidable outil pour la liberté d'expression. Ils ont délié les langues des citoyens ordinaires. Ceux qui jusqu'à présent n'étaient que des consommateurs d'information sont devenus les acteurs d'une nouvelle forme de journalisme, un journalisme « à la racine » selon les termes de Dan Gillmor (Grassroots journalism – voir le chapitre Quelle éthique pour les bloggers ?), c'est-à-dire fait « par le peuple et pour le peuple ».

Dans les pays où la censure est reine, lorsque les médias traditionnels vivent à l'ombre du pouvoir, les bloggers sont souvent les seuls véritables journalistes. Ils sont les seuls à publier une information indépendante, quitte à déplaire à leur gouvernement et parfois au risque de leur liberté. Les exemples de bloggers emprisonnés ou harcelés ne manquent pas. L'un des contributeurs à ce guide, Arash Sigarchi, a été condamné à 14 ans de prison pour

quelques « posts » critiques du régime iranien. Son témoignage rappelle que certains bloggers conçoivent leur travail comme une nécessité et un devoir, pas comme un simple passe-temps. Ils ont conscience d'être la bouche et les oreilles de milliers d'autres internautes.

Lorsque produire de l'information est une activité à risques, les bloggers ont tout intérêt à préserver leur anonymat. Car les cyberpolices veillent et sont devenues maître dans l'art d'épier la Toile et débusquer les « trouble-Net ». Ce guide donne donc également quelques conseils pratiques pour publier sur Internet sans dévoiler son identité (Comment blogger de manière anonyme ?, d'Ethan Zuckerman). Bien sûr, mieux vaut disposer de compétences techniques pour protéger la confidentialité de ses activités en ligne, mais le respect de quelques règles simples est parfois suffisant pour éviter d'être repéré. Ces conseils ne sont bien entendu pas destinés à ceux qui, terroristes, mafieux ou pédophiles, utilisent le Réseau pour mener à bien des activités criminelles. Ceux-là ne les ont pas attendus. Ce guide ne vise qu'à aider les bloggers qui, au nom de la liberté d'expression, entrent en résistance par leurs seuls écrits.

Toutefois, le premier problème auquel ces derniers sont confrontés, même dans un pays répressif, n'est pas lié à leur sécurité : ils doivent d'abord faire connaître leur publication, trouver leur public. Un blog sans lecteurs a certes peu de chances de s'attirer les foudres du pouvoir, mais à quoi sert-il ? Pour répondre à cette question, ce guide propose quelques conseils techniques pour bien référencer son blog sur les moteurs de recherche (voir l'article d'Olivier Andrieu), ainsi que des recommandations plus « journalistiques » (Faire sortir son blog du lot, de Mark Glazer).

Certains bloggers doivent surmonter une dernière difficulté : le filtrage. En effet, la plupart des régimes autoritaires sont aujourd'hui dotés de moyens techniques leur permettant de censurer le Réseau. A Cuba ou au Viêt-nam, inutile de chercher sur la Toile des informations qui remettraient en question la politique du gouvernement, dévoileraient des affaires de corruption ou dénonceraient des atteintes aux droits de l'homme. Les contenus « illégaux », ou « subversifs », sont bloqués automatiquement par des systèmes de filtrage. Or, tout blogger a besoin d'accéder librement au Net pour nourrir sa publication : coupé du Réseau et sans lien avec sa communauté, un blog ne peut que péricliter. La deuxième partie de ce guide est par conséquent consacrée aux techniques permettant de déjouer les technologies de filtrage (Choisir sa technique pour contourner la censure, de Nart Villeneuve). Avec un peu de bon sens et de persévérance, et surtout en identifiant la technique la mieux adaptée à sa situation, tout blogger devrait être capable de s'affranchir de la censure.

Ce guide rassemble des conseils et des astuces techniques pour lancer son blog dans de bonnes conditions. Mais ce qui fait le succès d'un blog, au bout du compte, s'apprend difficilement. Pour émerger de la masse, ce type de publication doit avoir une voix originale, apporter un point de vue ou des informations délaissés par les médias traditionnels. Dans certains pays, la principale préoccupation des bloggers est de rester en liberté. Dans d'autres, ils cherchent à asseoir leur crédibilité et à s'imposer comme une source fiable d'information. Tous ne sont pas confrontés aux mêmes problèmes, mais tous, à leur façon, sont aujourd'hui en première ligne du combat pour la liberté d'expression.

**JULIEN PAIN**

Responsable du bureau Internet et libertés de Reporters sans frontières





# UN BLOG, C'EST QUOI ?

**UN « BLOG » (OU « WEBLOG ») EST UN SITE WEB PERSONNEL :**

- composé essentiellement d'actualités (« billets » ou « posts »)
- alimenté au fil de l'eau, sur une base régulière
- présenté sous la forme d'un journal (les billets les plus récents en haut de page). En général, les « posts » sont également regroupés par catégories
- publié à l'aide d'un outil dynamique conçu spécialement dans ce but
- le plus souvent créé et animé par un individu unique, anonyme ou non.

**LES BILLETS PUBLIÉS SUR UN BLOG :**

- sont le plus souvent composés de texte (et de liens externes), mais peuvent être enrichis d'images et, de plus en plus facilement, de son et de vidéo
- sont susceptibles d'être commentés par les lecteurs
- sont archivés sur le blog et accessibles à la même adresse sans limitation de durée.

**UN BLOG N'EST DONC PAS FONDAMENTALEMENT DIFFÉRENT D'UNE SIMPLE « PAGE PERSONNELLE », À CECI PRÈS :**

- qu'il est plus simple à créer et à mettre à jour, donc beaucoup plus dynamique et plus fréquemment actualisé
- qu'il incite à adopter un style et un point de vue plus personnel, caractérisé par une grande liberté de ton
- qu'il favorise fortement les échanges avec les visiteurs ou d'autres bloggers
- qu'il définit un format commun à tous les blogs de la planète, caractérisé par l'utilisation de procédés similaires (présentation en deux ou trois colonnes, commentaires des billets, fils RSS, etc.)

**POINTBLOG.COM**

# PETIT LEXIQUE DU BLOGGING

**AGRÉGATEUR RSS**
Logiciel ou service en ligne permettant au blogger de lire des fils RSS, en particulier les derniers billets publiés sur ses blogs favoris. On parle également de « lecteur RSS ».

**BILLET (OU « POST »)**
Entrée publiée sur un blog. Synonyme de « note » ou d'actualité, au sens large. Peut se limiter à un simple lien ou à une photo, mais se compose le plus souvent d'un texte court enrichi de liens externes. Le plus souvent, chacun des billets publiés peut être commenté par les visiteurs du blog. *Post* en anglais.

**BLOG**
Contraction de « Web Log ». Site Web caractérisé par un format qui prend la forme de textes, de liens hypertextes et/ou d'images publiés au fil de l'eau, en général par un auteur unique, à titre personnel.

**BLOGEOISIE**
Contraction de « Blog » et de « Bourgeoisie ». Terme ironique désignant « l'élite » des bloggers, c'est-à-dire les bloggers les plus connus/populaires.

**BLOGICIEL**
Logiciel permettant la publication d'un blog. *Blogware*, en anglais.

**BLOGOSPHÈRE**
L'ensemble des blogs existants, ou la communauté des bloggers.

**BLOGROLL**
Liste de liens externes inclus sur les pages d'un blog et apparaissant en général en colonne dès la page d'accueil. Souvent composé de liens vers d'autres blogs, le blogroll délimite souvent une « sous-communauté » de bloggers « amis ». Parfois traduit en français par « blogoliste ».

**BLOGUER**
Action de tenir un blog ou de publier sur un blog.

**BLOGGER**
Celui ou celle qui publie un blog.

**CARNET WEB**
Synonyme de blog.

**FIL / FLUX RSS**
Désigne le fichier contenant les derniers billets publiés sur un blog. Ce fichier, lu par un agrégateur RSS, permet d'être informé dès qu'un blog a été mis à jour. *Feed*, en anglais.

**MOBLOG**
Contraction de « Mobile Blog ». Caractérise un blog pouvant être mis à jour à distance et en restant « mobile », par exemple via un téléphone mobile ou un assistant numérique.

**PERMALIEN**
De l'anglais *Permalink*, contraction de « Permanent Link ». Adresse Web de chaque





billet publié sur un blog. Le permalien est un moyen pratique de pointer vers un billet donné, sans limitation de durée, même après qu'il a été archivé sur le blog d'origine.

**PHOTOBLOG**
Blog essentiellement composé de photographies, publiées chronologiquement et au fil de l'eau.

**PODCASTING**
Contraction de « iPod » et de *broadcasting*. Terme générique désignant la possibilité de publier via un blog et ses fils RSS du contenu audio ou vidéo, à destination d'un baladeur numérique.

**RSS**
Une méthode de description des actualités publiées sur un site Web. Particulièrement adaptée aux blogs, elle permet à un utilisateur d'être alerté dès que ses blogs favoris ont été mis à jour. La méthode sert également à « syndiquer » le contenu publié, en permettant – simplement et de façon automatisée – à d'autres sites Web de republier tout ou partie de ce contenu. En cours de généralisation, notamment sur les sites médias.

**SPAM DE COMMENTAIRES**
A l'instar du spam email, procédé qui consiste à inonder un blog de faux commentaires à caractère publicitaire, postés sans relâche par des « robots-spammeurs » (*spambots*). Un véritable fléau qui nécessite – pour le blogger ou les plates-formes de blog – de se doter d'outils permettant de bannir certains utilisateurs ou d'interdire certaines adresses dans les commentaires.

**SYNDICATION DE CONTENU**
Procédé selon lequel l'auteur ou l'éditeur d'un site rend disponible tout ou partie de son contenu, pour publication sur un autre site Web.

**TRACKBACK**
Protocole établi pour permettre à des sites Web ou des blogs de communiquer entre eux de façon automatique, en s'alertant mutuellement du fait qu'un billet sur un blog fait référence à un autre billet publié auparavant.

**WIKI**
De l'hawaïen « wikiwiki », signifiant « vite ». Site Web susceptible d'être mis à jour facilement et rapidement par n'importe quel visiteur. Par abus de langage, le terme désigne aussi bien les outils utilisés pour créer un wiki (*Wiki engines*, en anglais) que les sites wiki proprement dits. Bien qu'il existe une certaine connexité entre les deux mondes, blogs et wikis sont des outils distincts.

**POINTBLOG.COM**



# BIEN **CHOISIR** SON OUTIL

Les blogs doivent beaucoup à l'émergence d'outils de publication dynamiques, qui simplifient considérablement le processus d'alimentation en contenu de sites. Le principe d'un outil de blog est simple : proposer une interface facile d'emploi (accessible via un navigateur Web) et gérer de façon dynamique le contenu publié (archives automatiques, recherche indexée dans le contenu, etc.).

Un blog s'accompagne donc de deux adresses Web, qui ne changeront jamais après l'ouverture du blog :

- l'adresse du blog proprement dite, qui en permet l'accès public
- l'adresse de l'interface d'administration du blog, protégée par un mot de passe et accessible uniquement par le blogger.

Il existe deux possibilités pour créer un blog : rejoindre une communauté de blogs ou installer un outil de blog avec son propre hébergement.

**LES COMMUNAUTÉS DE BLOGS**

(Voir le chapitre « Présentation d'un outil de blog : Civiblog »)

Ouvrir un blog sur une communauté existante ne prend en général que quelques minutes. On choisit un identifiant, un mot de passe et en quelques clics le blog est ouvert. Selon les communautés, le service peut être gratuit ou payant.

Cette solution est à recommander si l'on souhaite ouvrir un blog « pour voir ». Elle est peu coûteuse (soit gratuite, soit quelques euros par mois), simple, rapide et permet de bénéficier d'un « effet communauté » (trafic issu de la communauté elle-même ou de sa notoriété à l'extérieur).

Elle comporte toutefois quelques inconvénients, comme des options souvent limitées (choix de l'aspect du blog, fonctions avancées...) ; des publicités gérées par la communauté ; le risque d'une fermeture de la communauté...

**LES OUTILS DE BLOG À INSTALLER**

Les outils de blog – ou « blogiciels » – sont des programmes qui s'installent sur un serveur Web. Ils utilisent des scripts pour gérer le site de façon automatisée et une base de données pour stocker l'information publiée. Une fois installé, l'outil

s'utilise via un simple navigateur Web connecté à Internet. Il n'est pas nécessaire de maîtriser les « techniques Web », notamment le langage HTML, pour créer et animer son blog, mais l'installation et le paramétrage de l'outil de blog ne sont pas toujours aisés (gestion des droits d'accès, création d'une base de données, télé-chargement FTP...).
Cette solution est donc à recommander pour celles et ceux qui savent déjà que le blog est fait pour eux ! Elle présente l'avantage d'être « chez soi », donc de pouvoir adapter, configurer, modifier le blog à sa convenance.
Elle nécessite toutefois quelques compétences techniques. Le blog est aussi plus exposé (notamment au spam de commentaires) et suppose d'effectuer soi-même la sauvegarde des contenus.

## COMMENT CHOISIR UNE COMMUNAUTÉ DE BLOGS ?

Il n'est pas toujours facile de migrer un blog existant d'une communauté vers une autre. Il est donc important d'effectuer le choix d'une communauté en connaissance de cause.

Avant de choisir une communauté de blogs, il est préférable d'étudier les points suivants :

**LES AUTRES BLOGS DE LA COMMUNAUTÉ**
Certaines communautés de blogs fédèrent des internautes de façon thématique ou générationnelle. Il est indispensable de consulter quelques dizaines de blogs d'une communauté donnée pour se faire une idée du « profil type » de ses membres, s'il y en a un.

**L'ASPECT DU BLOG**
Bien que les possibilités en matière de personnalisation soient souvent limitées, chaque plate-forme propose en général des gabarits multiples, permettant au blogger de choisir les couleurs, les polices de caractères, la structure de la page d'accueil, etc. Là aussi, on peut se faire une bonne idée des possibilités en observant des blogs pris au hasard dans la communauté. Il est bon de savoir que beaucoup de plates-formes gratuites imposent des publicités sur toutes les pages des blogs. Vérifier aussi les options quant à l'adresse finale du blog, qui pourra être http://monblog.lacommunaute.fr, http://www.lacommunaute.fr/monblog ou http://www.lacommunaute.fr/monnumero

**LES FONCTIONNALITÉS**
Il faut bien étudier les fonctionnalités offertes par le service, afin de savoir s'il sera possible de changer l'aspect du blog, d'y faire collaborer plusieurs auteurs, d'y inclure des images ou du son, d'y publier à partir d'un téléphone, d'en limiter l'accès – totalement ou partiellement – à des visiteurs dûment enregistrés, etc. Il est également utile de savoir si les données publiées sur le blog seront facilement exportables, le cas échéant, vers une autre communauté. Vérifier enfin, si cela fait partie de vos motivations, s'il est possible d'ajouter des publicités générant des revenus pour le blogger.





**LES COÛTS CACHÉS**
Certaines communautés sont gratuites, mais deviennent payantes lorsque des limites sont atteintes, en particulier en matière de taille des données stockées ou du volume de bande passante consommée. A vérifier avant de démarrer.

On dénombre dans le monde francophone une cinquantaine de communautés de blogs et de nouvelles plates-formes apparaissent régulièrement. La liste quasi exhaustive de ces communautés est accessible sur « l'annuaire des outils de blog » (http://www.pointblog.com/annu).

**QUELQUES PLATES-FORMES FRANCOPHONES :**

20six - http://www.20six.fr
Gratuite ou payante (3 ou 7 euros/mois).
Beaucoup de fonctionnalités, dont certaines avancées, y compris en version de base.

Over-Blog - http://www.over-blog.com
Gratuite.
Simple d'emploi et bien réalisée.

Skyblog - http://www.skyblog.com
Gratuite (avec publicité).
La plus grosse plate-forme de blogs francophone, plébiscitée par les adolescents, malgré des fonctionnalités parfois limitées.

Typepad - http://www.typepad.com/sitefr/
Payante, de 5 à 15 euros/mois, selon les fonctionnalités choisies.
Une solution très professionnelle, offrant des fonctionnalités étendues.
A noter qu'une version gratuite de la plate-forme est accessible via les communautés de blog mises en place par des tiers, par exemple Noos (http://www.noosblog.fr) ou Neuf Telecom (http://www.neufblog.com).

ViaBloga - http://viabloga.com
Gratuite pour les associations, 5 euros/mois sinon.
Une plate-forme dynamique et originale, offrant quelques fonctionnalités inédites.

**QUELQUES PLATES-FORMES INTERNATIONALES :**

Blogger - http://www.blogger.com
Gratuite.
Une plate-forme de blogs créée en 1999 et rachetée en 2003 par Google. La plus imposante (8 millions de blogs), simple d'emploi mais un peu limitée en termes de fonctionnalités.

**BIEN CHOISIR SON OUTIL**

LiveJournal - http://www.livejournal.com
Gratuite ou payante (environ 2$/mois).
L'une des plus anciennes plates-formes de blog, abritant 6 millions de blogs (public jeune en majorité).

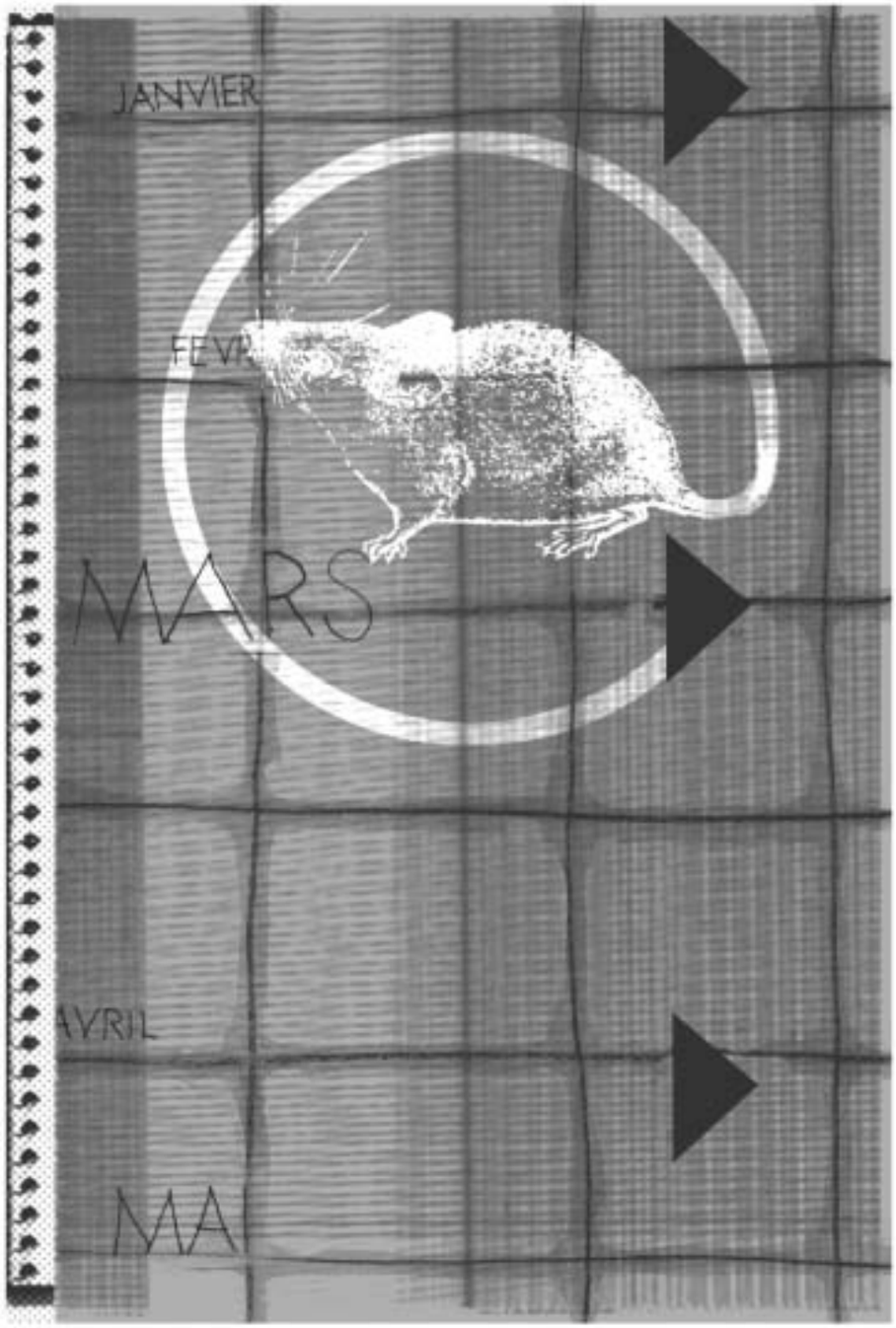
MSN Spaces - http://www.msnspaces.com
Gratuite.
Plate-forme de Microsoft, lancée fin 2004. Offre de nombreuses fonctionnalités, dont certaines au-delà du blog (partage de photos, interface avec MSN Messenger...).
A partir de 13 ans.

**En matière d'outils à installer, les principaux blogiciels à considérer sont :**

DotClear - http://www.dotclear.net
MovableType - http://www.movabletype.org
Wordpress - http://www.wordpress.org

**CYRIL FIÉVET ET MARC-OLIVIER PEYER,**
pointblog.com

pointblog.com est un blog consacré au phénomène des blogs. Destiné aux néophytes aussi bien qu'aux bloggers avancés ou aux simples observateurs, il a pour but d'éclairer sur l'importance et l'ampleur de cette évolution essentielle de l'Internet d'aujourd'hui. Il se compose d'un blog et de plusieurs rubriques indépendantes. Il est édité par la société Pointblog SARL cofondée et dirigée par Christophe Ginisty et Cyril Fiévet.






# COMMENT **CRÉER ET METTRE À JOUR** SON BLOG

Présentation du système Civiblog (www.civiblog.org)

Un blog est beaucoup plus facile à mettre à jour qu'un site Web classique. Les plates-formes de blog proposent des méthodes de mise en ligne légèrement différentes, mais les principes de base restent les mêmes. Cet article a été conçu pour aider les utilisateurs de Civiblog, un service de blog destiné aux membres de la société civile, mais les explications fournies dans ce document sont valables quelle que soit la plate-forme utilisée. Civiblog utilise une plateforme « Blogware » que la société Tucows Inc a mise gratuitement à notre disposition.

Avant de rentrer dans les détails sur la façon de poster ou de mettre en ligne des photos, il faut rappeler quelques principes de base qui ont fait le succès du blogging.

L'élément technologique qui permet à la « blogosphère » de fonctionner est la syndication des contenus – RSS (really simple syndication). Un contenu RSS est un fichier XML (eXtensible Markup Language), qui est automatiquement généré par un blog et qui peut être utilisé par un autre site ou weblog. Lorsqu'on « syndique » le flux RSS d'un blog, tous les titres des « posts » publiés sur ce blog apparaissent automatiquement dans votre lecteur de news (les logiciels de mail comme Outlook ou Thunderbird proposent ce service) ou directement sur votre site ou blog personnel. Lorsqu'un blog est mis à jour, le flux RSS l'est également, ce qui permet de diffuser l'information rapidement et automatiquement. Pour devenir blogger, il faut, entre autres, apprendre à connaître cette technologie et à l'utiliser de façon à faire circuler au mieux les informations.

L'autre élément technologique sur lequel se fonde la communauté des bloggers est le « trackback ». Ce système, disponible sur la plupart des plates-formes, permet d'identifier l'origine des informations publiées sur les blogs.
Lorsqu'on publie une info qui est inspirée ou extraite d'un autre blog, on peut y ajouter un « trackback ». Le « trackback » envoie automatiquement une notification au site auquel on fait référence, ce qui permet à celui-ci de lister tous les sites qui reprennent ou commentent ses « posts ». Cela semble un peu compliqué, mais c'est en fait très simple et gratifiant, car il est toujours agréable de savoir que quelqu'un mentionne un de ses textes. C'est également très utile pour faire circuler l'information et générer des discussions croisées entre plusieurs blogs.

Lorsqu'on crée son propre blog, il faut donc prendre un peu de temps pour se familiariser avec ces technologies.

## PAGE D'ACCUEIL DE CIVIBLOG

A noter : le flux RSS de Civiblog figure à droite. Cet espace est mis à jour automatiquement, chaque fois qu'un membre de la communauté publie un nouveau message.

## PAGE D'ENREGISTREMENT

Pour mettre en place un blog, il faut commencer par s'enregistrer. La plupart des services de blog proposent un système d'inscription très simple. Civiblog requiert un minimum d'informations lors de l'enregistrement. Nous devons toutefois vérifier que les blogs que nous hébergeons sont bien des « acteurs » de la société civile - nous n'acceptons pas, par exemple, les blogs « perso » destinés à la famille ou uniquement à un cercle d'amis. Il faut environ 24 heures après l'inscription pour que le blog apparaisse en ligne. L'internaute reçoit par e-mail les codes d'accès qui lui permettront de démarrer son blog.





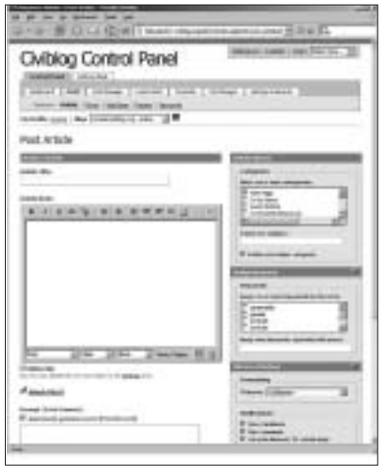
## CONNEXION AU SYSTÈME D'ADMINISTRATION

Le blog a une « face publique » qui est la page sur laquelle les visiteurs se rendent, et une « face privée » qu'on utilise pour sa mise à jour et son administration. On accède à la face privée en allant sur une page où l'on rentre le login et le mot de passe qu'on a reçus lors de la création du compte.

## TABLEAU DE BORD


La plupart des blogs ont un « tableau de bord », c'est-à-dire un endroit où l'on peut se rendre compte en un clin d'œil de ce tout ce qui se passe sur le blog. On y trouve les messages, les commentaires et les « trackbacks » les plus récents. A partir de ce tableau de bord, on accède à toutes les fonctions : on peut changer la mise en page, accroître sa bande passante, modifier les anciens messages, et gérer les utilisateurs et leurs autorisations – comme le droit de publier des commentaires.

## COMMENT POSTER UN MESSAGE




Une des différences majeures entre un blog et une page Web est la facilité avec laquelle on peut le mettre à jour. La plupart des outils permettent de taper les « posts » dans un éditeur de texte sans se préoccuper de la mise en page Web. Les outils récents, comme Civiblog, permettent de modifier les polices des caractères, les tailles, les couleurs, et d'insérer des liens et des images.

La procédure à suivre pour poster est très simple :

1. S'enregistrer
2. Cliquer sur le lien « Post »
3. Donner un titre à son article et taper le contenu dans le corps de l'article
4. Formater le texte en utilisant l'interface

5. Assigner au texte une catégorie (les catégories permettent de regrouper les messages qui ont des thèmes similaires) ou créer une nouvelle catégorie
6. Cliquer sur « Save » en bas de la page.

Et c'est tout. Avec l'expérience, on peut commencer à utiliser d'autres caractéristiques comme les « trackbacks », les « pings » et les mots clefs.


**LES « TRACKBACKS »**

Il est facile d'ajouter un « trackback » à son message. On a juste besoin de l'URL permanente du « post » auquel on fait référence. Il suffit d'ajouter cette URL dans la barre de droite, dans un espace nommé « trackback, URL to notify » et le « trackback » sera automatiquement envoyé, quand le message sera enregistré, au site auquel on fait référence.

**SYNDICATION RSS**

Syndiquer l'alimentation RSS d'un autre site ou blog est également très simple :

1. Se connecter à la face privée du blog
2. Cliquer sur « Favourites »
3. Cliquer sur le lien « RSS Headline Components »
4. Suivre les instructions sur la page et insérer l'URL du flux RSS que l'on souhaite syndiquer – cette URL se termine habituellement par .xml ou .rdf (parfois par .py ou .php)
5. Attribuer un titre au flux et cliquer sur « add feed »
6. Maintenant que le flux est créé, il faut l'insérer à la mise en page du blog
7. Cliquer sur « Look and Feel »
8. Cliquer sur « Layout »
9. Cliquer sur « RSS : Your feed » (où « your feed » est le titre donné à l'étape 5) et faire coulisser le flux vers la colonne où l'on veut le voir apparaître
10. Cliquer sur « Save » en bas de la page et c'est fini.





Il existe de nombreux sites qui expliquent les subtilités du blogging.
En voici quelques-uns :

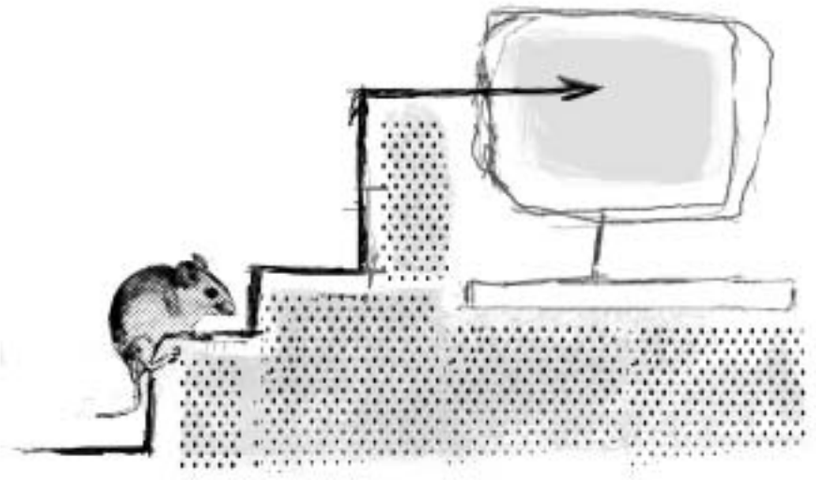
Civiblog Central Resources Blog :
http://central.civiblog.org/blog/BloggingResources

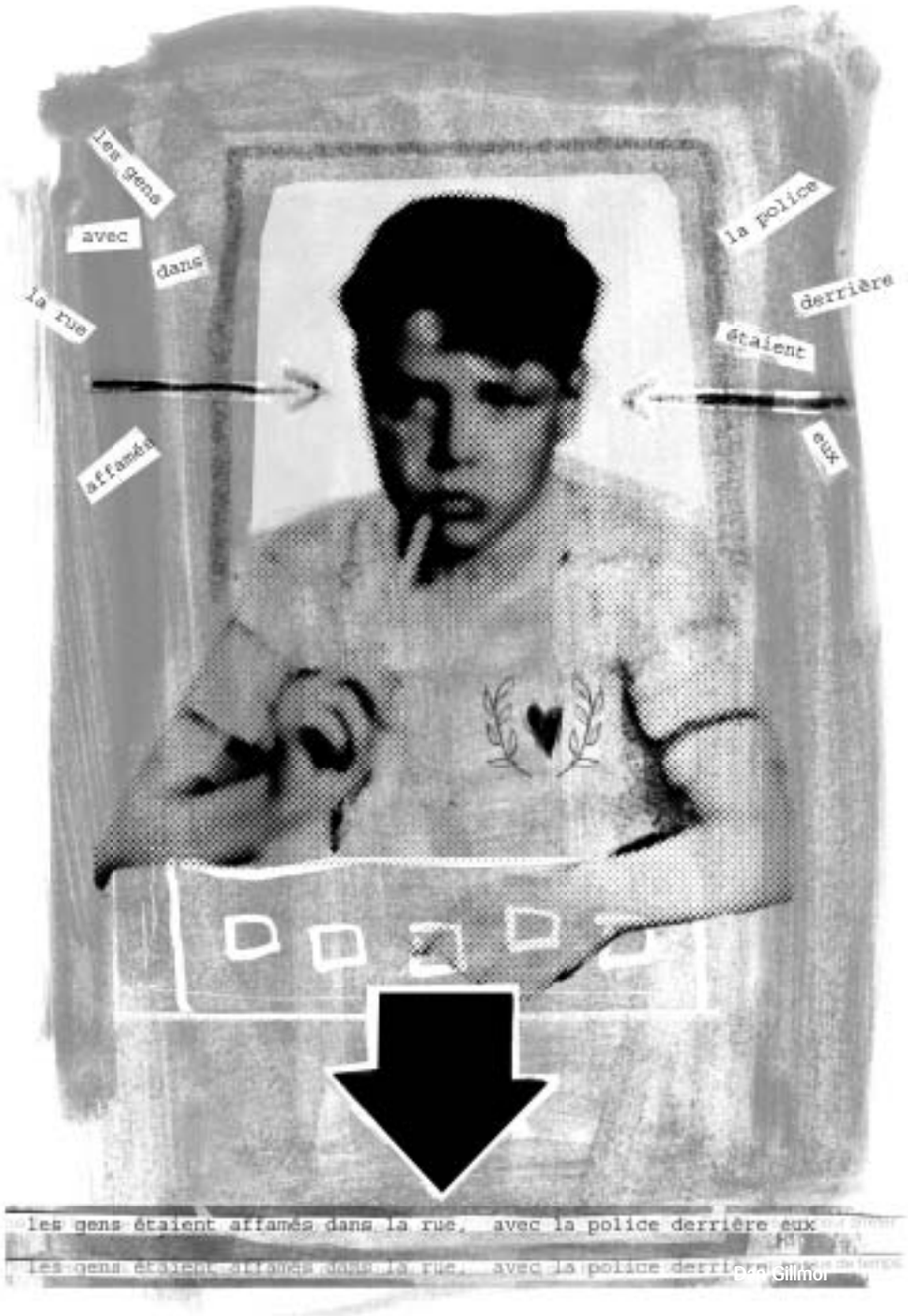
Comment blogger :
http://blogging.typepad.com/how_to_blog/

La blogsphère :
http://blog.lib.umn.edu/blogosphere/

L'atelier du blog :
http://cyber.law.harvard.edu:8080/globalvoices/wiki/index.php/WeblogWorkshop

Blogging 101 :
http://www.unc.edu/%7Ezuiker/blogging101/index.html






# QUELLE ÉTHIQUE POUR LES BLOGGERS ?

Tous les bloggers ne font pas du journalisme. La plupart n'en font pas. Mais lorsqu'ils en font, ils devraient s'astreindre à respecter quelques principes éthiques. Cela ne signifie pas qu'ils doivent s'engager à suivre une sorte de code éthique.

Le journalisme professionnel croule sous les codes éthiques. Certains, plus longs que la Constitution des Etats-Unis, essaient d'envisager tous les problèmes possibles. D'autres, courts et succincts, proposent des conseils concrets plus utiles. Le site *Cyberjournalist* a adapté pour les bloggers le code éthique de la branche américaine de la Society of Professional Journalists (http://www.cyberjournalist.net/news/000215.php). Il faut reconnaître que cette initiative est intéressante et méritante.

Tous les codes éthiques sont créés pour remplir une fonction essentielle : donner confiance. Si un lecteur (ou un spectateur, ou un auditeur) ne peut avoir confiance dans un article ou un « post », il ne prendra pas la peine d'y consacrer du temps. Sauf si, bien sûr, on sait que le contenu ne respecte aucun principe éthique : dans ce cas-là, la lecture a presque un but éducatif (on apprend beaucoup des gens qui n'ont pas de déontologie…).

En ce qui me concerne, je considère que l'éthique est quelque chose de simple : c'est une question d'honneur. Ce concept est certes très large. Mais on ne peut pas s'attendre à ce que les gens nous fassent confiance si on n'agit pas avec honneur.

Aux Etats-Unis, on associe souvent la confiance à « l'objectivité » : un article doit être nuancé et équilibré pour permettre au lecteur de se forger sa propre idée. Je crois malheureusement que l'objectivité est un objectif louable, mais inaccessible : on teinte toujours nos écrits d'un certain parti pris.

Dans ce monde du « nouveau journalisme », où la simple écriture fait place au dialogue, le journalisme éthique dépend moins d'un code de déontologie que des valeurs et des principes d'un journalisme « honorable ».

Ce type de journalisme s'appuie sur cinq piliers : la minutie, l'exactitude, l'impartialité, la transparence et l'indépendance.La ligne qui sépare ces cinq concepts n'est pas toujours

très claire. Les interprétations sont nombreuses, tout comme les nuances. Mais je pense qu'ils sont utiles pour cerner ce qu'est un journalisme éthique, et plus faciles à mettre en pratique sur Internet que dans la presse traditionnelle. Examinons-les de plus près.

**LA MINUTIE**

Lorsque j'étais reporter, et plus tard journaliste de presse écrite, mon principal objectif était d'apprendre autant que je le pouvais. Après tout, le B.A.BA du journalisme, c'est de rassembler des faits et des opinions. Il me semblait que j'avais accompli ma mission lorsque mon article terminé, je n'avais utilisé que 5 % de ce que j'avais appris. Les meilleurs reporters que j'ai rencontrés veulent toujours passer un dernier coup de téléphone, vérifier une dernière source (La dernière question que je pose dans tous les entretiens que je mène est : « Qui d'autre peut me renseigner à ce sujet ? »).

Etre minutieux, c'est ne pas s'arrêter à l'interview de nos quelques contacts habituels, qu'ils soient réels ou virtuels. Cela implique, autant que possible, de demander à nos lecteurs d'apporter leur contribution à notre travail. C'est ce que j'ai fait lorsque j'ai écrit un livre sur le journalisme « à la racine » (grassroots journalism), en 2004, et comme d'autres auteurs l'ont fait par la suite. A cause de la compétition qui existe entre les journalistes, ce type de pratique est encore très rare, mais je suis sûr qu'elle va se développer.

**L'EXACTITUDE**

Se baser sur les faits.

Dire ce que l'on ne sait pas, et pas seulement ce que l'on sait. (Si le lecteur/spectateur/auditeur sait ce que vous ne savez pas, vous l'invitez ainsi à vous tenir informé.)

L'exactitude implique qu'il faut corriger ce qui est faux, et le corriger rapidement. C'est beaucoup plus facile en ligne car on peut atténuer, ou au moins limiter, les effets de nos erreurs.

**L'IMPARTIALITÉ**

En pratique, celle-ci est aussi compliquée que l'exactitude est facile. L'impartialité est une question de point de vue. Pourtant, même ici, je pense que quelques principes peuvent s'appliquer de façon universelle.

L'impartialité, cela veut dire, entre autres, écouter différentes opinions et les intégrer dans son travail de journaliste. Cela ne veut pas dire aller colporter des mensonges pour arriver à un faux équilibre - certains journalistes aiment compiler les arguments contradictoires, même s'ils ont la preuve qu'un seul des points de vue est le vrai.

L'impartialité, c'est aussi permettre aux gens de répondre lorsqu'ils pensent que vous avez tort, même si vous n'êtes pas d'accord. Une fois de plus, cela est beaucoup plus facile en ligne que dans les autres médias.

En fin de compte, l'impartialité découle plus d'un état d'esprit. Nous devrions être conscients de ce qui nous pousse à faire les choses, et nous devrions écouter les gens qui ne sont pas d'accord avec nous. La première règle quand on cherche à dialoguer est de savoir écouter, et pour ma part, j'apprends davantage avec les gens qui pensent que j'ai tort qu'avec ceux qui pensent que j'ai raison.





**LA TRANSPARENCE**

La transparence est de plus en plus répandue dans le journalisme. Bien sûr, c'est plus facile à dire qu'à faire.

Personne ne peut nier que les journalistes se doivent de révéler certaines choses, comme des conflits d'intérêts financiers. Mais jusqu'à quel point ? Tous les journalistes sont supposés exposer leur vie à livre ouvert ? Dans quelle mesure doivent-ils être transparents ? Les partis pris, mêmes inconscients, affectent également le journalisme. Je suis américain, j'ai été élevé dans certaines croyances, que de nombreuses personnes dans d'autres pays, et même dans mon propre pays, rejettent complètement. Je dois être conscient de ces choses que je prends pour argent comptant, et je dois les remettre en question de temps en temps au cours de mon travail.

La transparence tient aussi à la manière dont on présente une histoire. Nous devons créer des liens vers nos sources et appuyer nos affirmations par des faits et des données concrètes. (Peut-être que cela fait aussi partie de l'exactitude ou de la minutie, mais cela me semble mieux ici.)

**L'INDÉPENDANCE**

Le journalisme d' « honneur » demande que l'on suive l'histoire où qu'elle nous mène. Lorsque l'ensemble des médias est détenu par quelques grosses compagnies, ou qu'ils sont sous le joug du gouvernement, cela n'est pas possible.

C'est facile d'être indépendant en ligne : il suffit de faire un blog. Mais il ne faut pas croire qu'une personne qui essaie de vivre du blogging pourra s'extraire des pressions du business et des gouvernements.

Jeff Jarvis, un blogger américain renommé (buzzmachine.com), a bien traité cette question. Il explique par exemple que les bloggers doivent chérir le dialogue. Il insiste sur un point que je considère comme la base de ce nouveau monde : la conversation mène à la compréhension. Or, lors d'une conversation, la première règle est d'écouter. L'éthique est affaire d'écoute, parce que c'est notre façon d'apprendre.

**DAN GILLMOR**

Dan Gillmor est le fondateur de Grassroot Media Inc., une entreprise qui vise à faciliter et promouvoir le journalisme « à la racine » (grassroot journalism). Il est l'auteur de « Nous, les médias : le journalisme 'à la racine' par le peuple et pour le peuple » (O'Reilly Media, 2004).

Son blog :
http://bayosphere.com/blog/dangillmor

# BIEN RÉFÉRENCER SON BLOG SUR LES MOTEURS DE RECHERCHE

Les blogs étant des sites web à part entière, il est logique que l'on se pose à court terme la question de leur référencement sur les moteurs de recherche comme Google, Yahoo! Search ou MSN Search. En effet, un blog doit pouvoir obtenir une bonne visibilité sur ces moteurs pour les mots clés importants se rapportant à son contenu. Etre bien positionné dans les pages de résultats des moteurs est l'une des facettes essentielles de cette visibilité. Encore faut-il que le site ait été conçu, au départ, pour être réactif aux critères de pertinence des algorithmes de classement utilisés par ces outils.

Par chance, les weblogs (ou blogs) ont plusieurs caractéristiques, de par leur nature même, qui font qu'ils sont souvent « bien aimés » de ces moteurs et qu'ils sont bien indexés et bien positionnés dans leurs pages de résultats. En effet :

• Les weblogs étant – au départ tout du moins – des carnets de bord ou des journaux personnels, ils contiennent très souvent beaucoup de texte. Cela tombe bien, les moteurs adorent le contenu textuel. Google et ses acolytes n'apprécient que modérément les sites trop graphiques (ou proposant beaucoup d'animations au format Flash, par exemple) et comportant peu de texte.

• Chaque article (ou « post ») fait la plupart du temps l'objet d'une page spécifique, accessible par le biais d'un « lien permanent » (ou « permalink »), ne parlant que d'un sujet précis, bien mieux prise en compte par les moteurs que de longues pages parlant de nombreuses thématiques différentes (comme les archives ou la page d'accueil du blog, par exemple). Ces « pages uniques » pour chaque « post », traitant d'un sujet à la fois, seront pain béni pour les moteurs.

• Le titre du « post » est le plus souvent repris dans le titre de la page et dans son url (adresse). Exemple : pour le blog « Radio Free Nepal », qui est disponible à l'adresse http://freenepal.blogspot.com/, chaque « post » est disponible sur une page spécifique comme celle-ci (http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html) :






Le titre du « post » (« State Vandalism in Nepal ») est non seulement repris dans l'url de la page, mais également dans le titre du document sous cette forme :


Ainsi, le titre du « post » (« State Vandalism in Nepal ») a été ajouté à la suite du nom du blog (« Radio Free Nepal ») qui pour sa part apparaît seul sur la page d'accueil (http://free-nepal.blogspot.com/).

Or, la présence de mots clés descriptifs dans le titre des pages (contenu de la balise <TITLE> pour ceux qui connaissent le langage HTML) et dans l'url de ces mêmes documents sont des critères importants pour les moteurs de recherche. Nous verrons dans la suite de cet article qu'il est primordial de bien choisir les titres de ses « posts » pour obtenir une meilleure visibilité sur les moteurs !


• Les liens sont créés automatiquement, notamment pour les archives, et sont textuels. Exemples (sur la droite des pages du blog « Free Nepal ») ci-contre :
Là encore, c'est excellent pour le référencement puisque le contenu textuel des liens (que l'on appelle couramment « ancre » ou « texte offshore des liens ») est important pour la pertinence des pages vers lesquelles pointent ces liens dans les moteurs de recherche. Ainsi, dans l'exemple ci-contre, la présence du texte « State Vandalism in Nepal » dans le premier lien ou « Radio Free Nepal » dans le 9e va renforcer la pertinence de la page pointée par ce lien pour ces termes. Mieux, pour ces expressions, le bénéfice est double puisque à la fois la page qui contient ces liens

(le texte cliquable est considéré comme une « mise en exergue » par les moteurs) ET la page pointée par eux seront considérées comme pertinentes.

## COMMENT AMÉLIORER LE RÉFÉRENCEMENT D'UN BLOG ?

On le voit, les blogs rassemblent, de par leur nature même, de nombreux avantages pour un bon référencement. Logiquement, sans rien faire, une fois en tout cas que le moteur aura « trouvé » le blog, soit par soumission manuelle, soit par le suivi de liens de la part des « spiders » des moteurs, un blog aura certainement plus de chances qu'un site « classique » d'être bien positionné car il propose déjà une certaine « optimisation naturelle ». Mais ce n'est pas une raison pour ne pas essayer d'améliorer cette visibilité en allant un petit peu plus loin.

Voici, pour ce faire, quelques conseils à suivre pour obtenir un meilleur référencement de votre weblog d'après les mots clés importants du thème traité dans votre site :

### 1. Privilégiez les technologies favorisant votre référencement

Si votre site n'est pas encore en ligne, faites attention au choix de la technologie utilisée (Blogger, Dotclear, BlogSpirit, Joueb ou bien d'autres) pour créer votre blog. Optez pour l'outil qui prend en compte le plus de spécificités en regard de votre référencement :
• Le titre du « post » doit être repris en intégralité dans le titre de la page (balise <TITLE>) ainsi que dans son url (ce qui n'est pas toujours le cas, certains outils « coupant » dans l'adresse le titre du « post » au bout d'un certain nombre de caractères).
• La création de « permalinks » (lien vers une page proposant le contenu d'un seul « post ») doit être possible.
• La technologie adoptée doit vous permettre d'aller le plus loin possible dans la mise en pages et la personnalisation de votre site : utilisation de votre propre charte graphique, de vos feuilles de style personnelles, etc. Globalement, vous devez pouvoir maîtriser le plus de points techniques possible afin d'avoir « la main » sur le plus grand nombre de facteurs favorisant votre référencement.
Pour vérifier tous ces points, allez sur des sites utilisant la technologie envisagée (vous en trouverez toujours un échantillon plus ou moins important sur les sites des prestataires en question) et regardez la façon dont ils sont affichés. Vous y apprendrez certainement pas mal de choses.

### 2. Choisissez au mieux les titres de vos « posts »

Ce point est très important : le titre de votre « post » sera repris dans le titre des pages uniques affichant vos « posts », dans leur url ainsi que dans le texte des liens qui y mènent, bref, dans trois zones parmi les plus importantes actuellement pour les moteurs de recherche. Vos titres de « post » doivent donc contenir, en quelques mots, les termes les plus importants permettant de les trouver sur le Web. Evitez des titres comme « Bravo », « Bienvenue », « C'était super », etc. Idéalement, le titre du « post » doit décrire et résumer,





en moins de cinq mots, ce que l'on va trouver dans le texte correspondant, qui se trouve en dessous. Imaginez avec quels mots vous voudriez que l'on trouve votre « post » sur les moteurs... Et insérez-les dans le titre ! Pas si simple... Mais diablement efficace !

### 3. Fournissez du texte

Les moteurs de recherche aiment le texte : il faut donc leur en donner... Vous pouvez, cependant, afficher toutes les photos que vous désirez, à partir du moment où elles sont accompagnées de texte. Idéalement, ne restez jamais en dessous de la barre des 200 mots pour chaque « post », afin qu'il soit bien pris en compte par les moteurs. Evitez également de traiter plusieurs points très différents dans un même « post ». Les moteurs n'aiment pas les contenus multi-thèmes... Ayez toujours en tête l'équation 1 thème = 1 « post » !

### 4. Soignez le premier paragraphe de vos « posts »

La localisation des mots importants à l'intérieur du texte est également primordiale. Soignez tout particulièrement le premier paragraphe de votre « post ». Si vous désirez être trouvé d'après les mots « liberation otages », placez-les dans les 50 premiers termes de votre « post ». Il en sera de même pour tous les mots clés que vous estimez importants pour la page en question. Une page qui contient les termes de recherche en début de contenu est toujours mieux classée qu'une autre page contenant ces termes à la fin (toutes choses étant égales par ailleurs...). N'hésitez pas également à mettre en exergue ces mots, par exemple en gras. Toute mise en exergue indique aux moteurs que les mots ainsi désignés sont importants.

### 5. Evitez le trop plein de contenus identiques sur chaque « post »

Tous les moteurs ont mis en place des systèmes de détection de « duplicate content ». En d'autres termes, si le contenu de deux pages est trop proche, seule l'une d'entre elles sera gardée, l'autre étant mise en réserve et peu souvent affichée dans les résultats. Un message de ce type est alors affiché (ici par Google) :

Il s'agit d'un phénomène que l'on rencontre souvent dans les blogs, les pages présentant chaque « post » pouvant paraître très proches les unes des autres.

Par exemple, si vous avez un texte de présentation identique sur toutes les pages, affichez-le plutôt en bas de page ou ne l'affichez que sur la page d'accueil, bref, faites en sorte que le contenu de toutes vos pages soit fortement différent d'un document à l'autre.

### 6. Ne proposez pas un titre trop long pour votre blog

En règle générale, on a coutume de dire qu'un titre (contenu de la balise <TITLE>) optimisé pour les moteurs de recherche doit contenir entre 5 et 10 mots, en dehors des « mots

vides » (ou « stop words » comme le, la, les, et, vos, etc.). Le plus souvent, le titre d'une page sur un blog est représenté par deux zones :
• Le titre général du blog.
• La reprise du titre du « post ».
Pour ne pas dépasser le nombre de 10 mots dans le titre général des pages présentant chaque « post », il vous faudra donc diviser ce nombre par deux : pas plus de 5 mots descriptifs pour le titre général du blog et pas plus de 5 mots pour le titre de vos « posts ». Certes, c'est peu... Mais savoir être concis tout en restant précis est l'un des secrets du référencement.
Enfin, si vous en avez la possibilité (toutes les technologies ne le proposent pas), affichez en premier le titre du « post » suivi du titre général du blog plutôt que l'inverse.

**7. Syndiquez votre site**

La plupart des technologies de création de blog vous donnent la possibilité de créer un « fil XML » ou « fil RSS » permettant aux internautes de récupérer vos « posts » dans un logiciel adéquat. N'hésitez pas à proposer cette possibilité (elle se met en place en quelques minutes seulement) sur votre site. Non seulement vous gagnerez du trafic supplémentaire, mais en plus, sur le moteur Yahoo!, cette fonctionnalité sera affichée en exergue comme ceci :

Pourquoi s'en priver ?

**8. Soignez votre réseau de liens**

Les liens sont très importants pour les moteurs de recherche car ils leur permettent d'établir un « indice de popularité » (appelé « PageRank » chez Google) des pages web. N'hésitez pas à développer les liens vers votre blog :
• En l'inscrivant dans des annuaires (voir ci-après).
• En recherchant des « sites cousins » non concurrents mais proposant de l'information dans la même thématique. Des échanges de liens entre divers blogs d'un même domaine sont donc à rechercher au plus vite (ils sont assez fréquents et bien vus dans la communauté des bloggers, c'est encore là un avantage de ce type de site). De plus, les blogs s'y prêtent bien, de la place dans la marge étant souvent libre pour les afficher.

## LE RÉFÉRENCEMENT DANS LES ANNUAIRES THÉMATIQUES

Si le référencement dans les moteurs de recherche (Google, MSN, Yahoo!, Exalead...) et les annuaires (Yahoo! Directory, Guide de Voila, Open Directory) généralistes est important





et primordial, un référencement plus thématique n'est pas à négliger. Il a en effet plusieurs intérêts :
• Il génère du trafic très qualifié.
• Il multiplie les liens vers votre site, ce qui est toujours bon pour votre popularité.
• Il permet de vous faire connaître auprès d'autres éditeurs de blogs qui désireraient échanger des liens avec d'autres sites similaires au leur.

Il existe en effet de nombreux outils de recherche (moteurs, annuaires) recensant les blogs de la planète web. En voici une première liste, qui est loin d'être exhaustive :

| | | |
|---|---|---|
| **Outils anglophones** | Blogwise : | http://www.blogwise.com/ |
| | Daypop : | http://www.daypop.com/ |
| | Feedster : | http://www.feedster.com/ |
| | Technorati : | http://www.technorati.com/ |
| | Waypath : | http://www.waypath.com/ |
| | Blogarama : | http://www.blogarama.com/ |
| | Syndic8 : | http://www.syndic8.com/ |
| **Outils francophones** | Blogonautes | http://www.blogonautes.com/ |
| | Blogolist | http://www.blogolist.com/ |
| | Weblogues | http://www.weblogues.com/ |
| | Blogarea | http://www.blogarea.net/Links/ |
| | Pointblog | http://www.pointblog.com/ |
| | Les Pages Joueb | http://pages.joueb.com/ |

Une liste plus complète peut être trouvée ici :
http://moteurs.blogs.com/mon_weblog/2005/05/les_moteurs_de_.html

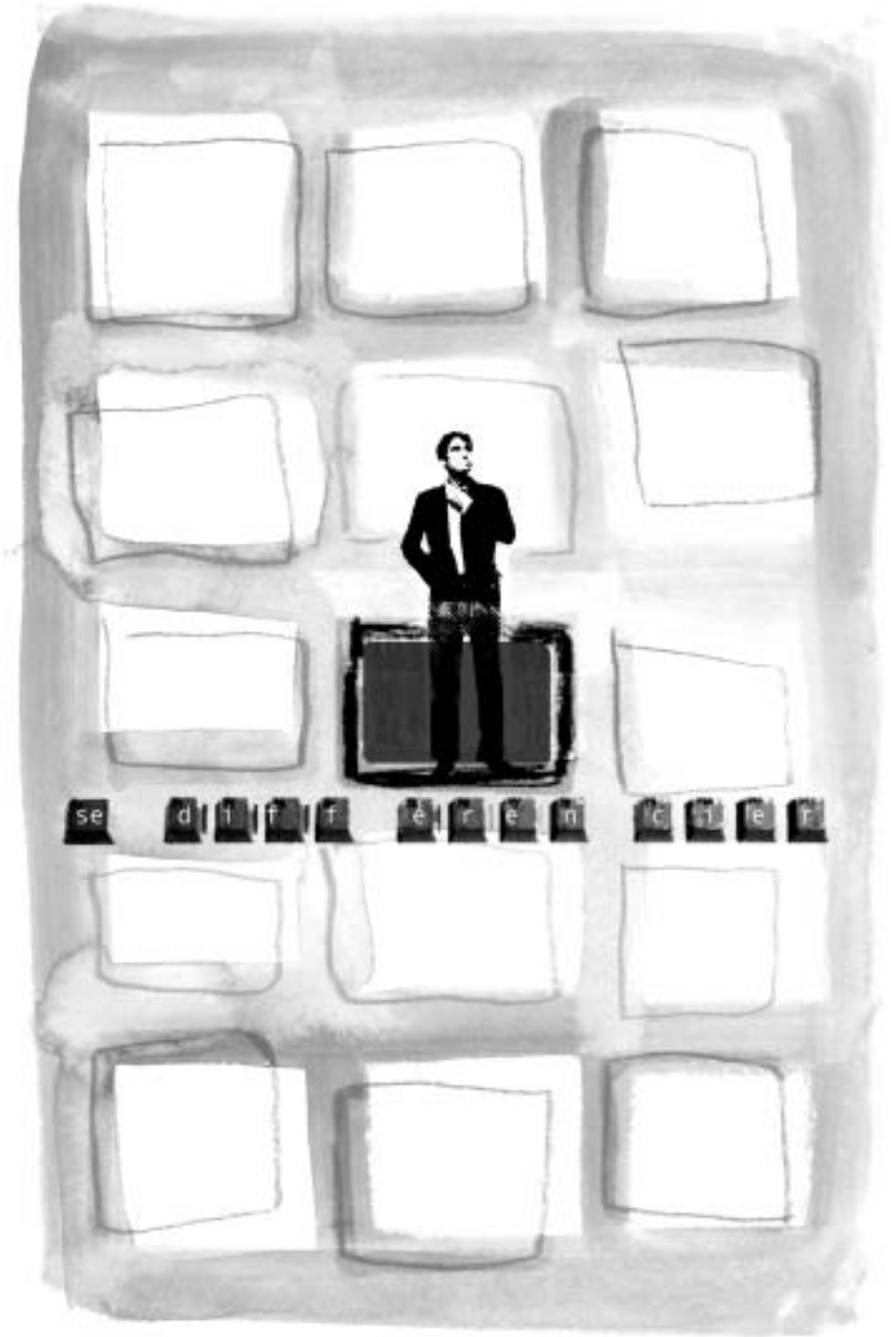
A explorer également, les annuaires de chaque prestataire de technologies, comme :
http://www.canalblog.com/cf/browseBlogs.cfm
http://www.dotclear.net/users.html
http://www.blogspirit.com/fr/communautes_blogspirit.html
Etc.

## CONCLUSION

On l'a vu, par essence, un weblog a toutes les qualités pour être bien référencé sur les moteurs de recherche. En appliquant bien les quelques conseils divulgués dans cet article, vous devriez arriver à des résultats très intéressants et multiplier ainsi votre visibilité ! A vous de jouer maintenant... A vos « posts » et n'oubliez pas... Content is King !

**OLIVIER ANDRIEU**

Olivier Andrieu est consultant indépendant dans le domaine d'Internet et spécialiste du référencement sur les moteurs de recherche. Il est également l'éditeur du site www.abondance.com.




# FAIRE
# SORTIR SON BLOG DU LOT

Parmi les milliards de mots inscrits dans les millions de blogs publiés de par le monde, qu'est-ce qui fait ressortir l'un d'entre eux de la masse ? Qu'est-ce qui peut mettre un blogger sous le feu des projecteurs, qui fait revenir les lecteurs jour après jour, qui suscite les éloges de la presse ?

Un vrai lien avec ses lecteurs. Les blogs les plus lus sont ceux dont les lecteurs, qu'ils soient 10 ou 10 000, sentent qu'ils partagent quelque chose avec leurs auteurs. Le blogger va entretenir ce lien en les distrayant ou en les instruisant sur un sujet ou un autre. Même si, pour beaucoup, il existe une réelle différence entre les « posts » publiés sur un blog et les autres formes d'écriture (qu'il s'agisse d'articles de journaux, de littérature ou de publicité), bloggers, écrivains et journalistes ont bel et bien le même objectif : captiver le lecteur et ne pas le lâcher.

Certains des bloggers présentés dans ce guide – Chan'ad Bahraini au Bahreïn, Yan Sham-Shackleton à Hong Kong et Arash Sigarchi en Iran – vivent dans des pays où les gouvernements surveillent de très près ce qu'ils écrivent. Le monde aussi est à l'affût de ces publications, trop content de lire ce que la presse locale n'ose pas raconter. Là où la liberté de parole et la liberté de la presse sont en danger, les bloggers sont un lien important avec la réalité quotidienne des gens. Les photos qu'ils prennent, les histoires qu'ils racontent, sont essentielles.

Mais pourquoi ces blogs et certains autres sortent-ils du lot ? Vous trouverez ici quelques-unes de leurs principales qualités, qui les distinguent des millions de blogs présents sur la Toile.

**UN TON PERSONNEL**

Les meilleurs bloggers sont ceux qui ont trouvé une voix originale, qui expriment leur identité propre et racontent des histoires qui ont une réalité pour eux. Le blog est au départ un journal personnel en ligne, ce qui signifie qu'il n'a rien d'académique et qu'il ne cherche pas à avoir le ton neutre d'une dépêche d'agence. Chan'ad Bahraini est le pseudonyme d'un blogger asiatique vivant dans un pays majoritairement arabe, Bahreïn, ce qui lui donne une vision inhabituelle des événements qui s'y déroulent. Yan Sham-Shackleton est une artiste ayant vécu dans diverses régions du monde et participé à un mouvement

de protestation contre les autorités chinoises lorsqu'elles ont décidé de bloquer le site de blog TypePad. Elle connaît d'autant mieux la question que, quelques années plus tôt, elle aidait elle-même les autorités à filtrer le Net en Chine.

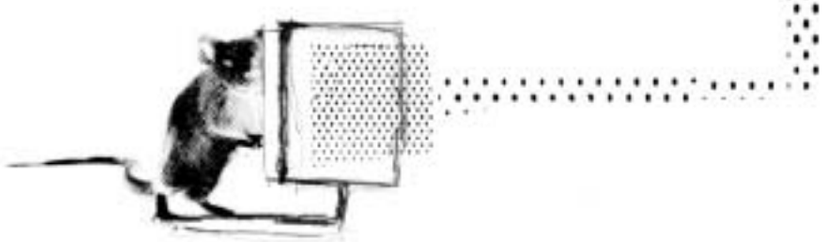
**L'ACTUALISATION**

Le plus gros problème de l'immense majorité des blogs est qu'ils ne sont pas actualisés. La plupart des gens ne sont pas payés pour tenir leur blog et ont du mal à intégrer l'écriture et la publication de messages dans leur routine quotidienne. Nombreux sont ceux qui lancent un blog, mais qui n'ont jamais le temps de le mettre à jour. La réussite d'un blog nécessite d'écrire régulièrement sur ses centres d'intérêts, si possible en suivant l'actualité. Cela ne veut pas dire qu'il faille écrire douze fois par jour, mais en quelques semaines de silence, un blog peut perdre son lectorat.

**DONNER LA PAROLE AUX LECTEURS**

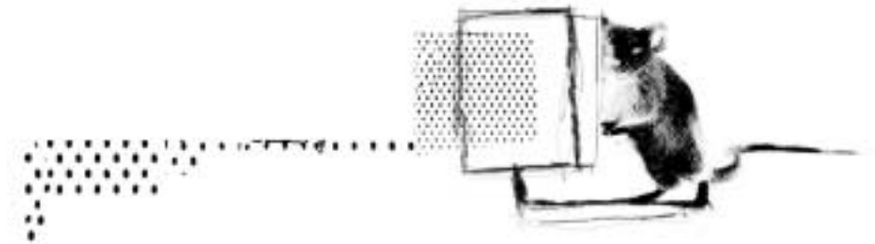
Ce qui fait ressortir un blog du lot, c'est également son interactivité. Il existe de nombreuses façons d'engager la conversation avec ses lecteurs, de les faire s'exprimer et d'utiliser leurs commentaires. Vous pouvez, par exemple, organiser un sondage en ligne, donner votre adresse électronique, ou autoriser les commentaires sous chaque « post ».

Jeff Ooi a reçu des menaces des autorités malaisiennes à cause d'un commentaire posté par l'un de ses lecteurs. A la suite de cette affaire, au lieu de retirer tous les commentaires en ligne, il a décidé d'assumer le rôle de modérateur et de s'assurer que ses lecteurs ne débordent pas du sujet débattu et restent responsables de leurs écrits. Il a par ailleurs lancé un blog en chinois intitulé « Le pilote de ferry » afin de construire un pont entre les univers des blogs malaisiens et chinois.





FAIRE SORTIR SON BLOG DU LOT

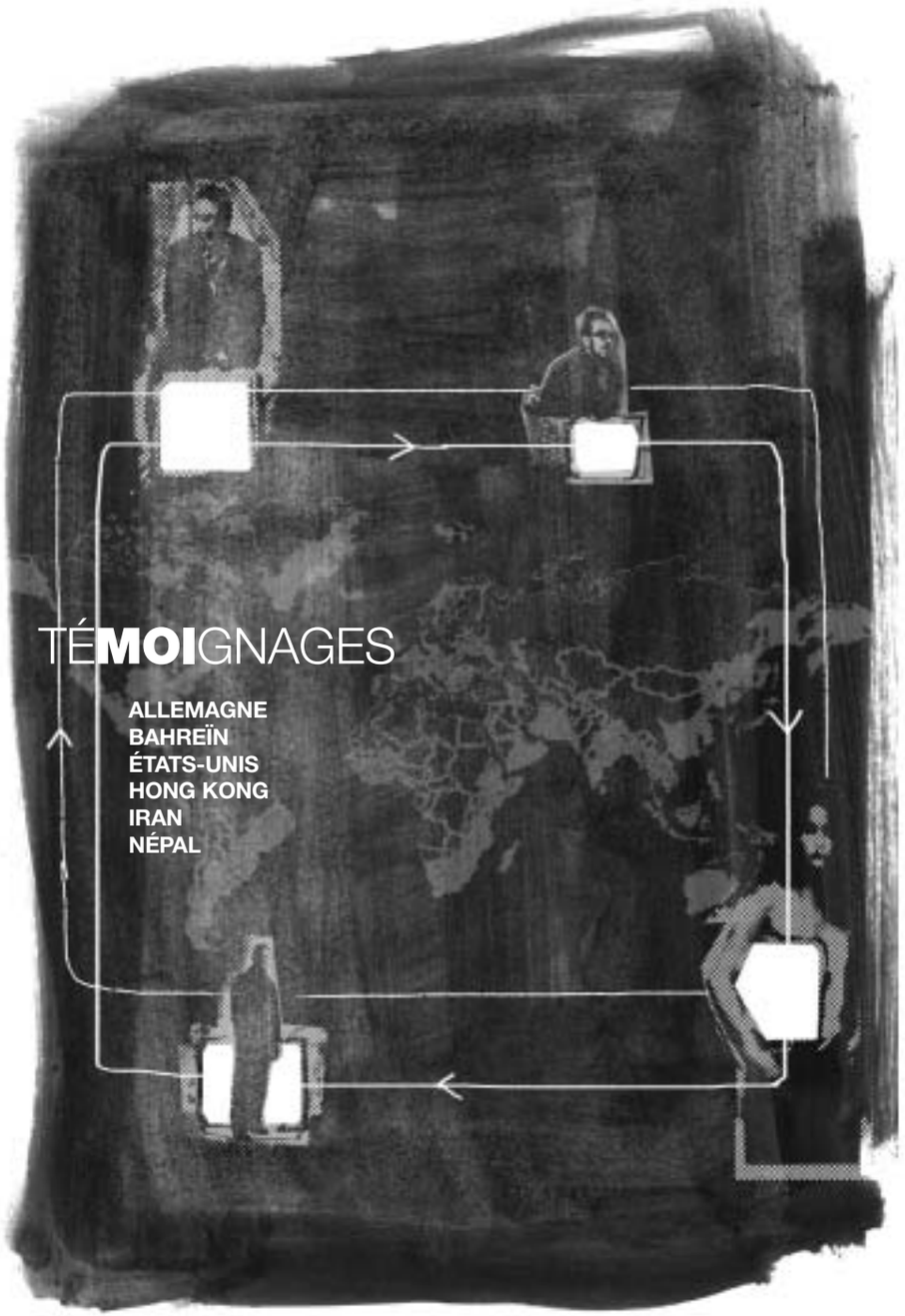


**PARLER FRANCHEMENT**

Si de nombreux blogs se contentent de commenter l'actualité, certains affichent aussi de véritables reportages. Il n'existe pas de recette en la matière, mais des reportages directs sur des événements ou un angle de vue spécial sur ceux-ci peuvent rendre un blog plus intéressant. Chan'ad Bahraini a publié des photos et une bande audio sur des manifestations à Bahreïn au cours desquelles un militant a été emprisonné en novembre 2004. Arash Sigarchi a, quant à lui, été arrêté en Iran et condamné à 14 ans de prison pour avoir protesté contre l'interpellation d'autres journalistes par le gouvernement. Ce qui est important, c'est que ces bloggers et beaucoup d'autres ont eu le courage de faire face collectivement, en tant que blogosphère, et ont parlé franchement aux autorités qui auraient volontiers caché la vérité.

**MARK GLASER**

Mark Glaser est journaliste pour *Online Jounalism Review* (www.ojr.org), une publication de l'Annenberg School for Communication de l'université de Southern California. Il est indépendant et travaille à San Francisco. Vous pouvez lui écrire à glaze@sprintmail.com.



# TÉMOIGNAGES

**ALLEMAGNE**
**BAHREÏN**
**ÉTATS-UNIS**
**HONG KONG**
**IRAN**
**NÉPAL**



# ALLEMAGNE

## « UN MOYEN RAPIDE ET EFFICACE DE PUBLIER DU CONTENU »

Markus Beckedahl
Netzpolitik.org

C'est à la fin des années 90, peu après mes 20 ans, que je suis devenu activiste et que j'ai commencé à militer pour une société de l'information libre et ouverte. J'ai alors fondé, avec quelques amis, une ONG en faveur des droits numériques « Réseau nouveaux médias ». Pendant cinq ans, nous avons fait la promotion des droits de l'homme dans l'univers numérique. Nous avons organisé des conférences, participé à diverses campagnes et milité dans des réseaux d'ONG. Par exemple, nous avons mis en place le « groupe de coordination de la société civile allemande pour le SMSI (Sommet mondial sur la société de l'information) » et nous avons déployé beaucoup d'efforts pour participer à ce Sommet.

Durant la première année de mon engagement politique, j'utilisais principalement des listes d'envoi par e-mail. J'ai ainsi transmis environ 5 000 articles sur des enjeux de netpolitique. Cependant, ces listes ne touchaient qu'un petit nombre d'internautes, toujours les mêmes. Les blogs, en revanche, sont ouverts, transparents et offrent beaucoup plus de possibilités pour partager mes connaissances et les résultats de mon travail.

J'ai commencé mon premier blog en 2002, à l'occasion de la première phase du SMSI. Je me suis rendu à Genève, pour une réunion préparatoire du Sommet, équipé uniquement d'un sac de couchage et d'un carnet de notes. J'avais besoin d'une infrastructure pour diffuser rapidement mes informations sans passer par un langage informatique comme le HTML – par le passé, l'utilisation de ce langage ralentissait la publication de mes articles sur le Net. J'ai raconté à ma façon cet événement sur un blog appelé « backpacking dans la politique mondiale ». Il s'agissait de mon premier blog, que j'ai ensuite abandonné pour me consacrer à mes activités professionnelles.

Au printemps 2004, j'ai commencé un nouveau blog, netzpolitik.org. J'ai essayé un certain nombre d'outils de publication et j'ai finalement opté pour Wordpress, un logiciel gratuit qui s'appuie sur une vaste communauté. Les blogs m'offrent un moyen rapide et pratique de produire, modifier et publier du contenu. Le plus important pour moi est d'avoir accès à une interface qui me permette de me concentrer sur la partie la plus importante de mon travail, à savoir la rédaction des articles, plutôt que de perdre du temps à réaliser des pages HTML. J'aime utiliser des interfaces conviviales pour récolter et compiler de l'information,

rédiger mes textes et les publier d'un simple click de souris. Les outils de blog simplifient énormément mon travail. J'utilise également la technologie du pousser-tirer (« push and pull »). La plupart de mes lecteurs reçoivent maintenant mes informations au travers du flux RSS de mon blog ; d'autres se rendent simplement sur mon blog ou y accèdent par l'intermédiaire de moteurs de recherche.

Comme je fais partie de plusieurs communautés politiques, je reçois beaucoup d'informations. J'essaie de compiler et de diffuser sur netzpolitik.org toutes les nouvelles portant sur les droits de l'homme, le monde du logiciel libre, l'accès libre à la connaissance, la société de l'information et les droits d'auteur. Les lois sur les droits d'auteur et la gestion des droits numériques ont des conséquences importantes sur la liberté d'expression, mais peu de gens comprennent l'importance de ces questions. J'essaie de sensibiliser mes lecteurs à ces problèmes afin qu'ils puissent défendre leurs droits. Les droits de l'homme sont menacés partout dans le monde, et l'Allemagne ne fait pas exception. Les initiatives qui visent à accroître la sécurité des populations s'accompagnent d'un resserrement abusif de la surveillance. Le grand public ne se rend malheureusement pas compte que sa liberté est menacée.

J'écris sur les logiciels gratuits, comme le système d'exploitation Linux, qui offrent des possibilités infinies pour promouvoir la liberté d'expression et le pluralisme. J'écris également sur les nouveautés en matière de logiciels gratuits et sur leur dimension politique, en tâchant notamment d'expliquer comment utiliser ces systèmes. Je suis de près le développement de l'encyclopédie en ligne Wikipedia et des « creative common (CC) licenses ». Mon contenu est lui-même offert sous licence CC et j'encourage activement mes lecteurs à copier mon travail, à condition de le faire à des fins non commerciales et en citant mon nom.

Un autre sujet qui m'intéresse est la façon dont Internet peut être utilisé par des organisations de la société civile dans le cadre de campagnes. Je connais bien cette question car j'ai été chef de projet et consultant en communication politique sur Internet. Deux catégories de mon blog, eCampaigning et eDemocracy, sont dédiées à ces questions. J'y analyse les outils gratuits permettant le travail collaboratif et l'activisme, en montrant comment diffuser largement un contenu généré par un groupe de travail.

Dans netzpolitik.org, je récolte également des informations sur les conférences et les réunions portant sur la société de l'information. Chaque jour, je produis une revue de






presse, contenant de nombreux hyperliens, où je commente par exemple l'élaboration de nouvelles lois et où je suis l'activité des ONG dans ce domaine. Mon blog tisse constamment de nouveaux liens au sein de la société civile germanophone. Je demande à des amis bloggers de rédiger des articles sur certains sujets importants et de m'aider à diffuser mes informations. Grâce aux flux RSS que je reçois, je peux compiler de l'information sur un sujet en très peu de temps. En 10 mois, j'ai réussi à publier plus de 800 articles, avec l'aide de seulement quelques amis.

A ma grande surprise, il y a maintenant en moyenne 2 500 personnes qui lisent mon blog. Je reçois des commentaires intéressants, particulièrement des jeunes. Ils lisent mon blog chaque jour et j'en profite pour les encourager à créer le leur.

Heureusement, l'Allemagne dispose de lois pour protéger la liberté d'expression. On ne m'enverra jamais en prison pour avoir critiqué le gouvernement. J'admire donc le courage des gens qui vivent sous une dictature et risquent leur vie pour mettre à jour leurs blogs.

**MARKUS BECKEDAHL**

Markus Beckedahl, 28 ans, est le directeur de Newthinking communications, une agence de conseil spécialisée dans l'utilisation des logiciels open source. Il est également cofondateur et président de l'ONG Netzwerk Neue Medien, qui œuvre dans le domaine des droits numériques.
Son blog : www. netzpolitik.org

# BAHREÏN

**« LE LIEU DE PRÉDILECTION POUR PARTAGER MES OPINIONS ET EN DISCUTER »**

Chan'ad Bahraini

J'ai créé mon blog pour deux raisons : premièrement, pour pouvoir écrire sans restriction et être publié sans délai ; deuxièmement, pour susciter des discussions sur des sujets qui sont peu ou mal couverts par les médias du Bahreïn.

En effet, toutes les chaînes de télévision et de radio du pays sont dirigées directement par le gouvernement. Par conséquent, elles couvrent de manière très partiale la situation politique du pays. Les journaux locaux sont privés et jouissent donc d'une liberté un peu plus grande. Pourtant, la situation de la presse écrite n'est guère meilleure car les rédacteurs en chef n'osent par critiquer ouvertement les personnes influentes, comme les membres du gouvernement ou de la famille royale (particulièrement le roi et son oncle, le Premier ministre).

Dans ce contexte, Internet fournit à chacun un moyen d'exprimer publiquement son opinion sans être inquiété par le gouvernement. Les autorités du Bahreïn n'avaient certes pas l'habitude de surveiller et de censurer les sites Web politiques, mais la situation s'est récemment dégradée. Il est encore difficile pour le gouvernement de s'attaquer aux responsables de sites, en particulier parce qu'il est très facile de publier sur Internet de manière anonyme (comme je le fais).

Je pense qu'il est aujourd'hui nécessaire de créer des lieux où peuvent se tenir des discussions libres et ouvertes, y compris sur des questions politiques. Cette liberté est d'autant plus importante que notre pays est en pleine transition vers la démocratie. Internet me paraissait donc le lieu de prédilection pour partager mes opinions et en discuter. J'ai été encouragé par le fait que Mahmood (www.mahmood.tv), le pionnier des bloggers au Bahreïn, qui avait lancé un blog environ un an avant moi, n'a jamais été inquiété par le gouvernement.

L'un des objectifs de mon blog est de discuter et d'analyser ce qui se passe au Bahreïn. Compte tenu du peu d'informations de première main disponibles dans la presse, je me suis moi-même lancé dans un pseudo-journalisme. J'essaie par exemple de participer à des manifestations et d'en rendre compte ensuite sur mon blog, si possible en illustrant mes commentaires avec des photos.





Il existe maintenant plusieurs bloggers dans le pays et leur travail a déjà eu des retombées positives. Nous avons créé un espace où nous tâchons de débattre en toute honnêteté sur des sujets variés. Il ne fait aucun doute que ces blogs m'ont permis d'avoir accès à des informations dont je n'aurais pas eu connaissance autrement. J'ajoute que cette communauté n'est pas que virtuelle : certains bloggers bahreïnis se réunissent une fois par mois dans le « monde réel ».

Je veux souligner que les forums de discussion en langue arabe (comme bahrainonline.org), qui sont plus anciens que nos blogs, sont encore les espaces de discussion en ligne les plus importants au Bahreïn. Mais nos publications jouent de plus en plus un rôle de « passerelle » avec les internautes non arabophones (tel que défini par Hossein Derakshan : http://hoder.com/weblog/archives/013982.shtml). Comme la plupart des bloggers du Bahreïn écrivent en anglais, nous pouvons dialoguer avec des gens de toutes nationalités, qui nous considèrent comme une source d'information fiable sur ce qui se passe « réellement » au Bahreïn.

Lorsque les trois modérateurs de Bahrainonline.org ont été arrêtés en février 2005, nous avons diffusé la nouvelle sur nos blogs et elle s'est répandue à l'étranger encore plus rapidement qu'au sein même du pays. Reporters sans frontières a publié une déclaration sur cette affaire moins d'une journée après la première arrestation. J'estime que l'attention soulevée dans le monde par cette nouvelle a joué un rôle dans la décision du gouvernement de relâcher les trois modérateurs quelques semaines plus tard. De façon générale, nos blogs ont brisé le monopole du gouvernement sur les informations relatives à Bahreïn.

Jusqu'ici, les bloggers bahreïnis n'étaient pas inquiétés par le gouvernement, mais cette situation a changé depuis le début de l'année. En février, trois modérateurs d'un forum de discussion ont été arrêtés sous prétexte que certains messages affichés sur leur site « incitaient à la haine contre le gouvernement ». L'un des modérateurs, Ali Abdulemam, avait également son propre blog.

Par ailleurs, en avril, le gouvernement a annoncé qu'il allait obliger tous les propriétaires de sites Web à s'enregistrer auprès du ministère de l'Information, sous peine de poursuites judiciaires. Ces mesures indiquent que le gouvernement ne comprend pas bien le fonctionnement d'Internet (et des blogs) et ne sait pas comment réagir lorsqu'il se sent menacé par des textes publiés en ligne.

**CHAN'AD BAHRAINI**

Chan'ad Bahraini, citoyen d'un pays du Sud-Est asiatique, habite à Bahreïn où il a créé son blog : http://chanad.weblogs.us. Il a choisi de préserver son anonymat.





# ETATS-UNIS

## « MAINTENANT, JE PEUX ÉCRIRE CE QUE JE PENSE »

Jay Rosen / Press Think

Lorsque j'ai commencé à me renseigner sur les techniques de blogging, j'ai reçu toutes sortes de réponses. Un des conseils qui m'a été donné était : « Tu dois écrire des 'posts' courts ». C'est le bon style, d'après certains. C'est ce qui marche, m'ont dit d'autres. Et surtout cette remarque, la plus suspecte de toutes : c'est ce qu'attendent les lecteurs débordés qui naviguent sur le Web. Ils n'ont pas de temps pour de longues et profondes analyses, ai-je entendu dire. Par tout le monde.

Cela m'a rendu méfiant. Je n'avais pas l'intention d'écrire de longs « posts » de 2 000 mots, mais c'est ce qui est arrivé lorsque j'ai essayé d'exprimer dans mes « posts » quelque chose que les autres ne disaient pas. Et ça a attiré l'attention. Je ne voulais m'imposer aucune restriction : être libre de trouver par moi-même ce qui marche, ce que PressThink veut être.

Un raisonnement tel que « les gens n'ont pas de temps pour… » ne voulait rien dire pour moi, et je ne m'y suis pas fié. Ce genre de conseil limiterait ma liberté d'écrire ce que je pense, alors que j'ai justement créé PressThink pour qu'il soit une libération : « Ouah ! Maintenant, j'ai mon propre magazine. Maintenant, je peux écrire ce que je pense. » Ce qui m'intéressait, c'était les utilisateurs qui AVAIENT du temps pour de la profondeur, quel que soit leur nombre, à travers les océans, de « posts » à « posts ».

Mon approche était celle-ci : « ceci est mon magazine, PressThink… si vous l'aimez, revenez. » Peut-être que de façon mineure et abstraite, mon blog fait partie du marché des médias, rivalisant avec les jeux télévisés, le football et les rediffusions de la série « New York District » pour attirer les regards. Mais pas vraiment. PressThink, un citoyen libre dans une nation volontaire, n'a pas à se comporter comme un acteur du marché. D'où mon expérimentation des longs articles.

On doit se rappeler que le Web est bon pour plein de choses opposées. Pour des informations marquantes et rapides. Pour survoler un domaine en quelques clicks. Pour les discussions et les interactions. C'est aussi un moyen de sonder en profondeur un dispositif de mémoire, une bibliothèque instantanée, un filtre. Ne pas utiliser un blog pour des analyses approfondies parce que cela découragera la plupart des lecteurs est idiot du point de vue du Web, mais intelligent si on se place du côté des médias. Mais je ne suis

pas un média ! C'est étrange, j'essaie bien d'écrire des choses courtes et accrocheuses, mais ça tourne toujours en de longs « posts ». Un certain nombre de lecteurs se manifestent pour s'en plaindre (« trop de mots sur le mauvais sujet ! » est une récrimination typique) et ça devient amusant au bout d'un moment.

Chaque bon blog pose une question au Web au départ : y a-t-il une demande par ici pour quelqu'un d'original… Pour moi ? Mais on doit travailler sur son blog pendant un moment avant de découvrir ce qu'il est censé être.

Réfléchir sur la presse, c'est ce que je fais moi-même, en tant que critique et écrivain. C'est aussi ce que je fais lorsque je travaille sur mon blog. Je veux amener les gens à réfléchir sur la presse. Je crois que certains bloggers ne cogitent pas assez le titre de leur blog. Dans mon cas, je n'ai été prêt à commencer mon blog que lorsque j'ai eu le bon titre.

J'essaie de laisser la critique idéologique de la presse à d'autres – certaines personnes et organisations – qui font ça très bien et avec avidité. PressThink n'est pas un site d'observation et de surveillance des médias, même si j'ai écrit sur les observateurs des médias. PressThink ne fait pas à la chasse aux « partis pris », dans le sens habituel du terme, mais j'ai écrit sur la chasse aux partis pris. Je ne soutiens pas George Bush, j'écris sur sa conception de la presse. Comme je l'ai dit dans l'introduction à mon blog : « J'essaie de découvrir les conséquences qui découlent du genre de presse que nous avons. »

Une fois, quelqu'un m'a demandé si j'avais une « méthode » de blogging. Je lis la presse, regarde les journaux télévisés, clique dans mon blogroll et je cherche quelque chose de croustillant, d'actuel, d'intéressant. Puis je rassemble les liens et je commence à écrire. Ou bien quelqu'un m'envoie quelque chose par e-mail qui m'incite à écrire un « post ». Souvent, quelque chose se produit et je sais que mes lecteurs voudront savoir ce que j'en pense. Alors je dois rédiger un « post ». Ce que j'ai, ce n'est pas une méthode concrète mais une sorte de feuille de style avec des instructions que je me suis moi-même imposées sur la façon de rédiger un « post » pour PressThink.





Voici un des mes « posts » typique : « Laying the Newspaper Gently Down to Die » (Poser doucement le journal pour qu'il meure)…
(http://journalism.nyu.edu/pubzone/weblogs/pressthink/2005/03/29/nwsp_dwn.html)
Il y a cinq parties qui doivent être traitées : le titre, le sous-titre, l'essai, l' « après-sujet » (avec les notes, réactions et liens) et les commentaires. Chaque partie me demande un style d'écriture différent. Le titre condense le sujet du « post » et attire l'attention. Le sous-titre explique la discussion et présente l' « histoire ». L'essai… c'est l'essai – généralement de 1 500 à 2 500 mots, avec 20 à 30 liens. La section « après » suit la progression de la discussion dans la blogsphere, y compris les réactions à mon « post ». Avec les commentaires commence le dialogue.

Un « post » réussi de PressThink, c'est quand les cinq parties se parlent, lorsqu'elles sont lues en relation l'une avec l'autre. Un article de PressThink n'est pas fini jusqu'à ce que l'après-sujet, les « trackbacks » et les commentaires arrivent, ce qui prend quelquefois plus d'une semaine. C'est le cycle normal d'un blog. Lorsque ça marche (c'est toujours quelque chose de hasardeux), le « post » se transforme en forum de discussion sur le sujet en question, et le forum est ce qui « pense ». Bien sûr, je ne connaissais rien de cette feuille de style et des contraintes d'écriture qu'elle impose jusqu'à ce que je tombe dessus à force d'essais et d'erreurs. Il faut du temps avant de trouver comment bien faire son blog. Avant de commencer PressThink, toutes mes idées sur le journalisme et les journalistes devaient, pour être publiées, recevoir l'approbation des éditeurs, ceux-là mêmes sur qui j'écrivais. Maintenant que j'ai mon propre magazine, je n'ai plus à le faire et ce sont ces chiens de garde qui viennent sur mon blog et lisent ce que je pense. J'ai enfin une vraie liberté intellectuelle.

**JAY ROSEN**

Jay Rosen enseigne le journalisme à l'université de New York. Il a créé Press Think en 2003 : tp://journalism.nyu.edu/pubzone/weblogs/pressthink/




# HONG KONG

## *GLUTTER*, UNE PROMESSE TENUE

Yan Sham-Shackleton

Il est 0h23. La toute première heure du 4 juin. Aujourd'hui, c'est le 16e anniversaire du massacre de la place Tiananmen à Pékin. Lors des événements, j'étais assise dans un tunnel devant l'agence de presse *Xinhua* de Hong Kong, où s'étaient installées des personnes en grève de la faim. Nous soutenions les étudiants chinois. Nous voulions la démocratie, pour eux et pour nous. Nous ne voulions plus être les sujets d'une colonie britannique, pas plus que les sujets du Parti communiste. Nous voulions la liberté.

Dans deux, peut-être trois heures, viendra le moment exact où j'ai entendu à l'époque les premiers coups de feu à la radio, suivis de chants, de cris, de bruits de chars dont l'écho se répercutait sur les murs du tunnel. Le moment où nous nous étions regardés, moi et une trentaine d'autres, les larmes aux yeux.

Nous savons tous maintenant que la Chine n'hésitera pas à faire venir les chars pour abattre les combattants de la démocratie. Mais nous l'ignorions alors, il y a 16 ans. Et je crois que c'est à ce moment-là qu'est né *Glutter*, lorsque j'ai entendu à la radio la fin du mouvement démocratique de 1989, dans un tunnel éclairé par d'éclatantes lumières fluorescentes. J'avais 15 ans.

Et si ce n'était pas à ce moment précis, c'était peu de temps après, lorsque j'ai prononcé un serment que seule une jeune fille sans expérience de la vie pouvait faire avec autant de certitude :
« Je n'oublierai pas. Je jure de me souvenir pour toujours. Je vivrai une meilleure vie, pour nous tous, parce que je suis vivante et que vous ne l'êtes plus. Je ne laisserai plus de telles choses se reproduire. Je rappellerai au monde les étudiants de la place Tiananmen. Mes héros. Mes grands frères, mes grandes sœurs. »

J'ai fait ces promesses dans la hâte, dans la peur, avec naïveté. Je ne me suis jamais demandé comment faire, ou même si c'était possible. Je ne savais qu'une chose : ces mots sonnaient juste, et j'entendais tous les adultes les hurler dans des haut-parleurs.

Ce n'est que cette nuit que je l'ai réalisé : tous ces écrits, toutes ces photos, tous ces dessins que j'ai faits au nom de la démocratie, toutes ces cyber-protestations que j'ai organisées,


les interviews que j'ai données, les histoires que j'ai publiées au nom de la libre expression, je ne les ai pas faits uniquement parce que je crois fermement à cette liberté, c'était aussi pour panser les plaies de mon subconscient. Ce blog, c'est mon moyen de tenir une promesse faite aux morts.

J'écris ces mots pour que l'on sache pourquoi j'ai créé *Glutter*. Pas parce que j'ai suivi des règles, ou imité quelqu'un. Pas parce que j'étais en quête d'attention ou de renommée. D'ailleurs, je laisse souvent mon blog inactif un certain temps lorsqu'il attire trop d'attention, pour pouvoir ensuite écrire comme je veux et raconter mes histoires comme j'en ai envie, sans pression.

A ceux qui aimeraient commencer un blog, je conseillerais de n'écouter personne d'autre qu'eux-mêmes. N'essayez pas d'imiter. N'essayez pas de respecter des consignes. J'ai enfreint quantité de règles dont j'ignorais d'ailleurs l'existence, et je m'en suis pourtant bien sortie.

Tout ce qu'il vous faut pour créer un blog, c'est la volonté de le faire.

Tout ce qu'il vous faut pour le faire vivre, c'est la volonté de vous exprimer.

Nous connaissons tous un jour ou l'autre un moment d'éveil politique, un déclic qui nous fait prendre conscience d'une injustice à réparer. Que cette conscience vous guide. J'espère que vous arriverez à transmettre avec suffisamment de force vos convictions pour inspirer à d'autres le désir de se battre pour le changement. Voilà tous les sages conseils que je pourrais vous prodiguer ce soir.

Il est maintenant 2h33. J'entends les coups de feu. Pan, pan, pan. Je les entends chaque année à la même heure. J'avais 15 ans. J'étais trop jeune pour vivre ces événements comme je les ai vécus. Mais d'autres que moi étaient trop jeunes pour mourir.

**YAN SHAM-SHACKLETON**

Yan Sham-Shackleton a tenu à vous faire savoir qu'elle a passé six semaines à rédiger six versions différentes de cet article, qu'elle a essayé de réunir tout ce qu'elle savait sur l'art du blogging, avant de réaliser que la beauté de ce moyen de communication, c'est qu'il donne tout simplement la liberté d'être soi-même.
Sur son blog, glutter.com, Yan traite aussi bien d'art que de politique, au gré de son inspiration. Sa liberté de ton et ses prises de position en faveur d'une réelle démocratie dans sa province, Hong Kong, lui valent d'être régulièrement censurée en Chine.





# IRAN

## « UN BLOG PERMET D'ÉCRIRE LIBREMENT »

Arash Sigarchi

Aujourd'hui, la pensée de Mac Luhan selon laquelle « le monde est un village planétaire » prend tout son sens. Internet permet d'alimenter les médias à tel point que si quelque chose se passe en Extrême-Orient, en Amérique, en Europe ou même sur une île reculée d'Afrique, nous en sommes informés.

Pendant des années, le journalisme a été soumis à des restrictions, mais la technologie a le pouvoir de les faire disparaître.

Je suis journaliste dans un pays où, malheureusement, diverses contraintes m'empêchent de faire mon travail. En effet, outre des facteurs internes aux médias communs à la plupart des pays, il existe en Iran des facteurs extérieurs tels que les restrictions juridiques, l'influence exercée par le pouvoir et par certains particuliers, le soutien partisan à des médias, les groupes de pression et les propriétaires des médias. C'est donc tout naturellement que je me suis mis à penser à l'indépendance de mon pays et que j'ai voulu en rendre compte en publiant de vraies informations et en donnant ma propre analyse des événements. L'une des solutions pour contourner les obstacles était de créer un weblog.

Un blog permet d'écrire librement. Dans la mesure où il n'est pas nécessaire de l'imprimer ou de le diffuser via d'autres médias, c'est un outil qui permet d'informer et d'exprimer rapidement des opinions. D'une manière générale, on peut considérer les journaux en ligne comme de petites agences de presse ou des instituts d'analyse dans lesquels celui qui écrit est à la fois correspondant et rédacteur en chef.

Certains affirment que les blogs ne doivent pas chercher à publier de réelles informations. En effet, certains bloggers se contentent de raconter leur journée. Ces écrivains amateurs ont un public relativement restreint, souvent limité à leurs proches. A l'inverse, les chroniques de journalistes, d'artistes connus, de personnalités du monde politique, économique, social, sportif, etc., sont remarquées pour leur valeur éditoriale et pour la célébrité de leurs auteurs, même si leurs « posts » racontent le quotidien de ces célébrités. Dans la mesure où ils sont confrontés à toutes sortes de problèmes, ces bloggers ont un grand nombre de sujets sur lesquels écrire et qui intéressent les lecteurs.
Je pense que chaque publication attire ses propres lecteurs en fonction de ce que ces

derniers recherchent, de sorte qu'il n'est pas nécessaire d'instaurer des règles sur les thèmes à aborder ou le ton à utiliser sur un blog.

Pour ma part, j'ai choisi deux méthodes de journalisme en ligne. La première, exprimer de manière informelle (dans un style oral) mon avis sur les sujets d'actualité. La deuxième, rédiger des articles, des analyses, des interprétations, des entretiens, des rapports ou des essais. Ainsi, je peux avoir deux types de lecteurs : ceux qui veulent savoir ce que je fais au quotidien et ceux qui attendent que je donne mon avis en tant que journaliste, écrivain et poète.

Le weblog, en tant que média en ligne, permet à celui qui écrit d'avoir un retour franc et critique de ses lecteurs, mais aussi de leur répondre et ainsi, grâce à ces échanges, de se perfectionner. Ce feed-back permanent permet au blogger de mieux préciser son opinion et d'écrire sur ce qui intéresse le plus ses lecteurs.

Comme je l'ai déjà dit, dans mon pays, pour publier un livre, un poème, une histoire, un journal ou une revue, il faut l'autorisation d'organes officiels de l'Etat. Un grand nombre d'écrivains et de journalistes ne parviennent pas à se faire éditer, à moins d'avoir reçu l'approbation des instances chargées de la sécurité et de la justice.

Toute parution dans la presse est exposée au risque de censure. Il s'ensuit qu'en Iran, beaucoup de journalistes écrivent dans des journaux en ligne. Cela leur coûte moins cher et ils ne sont pas obligés de se censurer. C'est pourquoi, à l'instar d'autres Etats, comme par exemple la Chine, le gouvernement iranien surveille le Web aussi scrupuleusement que les médias traditionnels.





Cependant, je tiens à insister sur le fait que le journalisme via Internet peut contribuer à faire avancer la liberté d'expression et la diversité d'opinions. Bien que j'ai été condamné par la justice iranienne, je ne désespère pas et je suis certain que, d'ici quelques années, les dirigeants de mon pays seront obligés d'accepter la libre circulation de l'information et de respecter la liberté d'expression.

**ARASH SIGARCHI**

Arash Sigarchi est journaliste et weblogger. Né en 1978, en pleine révolution iranienne, il a commencé sa carrière de journaliste en 1993, alors qu'il n'avait que 15 ans. Lorsque Seyed Mohammad Khatami, président réformateur de la République islamiste d'Iran, a remporté les élections, en 1997, Sigarchi a rejoint la presse réformatrice. Quand l'ensemble des titres réformateurs ont été fermés, en avril 2000, il s'est installé dans une province du nord du pays où il est devenu rédacteur en chef d'un quotidien de 12 pages intitulé *Gilan Emrouz* (Le Gilan d'aujourd'hui).
En 2001, il a commencé à écrire pour un journal collectif en ligne : *Gileh Mard* (L'homme du Gilan). Puis, en 2002, il a créé son propre weblog (http://www.sigarchi.com/blog/) qu'il a intitulé « Panjareh yi Eltehab » (La fenêtre de l'espoir).
Début 2005, il a été arrêté et emprisonné pendant deux mois par le ministère de l'Information et de la Sécurité de la République, puis condamné à 14 ans d'emprisonnement par un tribunal révolutionnaire. Il a été remis en liberté dans l'attente du réexamen de son cas par une cour d'appel.


# NÉPAL

**« DIFFUSER AU RESTE DU MONDE DE L'INFORMATION SUR MON PAYS »**

Radio Free Nepal (RFN)

Le 1er février 2005, le roi du Népal Gyanendra s'est emparé du pouvoir et l'a annoncé lors d'un discours télévisé. Après ce discours, je voulais connaître la réaction des autres pays, j'ai donc essayé de me connecter à Internet. Un message s'est alors affiché m'indiquant qu'il n'y avait pas de ligne téléphonique en service. J'en ai conclu que les communications avaient été coupées. Afin de faire taire les critiques, le roi avait ordonné à l'armée de bloquer non seulement les fournisseurs d'accès à Internet mais aussi tous les services de télécommunications.

Dans le même temps, les gens parlaient des conséquences de cette prise de pouvoir et certains l'approuvaient. A la rédaction de mon journal, tous les employés envisageaient l'avenir avec crainte en imaginant que l'armée envahirait les bureaux pour exercer sa censure. J'ai alors songé qu'il serait approprié de noter dans un journal les événements au quotidien et les réflexions des gens qui m'entouraient. Pour ce faire, j'ai utilisé mon ordinateur.

Le 8 février, les services de télécommunications de base et les services Internet ont été rétablis. De nombreuses personnes m'avaient envoyé des e-mails pour me demander ce qui se passait au Népal. J'ai alors pensé que mon journal serait l'outil idéal pour expliquer la situation. Des amis vivant aux Etats-Unis m'ont suggéré de mettre ce journal sur un blog. Comme je ne connaissais pas ce type de publication, ils m'en ont ouvert un et ont posté les informations à ma place. Nous avons décidé que ce blog serait anonyme et j'ai demandé à d'autres amis d'y contribuer sous couvert de l'anonymat. Cette précaution nous permet d'éviter d'être victimes de harcèlement ou d'être emprisonnés.

La censure exercée dans les médias dans les premiers jours et le flot d'informations publiées sur RFN ont fait que Blogger.com a recommandé notre blog. Mes amis des Etats-Unis ont également fait leur possible pour accroître la popularité du site, dont le nombre de visites a rapidement explosé.

Nous avons pris la décision de lancer RFN afin que les gens d'autres pays puissent comprendre ce que nous ressentons face aux agissements du roi. Victimes de censure, les médias sont forcés d'écrire ce que veut le roi et ne peuvent exprimer ce que pense réellement le peuple.





Une des raisons d'être de RFN est de diffuser aux autres pays de l'information sur ce qui se passe au Népal. RFN est l'œuvre d'une seule personne, en collaboration avec un petit groupe, mais il représente bien ce que tous exprimeraient s'il n'y avait pas la censure et la peur d'être persécuté. Les premiers articles de RFN étaient principalement rédigés sous forme de journal décrivant les événements quotidiens. On y trouve maintenant des analyses plus rigoureuses de l'actualité. Dans une situation politique comme celle que vit le Népal, avec un roi qui prend le pouvoir sans tenir compte de l'avis de son peuple, RFN prend toute son importance car il exprime la pensée de la majorité.

Je lutte pour l'établissement de la démocratie au Népal car je crois que c'est la seule façon de faire prospérer le pays et de donner un sens à ma carrière de journaliste. Ecrire sous la censure, c'est un peu comme manger de la nourriture sans sel, cela perd toute sa saveur. En tant que journalistes, nous savons beaucoup de choses qui ne sont pas publiées dans les journaux, comme par exemple les informations parues sur RFN concernant l'acquisition par le roi de propriétés personnelles dans des circonstances troubles. De nombreux journalistes étaient au courant, critiquaient et ridiculisaient le roi, mais ils ne pouvaient pas publier leurs commentaires.

Sans notre blog, plusieurs milliers de personnes ignoreraient ce qui se passe réellement au Népal.

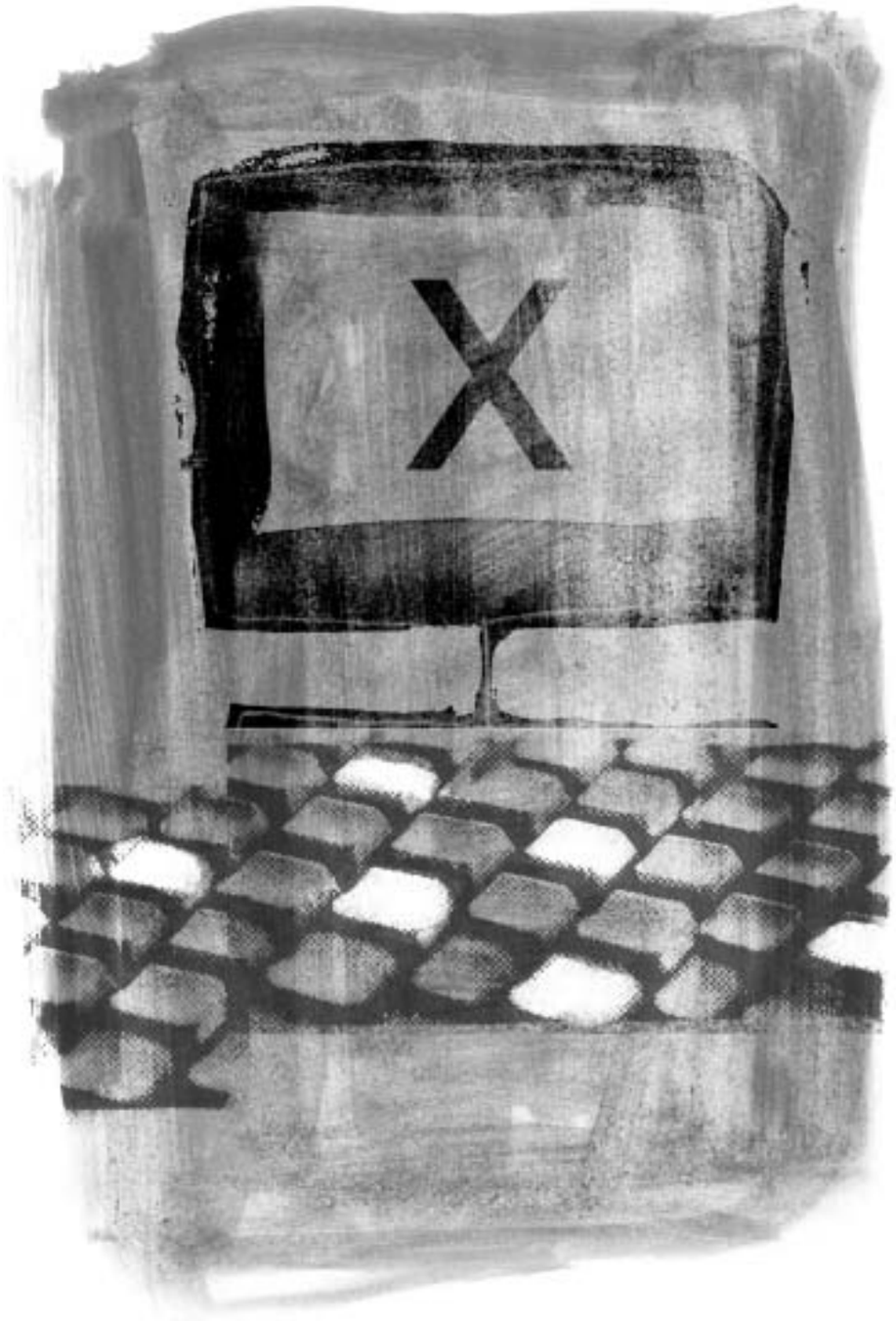
Les progrès techniques ont apporté beaucoup à notre société. J'écris en toute liberté et sans crainte car les moyens que j'utilise pour alimenter le blog (rédiger un texte puis l'envoyer à mes amis des Etats-Unis pour qu'ils le publient) ne sont pas identifiables, à moins que la police ne déploie d'importantes ressources techniques. Lorsque la démocratie sera rétablie et que nous pourrons vivre librement, je serai fier de moi car j'aurai contribué à cet événement.

De nombreuses personnes m'écrivent des e-mails pour savoir si les articles du blog sont fiables. Je leur réponds qu'un nom seul ne peut confirmer la fiabilité d'une information. Je préfère que nous restions anonymes car d'ici à ce que la démocratie soit rétablie, la situation peut se détériorer et il est possible qu'on m'envoie en prison à cause de mes écrits. Je n'ai pas peur de la prison, mais je souhaite continuer à maintenir RFN en vie afin de diffuser au reste du monde de l'information sur mon pays. J'ai promis de divulguer mon nom lorsque la dictature du roi sera terminée.

Merci à vous tous pour votre soutien jusqu'ici.

**BLOGGER DE RADIO FREE NEPAL**
wewantdemocracy@gmail.com

L'auteur de ce témoignage a préféré gardé l'anonymat.
Radio Free Nepal (http://freenepal.blogspot.com) est un blog qui dénonce la prise de pouvoir illégale du roi Gyanendra et défie sa politique de censure des médias. Travaillant pour restaurer la démocratie, RFN publie des informations de première main à propos du Népal.




# COMMENT BLOGGER **DE MANIÈRE ANONYME ?**

J'ai rédigé ce petit guide technique en me mettant dans la peau d'un fonctionnaire qui cherche à faire sortir des informations concernant un scandale dont il est le témoin, dans un pays où toucher à ce type de problème peut être dangereux. Ces conseils ne sont pas destinés aux as de la cryptographie, mais aux personnes qui, dans des pays peu respectueux de la liberté d'expression, s'inquiètent pour leur sécurité et veulent protéger leur vie privée. Un article de l'organisation américaine de défense des cyberlibertés Electronic Frontier Foundation's (EFF), « How to Blog Safely » (http://www.eff.org/Privacy/Anonymity/blog-anonymously.php), fournit des informations pratiques complémentaires sur ce sujet.

**SOMMAIRE**



## PRÉSENTATION DE SARAH

Sarah travaille comme comptable dans l'administration. Elle réalise que son patron, un ministre, détourne de larges sommes d'argent. Elle veut rendre ce délit public, mais elle a peur de perdre son emploi. Si elle en parle au ministre, pour peu qu'elle arrive à obtenir un rendez-vous, elle risque d'être licenciée. Elle fait tout d'abord appel à un journaliste qui travaille pour un journal local, mais il affirme qu'il ne peut traiter cette affaire avec le peu d'informations dont elle dispose et qu'il a besoin de documents qui apportent les preuves de ce qu'elle affirme.
Sarah décide donc de créer un blog, pour dévoiler au monde ce qui se passe au ministère. Pour se protéger, elle veut s'assurer que personne ne peut découvrir son identité à partir de son blog. Elle doit donc créer un blog anonyme. Or, il existe deux façons de découvrir

l'identité d'un blogger. La première : le blogger peut révéler lui-même son identité dans le contenu de sa publication. Par exemple, si Sarah dit : « Je suis l'assistante comptable en chef du secrétaire d'Etat aux Mines », quelqu'un lisant son blog aura vite fait de découvrir son identité. L'autre façon de découvrir l'identité de Sarah est d'exploiter les informations fournies par les navigateurs ou par les programmes d'e-mail. Tout ordinateur relié à Internet a, ou partage, une adresse IP : une série de quatre chiffres entre 0 et 255, séparés par des points. Par exemple : 213.24.124.38. Lorsque Sarah utilise son navigateur pour faire un commentaire sur le blog du ministère, l'adresse IP qu'elle utilise apparaît sur son message. En cherchant un peu, les informaticiens du ministère peuvent retrouver l'identité de Sarah grâce à cette adresse IP. Si Sarah se connecte de chez elle, par le biais d'un fournisseur d'accès Internet (FAI), ce dernier peut très certainement faire le lien entre l'adresse IP utilisée pour poster des messages et le numéro de téléphone de Sarah. Dans certains pays, le ministre devra demander un ordre judiciaire pour obtenir ces renseignements. Dans d'autres, et particulièrement ceux dans lesquels les fournisseurs Internet appartiennent à l'Etat, le gouvernement n'aura pas de mal à obtenir ces renseignements et Sarah risque de se retrouver dans une situation délicate.
Il existe plusieurs façons pour que Sarah dissimule son identité sur Internet. De manière générale, le degré de protection dépend de l'effort qu'elle est prête à fournir pour la cacher. Toutes les personnes désireuses de créer un blog de façon anonyme doivent décider jusqu'où elles sont prêtes à aller pour protéger leur identité. Comme nous allons le voir, quelques-uns des moyens employés pour protéger l'identité d'un internaute nécessitent des connaissances techniques approfondies et beaucoup de travail.

## PREMIÈRE ÉTAPE : LES PSEUDONYMES

Une façon simple pour Sarah de cacher son identité est d'utiliser un compte mail ainsi qu'un outil de blog gratuits, basés à l'étranger (utiliser un compte payant pour l'e-mail ou pour un outil de blog n'est pas une bonne idée puisque le paiement permettra de remonter à une carte de crédit, un compte courant ou un compte paypal et ainsi de retrouver la trace du blogger). Sarah peut se créer une fausse identité, un pseudonyme, qu'elle utilisera pour ces comptes. Quand le ministère trouvera son blog, il découvrira qu'il appartient à « A.N.O.Nyme », dont l'adresse e-mail est : « anonyme.blogger@hotmail.com ».

Quelques fournisseurs de comptes e-mail gratuits :
- Hotmail
- Yahoo
- Hushmail : e-mail gratuit qui apporte une solution de cryptage

Quelques outils de blog :
- Blogsome : outil de blog gratuit de WorldPress
- Blogger
- SEO Blog

Mais cette stratégie pose un problème : lorsque Sarah crée un compte mail ou un blog, le fournisseur qu'elle utilise enregistre son adresse IP. Si cette adresse IP est associée au





domicile ou au bureau de Sarah, et si l'entreprise qui gère le service d'e-mail ou de blog est obligée de livrer ses informations, le ministère peut retrouver Sarah. Il n'est pas facile de forcer les fournisseurs des services Web à donner ce type de renseignements. Par exemple, pour que Hotmail reconnaisse que Sarah a signé un contrat avec eux, le ministère sera certainement obligé de recourir à un ordre judiciaire, en collaboration avec l'agence américaine d'application des lois. Mais Sarah ne veut peut-être pas prendre le risque que son gouvernement parvienne à convaincre son fournisseur d'e-mail ou de blog de dévoiler son identité.

## DEUXIÈME ÉTAPE : LES ORDINATEURS PUBLICS

Un autre moyen que Sarah peut envisager pour cacher son identité est de se servir d'ordinateurs publics, c'est-à-dire utilisés par un grand nombre de personnes, pour gérer son blog. Au lieu de créer son compte e-mail ou son blog à partir de l'ordinateur qu'elle utilise chez elle ou au bureau, elle peut le faire à partir d'un cybercafé ou d'une bibliothèque. Lorsque le ministère vérifiera l'adresse IP utilisée pour poster des messages sur le blog, il découvrira que cela a été fait d'un cybercafé où les ordinateurs sont utilisés par beaucoup de monde.
Cette stratégie a des inconvénients. Si le cybercafé ou le laboratoire d'informatique de l'université note l'identité de l'utilisateur de tel ordinateur à telle heure, l'identité de Sarah risque d'être dévoilée. Il ne faut pas qu'elle essaie de poster des messages au beau milieu de la nuit, quand elle se retrouve seule au laboratoire d'informatique, parce que le veilleur se souviendra certainement de qui il s'agit. Elle devra changer souvent de cybercafé. En effet, si le ministère découvre que tous les messages le concernant proviennent de l'Internet café « Chez Jojo, bières et snacks », dans la rue principale, il risque d'y envoyer quelqu'un pour vérifier qui poste ces messages.

## TROISIÈME ÉTAPE : LES PROXIES ANONYMES

Sarah en a marre d'aller « chez Jojo » chaque fois qu'elle veut mettre à jour son blog. Avec l'aide d'un voisin, elle met en place un système lui permettant d'accéder au Web de son ordinateur en utilisant un proxy anonyme. A partir de maintenant, lorsqu'elle utilise son mail ou son blog, c'est l'adresse IP du proxy qui apparaîtra et non l'adresse de son ordinateur personnel. Le ministère aura ainsi beaucoup de mal à la retrouver.
D'abord, elle se procure une liste de proxies sur Internet, en recherchant « serveur proxy » sur Google. Par exemple, elle en choisit un dans la liste fournie par publicproxer.com, en préférant un proxy qui porte la mention « High anonymity » (Niveau d'anonymat élevé). Elle note ensuite l'adresse IP du proxy ainsi que son port. (Sur l'utilisation de proxies, voir également l'article « Comment contourner la censure »).

Quelques listes de proxies connues :
- publicproxer.com : liste de proxies anonymes et non anonymes.
- Samair (http://www.samair.ru/proxy/) : des proxies anonymes ainsi que des renseignements sur les proxies qui acceptent le système de cryptage SSL.
- Rosinstrument proxy database (http://tools.rosinstrument.com/proxy/) : une base de données de proxies.

Puis, elle va dans le menu « préférences » de son navigateur. Dans « Général », « Réseau » ou « Sécurité » (habituellement), elle va trouver une option lui permettant d'entrer les paramètres du proxy pour accéder à Internet. (Sur le navigateur de Firefox que j'utilise, on peut trouver cette option dans « préférences", « Général », « Paramètres de la connexion »).
Elle clique ensuite sur « Configuration du proxy pour accéder à Internet », entre l'adresse IP du serveur et du port de ce proxy dans les sections « proxy http » et « proxy SSL », puis enregistre ces paramètres. Elle redémarre son navigateur et peut ainsi naviguer sur le Web en utilisant désormais un proxy anonyme.
Elle se rend compte que sa connexion sur le Web est un peu lente. C'est parce que, pour chaque page Web qu'elle télécharge, elle est obligée de faire un détour. Au lieu de se connecter directement à Hotmail.com, elle se connecte d'abord au proxy, qui lui-même se connecte à Hotmail. Quand Hotmail lui envoie une page, celle-ci est dans un premier temps reçue par le server proxy, qui la lui renvoie. Elle remarque également qu'elle rencontre quelques difficultés pour accéder à certains sites Web, en particulier ceux qui nécessitent une inscription. Mais, au moins, son adresse IP n'est pas enregistrée par son outil de blog !
On peut s'amuser avec les proxies : allez sur noreply.org, qui est un site de re-mailer très populaire. Le site vous accueille en vous donnant votre adresse : « Bonjour pool-151-203-182-212.wma.east.verizon.net 151.203.182.212, bienvenue. »
Maintenant, rendez-vous sur anomyzer.com, un service qui permet de visionner (certaines) pages Web à travers un proxy anonyme. Dans la case en haut à droite de la page d'anomyser, tapez l'adresse URL : http://www.noreply.org. (Ou cliquez sur ce lien http://anon.free.anomyzer.com/http://www.noreply.org). Vous pouvez voir que noreply.com pense maintenant que vous venez de vortex.anomyzer.com (Anomyzer est un bon moyen de tester les proxies sans changer les paramètres du navigateur, mais cela ne fonctionne pas avec les services Web plus sophistiqués, comme les webmails ou les serveurs de weblog).
Enfin, suivez les instructions ci-dessus pour mettre en place votre navigateur afin d'utiliser un proxy anonyme, puis rendez-vous sur noreply.com pour savoir d'où il pense que vous venez.
Hélas, les proxies ne sont pas parfaits non plus. En effet, de nombreux pays bloquent l'accès aux proxies les plus populaires, afin d'éviter que les internautes ne s'en servent pour accéder à des sites interdits. Les internautes doivent donc changer de proxy lorsque celui-ci est bloqué par les autorités. Ces manipulations risquent de causer une importante perte de temps. Si Sarah est l'une des seules dans son pays à utiliser un proxy, elle peut rencontrer un autre problème. Si, à partir du blog, on peut remonter à un seul serveur proxy, et si le ministère a les moyens d'accéder aux données enregistrées par tous les FAI du pays, il risque de découvrir que l'ordinateur de Sarah était l'un des seuls à avoir accédé à ce proxy particulier. Il ne peut pas prouver que Sarah a utilisé le proxy pour aller sur un outil de blog. Mais il peut vérifier qu'elle est l'une des seules internautes à utiliser ce proxy et peut en déduire que c'est bien elle qui met à jour le blog en question. Sarah a ainsi tout intérêt à utiliser des proxies très populaires dans la région où elle se trouve et à en changer souvent.





## QUATRIÈME ÉTAPE : MAINTENANT, VRAIMENT, C'EST CONFIDENTIEL !

Sarah commence à se demander ce qui va se passer si les serveurs de proxy qu'elle utilise sont compromis. Si le ministère arrive à convaincre l'opérateur d'un proxy, de façon légale ou en le corrompant, de conserver des traces de tous ses utilisateurs et de noter quels sites ils visitent. Elle compte sur l'administrateur du proxy pour la protéger, mais elle ne le connaît même pas !
(En vérité, l'administrateur de proxy risque, de même, ne pas être au courant qu'elle passe par son intermédiaire pour se connecter au Net, car il a le plus souvent laissé ouvert son proxy accidentellement).
Heureusement, Sarah a un ami au Canada – un pays moins enclin que le sien à censurer Internet – qui sera peut-être d'accord pour l'aider à garder son blog tout en restant anonyme. Sarah l'appelle et lui demande d'installer « Circumventor »
(http://www.peacefire.org/circumventor/simple-circumventor-instructions.html) sur son système. Circumventor est un système qui permet à son utilisateur d'utiliser son ordinateur comme proxy pour d'autres internautes.
Jim, l'ami de Sarah, télécharge Circumventor à partir de Peacefire.org et l'installe sur Windows. L'installation n'est pas facile. Il faut qu'il commence par installer Pearl, puis OpenSA, pour enfin pouvoir installer Circumventor. Ensuite, il faut qu'il laisse son ordinateur connecté à Internet en permanence pour permettre à Sarah de l'utiliser comme proxy sans avoir à lui demander de se connecter chaque fois qu'elle veut surfer sur Internet. Il fait le nécessaire, appelle Sarah sur son portable, et lui donne une adresse URL qu'elle peut utiliser pour naviguer sur le Web ou aller sur son blog en utilisant le proxy qu'il a mis en place. C'est très pratique car Sarah peut utiliser le proxy de chez elle ou d'un cybercafé et n'a à changer aucun paramètre dans son système.
Bien que Sarah soit très reconnaissante envers Jim, cette solution présente un problème majeur. L'ordinateur de Jim, qui utilise Windows, redémarre assez souvent. Chaque fois, son ISP lui donne une nouvelle adresse IP et, chaque fois, Sarah ne peut plus utiliser son proxy sans connaître la nouvelle adresse. A chaque fois, Jim doit contacter Sarah pour lui donner la nouvelle adresse, ce qui est cher et frustrant. Sarah a par ailleurs peur qu'en utilisant la même adresse trop longtemps, son ISP cède à la pression du gouvernement et la rende inaccessible.

## CINQUIÈME ÉTAPE : L' « ONION ROUTING », GRÂCE AU SYSTÈME TOR

Jim suggère à Sarah d'essayer Tor, un système relativement nouveau dont le but est de conserver son anonymat tout en surfant sur Internet. L'« onion routing » reprend le même principe que les serveurs proxies, c'est-à-dire que Sarah se connecte à Internet en passant par un autre ordinateur comme intermédiaire, mais il va plus loin. Chaque demande faite à un réseau d'« onion routing » passe par plusieurs ordinateurs, entre 2 et 20. Il devient donc très difficile de savoir quel ordinateur est à l'origine de la requête.
Chaque étape de routage est chiffrée, ce qui rend plus difficile pour le gouvernement de retrouver la trace de Sarah. De plus, chaque ordinateur de la chaîne ne connaît que ses voisins les plus proches. En d'autres termes, le serveur B sait que le serveur A lui a envoyé une demande d'accès à une page Web, et qu'il fait passer la demande à un routeur C. Mais

la demande elle-même est chiffrée : routeur B ne sait pas quelle page a été demandée par Sarah ou quel est le routeur qui va finalement télécharger la page.
Vu la complexité de la technologie, Sarah est agréablement surprise de la facilité avec laquelle elle a pu installer Tor sur son système (http://tor.eff.org/cvs/tor/doc/tor-doc-win32.html). Puis, elle télécharge et installe Privoxy, un proxy qui fonctionne avec Tor et qui supprime toutes les publicités qui apparaissent sur les pages Web que Sarah regarde. Après avoir installé le logiciel et redémarré son ordinateur, Sarah va sur noreply.com et découvre qu'elle est « couverte » par le système Tor. Noreply.com pense qu'elle se connecte de l'université de Harvard. Elle réessaye, et là, noreply pense qu'elle est en Allemagne. Elle en conclut que Tor change son identité à chaque demande, ce qui l'aide à protéger son anonymat.
Cela entraîne cependant quelques conséquences étranges. Lorsqu'elle va sur Google en passant par Tor, il change constamment de langue ! Une recherche en anglais, une autre en japonais, puis en allemand, en danois et en hollandais, tout cela en quelques minutes. Sarah en profite pour apprendre de nouvelles langues, mais il y a d'autres conséquences qui l'inquiètent davantage. Sarah aime bien contribuer au dictionnaire collaboratif Wikipedia, mais elle se rend compte que celui-ci bloque ses tentatives d'édition d'articles lorsqu'elle passe par Tor.
Tor semble également rencontrer les mêmes problèmes que les autres proxies utilisés par Sarah. La navigation sur Internet est plus lente comparée à la navigation sans proxy. Elle finit par utiliser Tor uniquement lorsqu'elle va sur des sites dont le contenu est délicat ou pour poster sur son blog. Et, autre désavantage, elle ne peut pas installer Tor sur un ordinateur public et ne peut donc utiliser ce système que de son domicile.
Le plus inquiétant cependant, c'est que Tor cesse parfois de fonctionner ! En effet, le FAI de Sarah bloque certains serveurs relais utilisés par Tor et lorsque Tor essaie d'utiliser un routeur bloqué, elle peut passer de longs moments à attendre et n'obtient parfois jamais la page demandée.

## SIXIÈME ÉTAPE : MIXMASTER, INVISIBLOG ET GPG

Sarah se demande s'il existe une solution au problème pour blogger sans utiliser de serveur proxy. Après avoir passé pas mal de temps avec le technicien du coin, elle commence à explorer une nouvelle option : Invisiblog. C'est un groupe d'Australiens anonymes, appelé « vigilant.tv », qui gère ce site destiné aux paranos. On ne peut pas poster sur Invisiblog via le Web, comme on le fait avec la plupart des autres outils de blog. On poste en utilisant un e-mail spécialement formaté, dont la signature chiffrée est créée par un système de re-mailer : MixMaster.
Sarah a eu un peu de mal à comprendre cette dernière phrase. Elle finit par mettre en place le GPG, exécution GNU de Pretty Good Privacy, un système de cryptage à clef publique. En deux mots, le chiffrement à clef publique est une technique qui permet d'envoyer des messages à une personne en étant à peu près certain qu'elle est la seule à pouvoir les lire, sans qu'elle ait pourtant à partager une clef secrète avec vous (ce qui vous permettrait de lire les messages qu'elle reçoit d'autres personnes). Le chiffrement à clef publique permet de « signer » des documents en utilisant une signature numérique qu'il est presque impossible d'imiter. Elle crée une paire de clefs qu'elle utilisera pour poster





sur le blog, en signant son message de sa « clef privée ». Invisiblog utilisera la « clef publique » de Sarah pour s'assurer que le message vient bien d'elle avant de le poster sur son blog. (Sur le cryptage des e-mails, voir également le chapitre « Comment protéger la confidentialité de vos e-mails »).
Ensuite, elle installe MixMaster, un système de messagerie qui sert à brouiller l'origine d'un e-mail. MixMaster utilise une chaîne de re-mailers anonymes – des programmes qui détruisent toutes les informations permettant d'identifier un e-mail avant de l'envoyer à son destinataire en toute sécurité. En utilisant une chaîne de 2 à 20 re-mailers, il est très difficile de retrouver l'origine d'un message, même si un ou plusieurs re-mailers sont compromis, ou d'enregistrer des informations concernant son expéditeur. Il faut qu'elle « construise » MixMaster en compilant son code source, un projet qui nécessite l'assistance des techniciens du coin.
Elle envoie un premier message MixMaster à Invisiblog avec sa clef publique. Invisiblog s'en sert pour installer un nouveau blog qui s'appelle « invisiblog.com/ac4589d7001ac238 », cette série de chiffre étant les 16 derniers octets de sa clef GPG. Ensuite, les prochains messages qu'elle enverra à Invisiblog contiendront un texte signé avec sa clef publique et seront envoyés via MixMaster. C'est loin d'être aussi rapide que le blog habituel. A cause des re-mailers de MixMaster, cela peut prendre entre 2 heures et 2 jours pour que son message arrive au serveur. Il faut qu'elle fasse très attention de ne pas aller sur le blog trop souvent, car son adresse risque d'être enregistrée par l'outil de blog, signalant ainsi qu'elle est certainement l'auteur de ce blog. Mais elle peut être rassurée par le fait que les propriétaires d'Invisiblog n'ont aucune idée de qui elle peut bien être.
Le plus grand problème avec le système Invisiblog, c'est que la plupart des gens le trouvent très compliqué à installer et ont du mal à comprendre comment utiliser des clefs publiques et privées. La plupart des outils de chiffrement faciles à utiliser, comme Ciphire, ont été installés pour aider les moins doués d'entre nous, mais même ceux-là s'avèrent parfois difficiles à utiliser. Résultat : très peu utilisent le cryptage même parmi ceux qui en ont vraiment besoin.
Une remarque : MixMaster est un véritable challenge pour la plupart des utilisateurs. Les utilisateurs de Windows ne peuvent se servir que d'une première version DOS du programme de téléchargement. Je l'ai fait, mais cela ne semble pas fonctionner … ou peut-être que mon e-mail est toujours en train d'être renvoyé entre les re-mailers. Toute personne désirant utiliser la nouvelle version ou souhaitant l'utiliser sur Linux ou sur Mac doit compiler le programme elle-même, une tâche que même les experts ont du mal à accomplir. Invisiblog serait certainement plus utile s'il commençait par accepter les messages des re-mailers accessibles par le Web, comme riot.eu .org. Pour l'instant, il n'est pas très pratique pour les gens qui en ont le plus besoin.
Le cryptage pose un autre problème dans les pays où le gouvernement applique une politique de répression. Si l'ordinateur de Sarah est saisi par le gouvernement et que ce dernier trouve sa clef privée, il aura la preuve que Sarah est l'auteur du blog controversé. Et dans les pays où le chiffrement n'est pas utilisé de façon courante, le simple fait d'envoyer des messages MixMaster, des messages mail très chiffrés, risque de suffire aux autorités pour qu'elles commencent à contrôler l'utilisation Internet de Sarah.

### QUE PEUT-ON DÉVOILER ? QUELLE EST LA LIMITE ?

La solution qu'a choisie Sarah, qui consiste à apprendre les rudiments du cryptage et de MixMaster, est-elle forcément la bonne solution pour vous ? Ou, en combinant les étapes 1 à 5, vous assurerez-vous un anonymat suffisant à votre activité ? Il n'y a pas une seule et unique réponse. Lorsqu'on s'engage sur le chemin de l'anonymat, il faut prendre en compte les conditions du pays, votre propre compétence technique et votre niveau de paranoïa. Si vous avez des raisons de croire que ce que vous postez risque de vous mettre en danger, et que vous êtes capables d'installer Tor, alors allez-y.
Dernier conseil, n'oubliez pas de signer vos messages sur le blog avec un pseudonyme !

**ETHAN ZUCKERMAN**

Ethan Zuckerman est un étudiant chercheur au Berkman Center for Internet and Society de l'école de droit de Harvard. Sa recherche porte sur les relations entre le journalisme citoyen et les médias conventionnels, en particulier dans les pays en développement. Il est le fondateur et l'ancien directeur de Geekcorps, une organisation à but non lucratif qui travaille sur les technologies éducatives dans les pays en développement. Il est également l'un des fondateurs de l'entreprise d'hébergement Tripod.





# CHOISIR SA TECHNIQUE POUR **CONTOURNER LA CENSURE**

**SOMMAIRE**



### LE FILTRAGE DES CONTENUS SUR INTERNET

Une technologie de filtrage des contenus sur Internet permet de contrôler l'accès aux données diffusées sur le Web. Bien que cette technologie ait initialement visé le niveau individuel, permettant notamment aux parents de limiter l'accès de leurs enfants à des contenus inappropriés, elle est maintenant largement déployée à des niveaux institutionnels et nationaux. Le contrôle de l'accès aux contenus sur Internet est devenu la priorité pour un certain nombre d'acteurs institutionnels comme par exemple des écoles, des bibliothèques ou des entreprises. Le filtrage se développe par ailleurs de plus en plus au niveau national. Ainsi, l'accès à certains contenus en ligne se voit bloqué pour des populations entières, souvent sans que ces restrictions soient expliquées ou justifiées.

Les technologies de filtrage reposent en général sur le blocage d'une liste de noms de domaine ou d'URL, mais elles sont souvent également associées à des systèmes basés sur

la recherche de mots-clés permettant de bloquer les contenus de façon dynamique. Ces listes sont compilées et triées par catégories avant d'être chargées dans un logiciel de filtrage qui peut être configuré de façon à ne bloquer que certaines catégories. Quand les utilisateurs tentent d'accéder à une page Web, le logiciel vérifie sa liste de sites interdits et bloque l'accès à toute page qui s'y trouve. Si la censure par mots-clés est activée, le logiciel contrôlera chaque page (le domaine, l'URL et/ou le contenu même de la page demandée) et en bloquera l'accès de façon dynamique si l'un des mots-clés interdits y figure.

Les systèmes de filtrage présentent par nature deux défauts : le « sur-blocage » et le « sous-blocage ». En effet, les technologies de filtrage rendent souvent inaccessibles des contenus qui ne devraient pas figurer sur leur liste noire tout en laissant passer de nombreuses pages qu'elles auraient dû interdire. Toutefois, le principal problème est le secret entourant la création des listes de sites bloqués. Bien qu'il existe des listes ouvertes et accessibles (en « open source ») – se concentrant essentiellement sur la pornographie –, les listes noires commerciales ainsi que celles utilisées au niveau national restent le plus souvent secrètes. Les listes commerciales sont la propriété de leurs concepteurs et ne sont pas rendues publiques. Bien que certains fabricants de logiciels de filtrage mettent en ligne des systèmes permettant de contrôler les URL bloquées, la liste noire est, dans son ensemble, indisponible pour une vérification et une analyse indépendantes.

Les Etats mettent souvent en place des listes noires qui s'ajoutent à celles créées par les entreprises privées. Ces ajouts visent notamment des partis politiques ou des journaux d'opposition, des organisations de droits de l'homme, des agences de presse internationales et, d'une manière générale, les contenus qui sont critiques vis-à-vis des gouvernements concernés. La plupart des pays se concentrent sur le filtrage des contenus en langue locale et visent de plus en plus les espaces de discussion en ligne, comme les blogs et les forums.

## LES TECHNOLOGIES DE CONTOURNEMENT

En réponse aux méthodes de contrôle et de filtrage mises en place par les Etats, de nombreuses « technologies de contournement » sont apparues afin de permettre aux internautes de passer outre à ces restrictions. Ces technologies ont été développées pour aider les citoyens et la société civile à se protéger de, ou à lutter contre, la censure et la surveillance du Net. En général, ces techniques fonctionnent en transmettant la requête d'un internaute vivant dans un pays qui filtre le Web via une machine intermédiaire qui n'est pas bloquée. Cet ordinateur récupère le contenu demandé par l'utilisateur, qui devrait être bloqué par les filtres, et le lui retransmet. Parfois, ces technologies peuvent être conçues spécifiquement pour contourner la censure dans un pays donné, ou pour lutter contre une technique spécifique de filtrage ; dans d'autres cas, les usagers adaptent des technologies existantes, mais qui n'avaient pas au départ cette finalité.

Certaines de ces technologies sont développées par des entreprises privées, d'autres par des groupes de hackers et d'activistes. Ces outils vont de petits scripts informatiques et de programmes très simples jusqu'à des protocoles réseaux point à point (peer-to-peer)





très développés. Compte tenu de la variété des technologies, les utilisateurs doivent être capables de peser les points forts et les faiblesses de chacune afin de choisir celle qui répond le mieux à leurs besoins.

Il faut différencier le « fournisseur de contournement » et son utilisateur. Le fournisseur de contournement est celui qui installe un logiciel sur un ordinateur situé dans une zone où le Web n'est pas filtré et rend le service disponible aux internautes vivant dans des pays qui censurent Internet.

Cet article vise à informer les utilisateurs des technologies de contournement des options disponibles et à leur indiquer comment évaluer quelle technique est la plus adaptée à leurs besoins. Cela nécessite de déterminer les besoins et la capacité des internautes (aussi bien ceux qui utilisent que ceux qui fournissent la technologie de contournement), en tenant compte également du niveau de sécurité de chaque outil. Un contournement efficace, sûr et simple, ne peut être obtenu qu'en associant la bonne technologie avec le bon utilisateur.

## DÉTERMINER LES BESOINS ET LA CAPACITÉ À UTILISER LA TECHNOLOGIE

Les technologies de contournement ont pour cibles des utilisateurs disposant de ressources et de niveaux d'expertise variables. Ce qui peut bien fonctionner dans un cas peut ne pas être la meilleure option dans un autre. Quand on sélectionne une technologie, il est important que son fournisseur et son utilisateur se posent les questions suivantes :

Quel est le nombre d'utilisateurs attendus et la bande passante disponible ? (pour le fournisseur de contournement et pour l'utilisateur)
Où est le principal point d'accès à Internet pour les utilisateurs attendus et pour quoi l'utiliseront-ils ?
Quel est le niveau d'expertise technique ? (pour le fournisseur de contournement et pour l'utilisateur)
Quelle est la disponibilité de contacts – fiables – qui vont fournir la technologie de contournement ? (pour l'utilisateur)
Quel est le niveau des sanctions possibles si l'utilisateur est pris alors qu'il utilise ce type d'outil ?
Quel risque court l'utilisateur de ce type de technologie ? (pour l'utilisateur)

### NOMBRE D'UTILISATEURS ET BANDE PASSANTE DISPONIBLE

Le fournisseur de contournement doit estimer le nombre d'utilisateurs pour lesquels son outil est prévu et le mettre en rapport avec la bande passante dont il dispose. L'utilisateur final doit aussi prendre en compte sa bande passante car la technologie de contournement ralentira son utilisation d'Internet.

Les personnes désirant faire fonctionner des proxies publics doivent envisager que leur proxy peut être utilisé par des personnes qui ne se trouvent pas dans des endroits soumis à la censure. Par exemple, il peut être utilisé pour télécharger des films, ce qui consom-

mera une très grande quantité de sa bande passante. De ce fait, il peut souhaiter restreindre l'accès à son proxy ou déterminer quelle est la bande passante maximale qu'il souhaite allouer à son système de contournement. Il existe différentes technologies qui permettent ce type de paramétrage.

#### POINT PRINCIPAL D'ACCÈS ET UTILISATEUR

Il y aura différentes options technologiques applicables selon l'endroit d'où l'utilisateur final se connecte à Internet et selon les services Web auxquels il souhaite accéder. Ainsi, par exemple, les utilisateurs qui accèdent à Internet à partir d'ordinateurs publics ou de cybercafés peuvent ne pas être en mesure d'installer n'importe quel logiciel et seront limités à des solutions intégralement accessibles en ligne. D'autres utilisateurs pourront vouloir utiliser des applications différentes de la simple navigation Web (HTTP), telles que le courrier électronique (SMTP) et le transfert de fichier (FTP) ; ils devront alors installer un logiciel sur leur poste de travail et modifier les réglages de leur ordinateur. Naturellement, ce type d'intervention nécessite un certain niveau de compétence technique.

#### NIVEAU D'EXPERTISE TECHNIQUE

Plus le niveau d'expertise technique est élevé (et le nombre d'utilisateurs limité) et plus les options de contournement augmentent. Les obstacles pour les utilisateurs non aguerris se situent dans la procédure d'installation et de réglage, ainsi que dans toutes les modifications de configuration qui doivent être réalisées quand on utilise certaines technologies. Cela s'applique à la fois au fournisseur de contournement et à l'utilisateur final. Une mauvaise utilisation de la technologie de contournement peut mettre les utilisateurs dans des situations à risques.

#### DISPONIBILITÉ DE CONTACTS DE CONFIANCE

Les utilisateurs finaux peuvent largement augmenter leurs options de contournement s'ils connaissent des personnes de confiance à l'extérieur de leur pays. Si un utilisateur n'a pas de contact fiable, ses options sont alors limitées aux options accessibles au public et si l'utilisateur peut trouver ces systèmes, ceux qui mettent en place le filtrage le peuvent aussi. Grâce à un contact de confiance, l'utilisateur final peut trouver une solution qui réponde à ses besoins spécifiques et ainsi éviter d'être repéré. Un contournement stable, de long terme et réussi, est grandement facilité lorsque l'on dispose de ce type de contact, dans un pays qui ne censure pas le Net.

#### LA SANCTION PÉNALE PRÉVISIBLE

Il est extrêmement important de connaître la sanction pénale à laquelle s'exposent les utilisateurs s'ils sont surpris en train d'utiliser une technologie de contournement. Les options seront différentes en fonction de la sévérité de la sanction. Si la sanction pénale encourue est limitée, les internautes peuvent choisir la technologie de contournement la plus efficace, même si celle-ci n'est pas très sûre. Si l'environnement est extrêmement





dangereux, il faut prendre soin d'utiliser une technique qui est à la fois discrète et sûre. Certaines de ces techniques peuvent même être utilisées sous couvert d'un prétexte légitime ou en brouillant les pistes.

#### LES PROBLÈMES DE SÉCURITÉ

Trop souvent, les utilisateurs sont encouragés à utiliser des technologies de contournement sans en connaître les risques et les faiblesses en termes de sécurité. Ces risques peuvent être réduits en déployant la bonne technologie, au bon endroit, et en l'utilisant correctement.

### LES SYSTÈMES DE CONTOURNEMENT EN LIGNE

Les serveurs proxies / changer les paramètres de son navigateur

Les systèmes de contournement en ligne sont des pages Web affichant un formulaire qui permet aux utilisateurs de saisir simplement une adresse URL et de laisser le système récupérer puis afficher le contenu de la page demandée. Il n'y a aucun lien entre l'utilisateur et le site Internet demandé : le système relaie de façon transparente la requête et permet à l'internaute de naviguer sans heurt sur des sites bloqués. Cette technologie réécrit les liens inclus dans la page Web demandée, de sorte que l'utilisateur peut continuer à naviguer normalement sur le Net. L'utilisateur final n'a pas besoin d'installer un logiciel ni de changer les réglages de son navigateur. Tout ce qu'il a à faire est de se rendre à l'adresse URL du système, saisir l'adresse qu'il souhaite visiter dans le formulaire en ligne et cliquer sur le bouton « Soumettre ». (Les systèmes de contournement en ligne peuvent avoir des aspects différents, mais leur fonctionnalité de base est la même). Ainsi, aucune expertise n'est requise et ce système peut être utilisé à partir de n'importe quel point d'accès, public ou privé.

**Avantages :**
Les systèmes de contournement en ligne sont faciles à utiliser ; il n'y a aucun programme à installer au niveau de l'utilisateur.
Lorsqu'ils sont publics, ces systèmes sont accessibles aux utilisateurs qui ne disposent pas d'un contact fiable dans un pays non soumis au filtrage.
Lorsqu'ils sont privés, ils peuvent être personnalisés pour répondre aux besoins spécifiques de chaque utilisateur et ces derniers ont moins de risque d'être découverts par les autorités.

**Inconvénients :**
Les systèmes de contournement en ligne sont souvent limités au trafic Web (HTTP) et peuvent ne pas accepter un accès crypté (SSL). Certains services Internet (tels que les webmails) nécessitant une authentification peuvent ne pas être pleinement fonctionnels.
Lorsque ce sont des systèmes publics, ils sont généralement connus des autorités et sont bloqués. La plupart de ces services sont rendus inaccessibles par des logiciels commerciaux de filtrage.
Dans le cas de systèmes privés, ils nécessitent que l'utilisateur ait un contact dans un endroit non soumis au filtrage. Idéalement, les deux parties doivent être en mesure de communiquer entre elles de manière confidentielle.

### LES SERVICES PUBLICS DE CONTOURNEMENT EN LIGNE

Il existe des logiciels de contournement en ligne ainsi que des services accessibles directement sur le Web. La plupart de ces services offrent une version limitée gratuite et une version comprenant davantage d'options – comme un accès crypté – disponible sur abonnement. Certains services sont gérés par des entreprises, d'autres par des volontaires.

**Quelques exemples de services de contournement en ligne :**

| | |
|---|---|
| http://www.anonymizer.com/ | http://www.guardster.com/ |
| http://www.unipeak.com/ | http://www.webwarper.net/ |
| http://www.anonymouse.ws/ | http://www.proximal.com/ |
| http://www.proxyweb.net/ | http://www.the-cloak.com/ |

Dans la mesure où les adresses Internet de ces services sont largement connues, la plupart des applications de filtrage, de même que les systèmes de censure installés au niveau national, les ont déjà incluses dans leurs listes noires. Or, si les adresses de ces services sont bloquées, ils ne peuvent pas fonctionner. Ensuite, certains de ces services ne cryptent pas le trafic entre le système de contournement et l'utilisateur final. Toute information transmise par l'utilisateur peut donc être interceptée par le fournisseur du service.

*Récapitulatif :*
*Les services publics de contournement en ligne sont les plus adaptés pour les utilisateurs vivant dans des environnements à faible risque qui ne disposent pas de contacts fiables dans des endroits non filtrés, qui ont besoin de ce type de service de manière ponctuelle et qui ne transmettent pas des informations sensibles.*





### LES LOGICIELS DE CONTOURNEMENT EN LIGNE

L'installation d'un logiciel de contournement en ligne peut nécessiter un certain niveau d'expertise technique et des ressources appropriées, notamment un serveur Internet et de la bande passante. L'emplacement de ce service privé de contournement n'est connu que des utilisateurs cibles, alors que les systèmes publics de contournement et les services anonymes sont également connus de ceux qui ont mis en œuvre le filtrage (entreprises commerciales et services de censure gouvernementaux). Les risques de détection et de blocage des systèmes privés de contournement sont inférieurs à ceux des services publics.

Les systèmes privés de contournement peuvent être réglés et personnalisés pour répondre aux besoins spécifiques de l'utilisateur. Il est par exemple possible de modifier le numéro du port que le serveur utilise et d'utiliser une technologie de cryptage. Le protocole SSL (Secure Sockets Layer) est utilisé pour transmettre des données de façon sécurisée sur le Net. Il est souvent utilisé par les sites qui transmettent des informations sécurisées, comme des numéros de carte de crédit. On accède aux pages Web qui proposent ce système SSL via une requête « https », à la place de l'habituel « http ».

Une autre option pour l'utilisation de SSL est de créer une page d'apparence anodine à la racine du serveur Web et de masquer le système de contournement grâce à un chemin d'accès et un nom de fichier aléatoires. Bien qu'un intermédiaire puisse identifier le serveur auquel l'utilisateur se connecte, il ne sera pas capable de déterminer la page Web à laquelle il accède car cette partie de la requête est cryptée. Si, par exemple, un utilisateur se connecte sur « https://example.com/secretcircumventor/ », un intermédiaire sera capable de déterminer que l'utilisateur s'est connecté à example.com mais ils ne saura pas que l'utilisateur a utilisé un système de contournement. Si le gestionnaire du système de contournement crée ce type de page Web d'apparence anodine sur example.com, il ne sera pas possible de découvrir le système de contournement, même en cas de surveillance.

- Proxy CGI : un script CGI agit comme un proxy HTTP ou FTP.
  http://www.jmarshall.com/tools/cgiproxy/
- Le système de contournement Peacefire : un programme d'installation automatisé qui rend beaucoup plus facile l'installation et la configuration du proxy CGI pour des utilisateurs non expérimentés.
  http://www.peacefire.org/circumventor/simple-circumventor-instructions.html
- proxy pH : système de contournement expérimental entièrement paramétrable.
  http://ice.citizenlab.org/projects/phproxy/
- Psiphon : serveur Web disposant de la fonctionnalité SSL et d'un système de contour nement en ligne intégré.
  http://Soon to be released (annoncé bientôt)

*Récapitulatif :*
*Des systèmes de contournement privés en ligne, autorisant le cryptage, sont les plus adaptés pour les utilisateurs qui ont besoin d'un service de contournement stable et qui ont des contacts fiables dans un pays non soumis au filtrage – ces derniers devant eux-*

*mêmes disposer de compétences techniques suffisantes et d'une bande passante disponible permettant de régler et de maintenir le système de contournement. Il s'agit de l'option de contournement la plus souple. Elle est idéale pour surfer sur Internet et c'est la solution qui a le moins de chance d'être découverte et bloquée.*

### LES SYSTÈMES DE CONTOURNEMENT EN LIGNE : PROBLÈMES DE SÉCURITÉ

Il est à noter que les systèmes de contournement n'assurent pas nécessairement l'anonymat. L'identité des utilisateurs est masquée des responsables des sites visités. En revanche, si la requête entre l'utilisateur et le fournisseur de contournement n'est pas cryptée (requête HTTP), comme c'est souvent le cas pour les services gratuits, son contenu peut alors être facilement intercepté et analysé par un intermédiaire, par exemple un fournisseur d'accès à Internet (FAI). Aussi, bien que le contournement ait réussi, les autorités peuvent toujours pister l'utilisateur et découvrir qu'il a utilisé un système de contournement en ligne. De plus, elles peuvent déterminer quels contenus – y compris les sites que l'utilisateur a visités – ont été échangés entre le système de contournement et l'utilisateur final.

Les systèmes de contournement en ligne non cryptés utilisent parfois un brouillage de l'URL (Uniform Resource Locators) pour contrer les techniques de filtrage qui recherchent les mots-clés dans l'URL. Par exemple, avec l'utilisation d'une technique simple comme ROT-13, où une lettre est remplacée par la lettre située treize places plus haut dans l'alphabet, l'URL http://ice.citizenlab.org devient uggc://vpr.pvgvmrayno.bet/. Le texte de l'URL est encodé de telle sorte que les mots-clés que recherche la technologie de filtrage ne seront pas trouvés dans l'URL qui est demandée par le système de contournement. Toutefois, le contenu de la session peut toujours être « reniflé » (intercepté), même si le contournement a réussi.

Il existe également des risques associés à l'utilisation des cookies et des scripts. De nombreux systèmes de contournement en ligne peuvent être configurés pour supprimer les cookies et les scripts, mais de nombreux sites (par exemple les webmails) nécessitent leur utilisation. Un autre risque est lié à l'utilisation de services nécessitant un nom d'utilisateur et un mot de passe. Dans ce cas, l'internaute accède au système de contournement via une connexion en clair puis utilise le système pour faire une demande d'information à partir d'un serveur crypté. Dans ce cas de figure, le système de contournement récupère l'information demandée à partir du serveur actif SSL via une transmission cryptée, mais envoie ensuite son contenu en clair à l'utilisateur, exposant ainsi les données sensibles à une possible interception.

Certaines de ces questions de sécurité peuvent être résolues en utilisant des proxies via une connexion cryptée. Certains proxies sont configurés pour qu'on y accède en SSL (HTTPS), ce qui crypte la connexion dès le départ, c'est-à-dire entre l'utilisateur et le système de contournement. Dans ce cas de figure, des tiers ne peuvent qu'observer le fait que l'utilisateur s'est connecté à un système de contournement mais ils ne peuvent pas déterminer quels contenus ont été téléchargés. Il est très fortement recommandé aux utilisateurs de s'assurer qu'ils emploient un système de contournement utilisant SSL si les risques d'interception sont importants.





Cependant, bien que la connexion de l'utilisateur au système de contournement puisse être sécurisée, il faut garder à l'esprit que toute information passant par un système de contournement peut être interceptée par celui qui a mis en place ce système.

Les archives du système de contournement constituent un problème de sécurité supplémentaire. Selon la localisation du système de contournement ou de son serveur, les autorités peuvent en effet avoir accès à son historique et à ses archives électroniques.

Il existe encore d'autres problèmes dont les utilisateurs doivent être informés quand ils utilisent un système de contournement en SSL. En premier lieu, l'utilisation du cryptage peut attirer l'attention sur les activités de l'internaute qui utilise ce système, et ne pas être légale partout. Deuxièmement, les autorités assurant le filtrage ont la possibilité de déterminer quels sont les sites qui ont été visités grâce au contournement, même lorsqu'un cryptage SSL est utilisé, en recourant à des techniques connues sous les noms de « prise d'empreinte » HTTPS et d'attaques dites de « l'homme du milieu » (MITM ou Man in the Middle). Toutefois, les pages ayant un contenu dynamique ou les systèmes de contournement qui ajoutent au hasard du faux texte et de fausses images au contenu demandé peuvent rendre ces techniques d'interception inefficaces. Si les utilisateurs disposent de l'« empreinte » – ou signature sécurisée – du certificat SSL, ils peuvent vérifier manuellement que celui-ci est bien authentique et ainsi éviter une attaque de « l'homme du milieu » (1).

### LES SERVEURS PROXIES

Un « serveur proxy » est un serveur situé entre un client (comme un navigateur Internet) et un autre serveur (en général un serveur Web). Le serveur proxy agit comme tampon entre le client et le serveur, et peut supporter une variété de demande de données comme le trafic Internet (http), les transferts de fichier (ftp) et le trafic crypté (SSL). Les serveurs proxies sont utilisés par des individus, des institutions et des Etats pour toutes sortes de raisons dont la sécurité, l'anonymat, la mise en cache et le filtrage. Pour utiliser un serveur proxy, l'utilisateur doit configurer les paramètres de son navigateur avec l'adresse IP et le nom du serveur proxy ainsi qu'avec le numéro de port

**1** Pour davantage de renseignements sur les attaques potentielles contre les systèmes de contournement, reportez-vous à la « liste des faiblesses possibles des systèmes destinés à contourner la censure sur Internet », de Bennett Haselton (« List of possible weaknesses in systems to circumvent Internet censorship »). Disponible à l'adresse suivante : http://peacefire.org/circumventor/list-of-possible-weaknesses.html et à la réponse de Paul Baranowski : http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

utilisé par le serveur. Bien que cela soit relativement simple, il peut s'avérer impossible de modifier les réglages du navigateur à partir de points d'accès publics à Internet tels que des bibliothèques, des cybercafés ou sur les lieux de travail (sur les serveurs proxies, voir également le chapitre « Comment blogger de manière anonyme »).

**Avantages :**
On peut choisir parmi de nombreux logiciels capables de relayer le trafic http de façon transparente et pouvant être configurés pour fonctionner sur des ports non standards.
Il existe pléthore de serveurs proxies accessibles au public.

**Inconvénients :**
La plupart des serveurs proxies n'acceptent pas le cryptage par défaut, si bien que le trafic entre l'utilisateur et le proxy n'est pas sécurisé.
L'utilisateur doit avoir les autorisations nécessaires pour modifier les paramètres de son navigateur et si le FAI exige que tout le trafic passe par son propre serveur proxy, il peut s'avérer impossible d'utiliser un serveur proxy ouvert.
La recherche et l'utilisation de serveurs proxies publics peut être illégale et ces derniers peuvent être bloqués par les autorités.

### LES LOGICIELS DE SERVEUR PROXY

Un logiciel de serveur proxy peut être installé par des contacts de confiance disposant d'un certain degré de compétence technique et basés dans un pays qui n'est pas soumis au filtrage. Le logiciel de serveur proxy doit être mis en place sur un ordinateur disposant d'une grande bande passante et doit être configuré pour utiliser une technologie de cryptage. Cela est particulièrement utile lorsqu'un bureau ou une petite organisation a besoin d'une solution de contournement stable. Bien qu'il ne s'agisse pas de la solution de contournement la mieux cachée, les serveurs proxies privés représentent une solution plus stable et efficace que les systèmes de proxies en ligne. Ils sont également préférables pour accéder aux sites nécessitant une authentification ou l'installation d'un cookie, comme les webmails. Les serveurs proxies peuvent également être personnalisés pour répondre aux besoins spécifiques de l'utilisateur et s'adapter à l'environnement local de filtrage.

- Squid est un logiciel libre de serveur proxy qui peut être sécurisé avec Stunnel server.
  http://www.squid-cache.org/
  http://www.stunnel.org/
  http://ice.citizenlab.org/projects/aardvark/
- Privoxy est un proxy qui permet de protéger efficacement ses informations personnelles.
  http://www.privoxy.org/
- Secure Shell (SSH) a un proxy sock intégré ($ ssh -D port secure.host.com)
  http://www.openssh.com/
- HTTPport/HTTPhost





*Récapitulatif :*
*Les serveurs proxies privés autorisant le cryptage sont les plus adaptés pour des groupes, ou des utilisateurs dans un environnement de travail, qui ont besoin d'une solution de contournement permanente et stable. L'utilisateur doit disposer de contacts fiables, compétents techniquement, qui ont une bande passante suffisante et qui sont situés hors du pays, pour installer et assurer la maintenance du serveur proxy.*

### LES SERVEURS PROXIES ACCESSIBLES AU PUBLIC

Les proxies ouverts sont des serveurs qui sont volontairement ou involontairement laissés ouverts pour servir de relais à d'autres ordinateurs pour se connecter à Internet. On ne sait jamais si les proxies ouverts ont été réglés dans le but d'être utilisés par le public ou s'ils ont été simplement mal configurés.

MISE EN GARDE : Selon certaines législations nationales, l'utilisation d'un serveur proxy ouvert peut être considérée comme un « accès non autorisé » et les utilisateurs de serveurs proxies ouverts peuvent ainsi être l'objet de poursuites judiciaires. L'utilisation de proxies ouverts n'est donc pas recommandée.

#### Localiser les proxies ouverts

De nombreux sites proposent des listes de proxies, mais ces listes ont une durée de vie limitée et ne sont pas forcément fiables. Rien ne garantit que les proxies sont toujours actifs et que les informations les concernant, en particulier leur degré d'anonymat et leur localisation géographique, sont exactes. Vous utilisez donc ces services à vos risques et périls.

**Sites fournissant des listes de proxies ouverts :**

http://www.samair.ru/proxy/
http://www.antiproxy.com/
http://tools.rosinstrument.com/proxy/
http://www.multiproxy.org/
http://www.publicproxyservers.com/

**Logiciel : ProxyTools/LocalProxy**

http://proxytools.sourceforge.net/

### Les Proxies ouverts : ports peu fréquents

Certains pays effectuant un filtrage au niveau national bloquent l'accès aux ports proxies standards. Un « port » est un point d'entrée de connexion utilisé par des protocoles spécifiques. Certains services Internet utilisent des numéros de ports non standards. Les numéros de ces ports sont généralement attribués par une organisation spécialisée, la Internet Assigned Numbers Authority (IANA). Le port 80 est, par exemple, réservé au trafic HTTP. Quand vous accédez à un site avec votre navigateur, vous vous connectez en fait à un serveur Internet fonctionnant sur le port 80. Les serveurs proxies ont également des ports qui leur sont attribués par défaut. Pour les bloquer, de nombreuses technologies de filtrage ne permettront pas l'accès à ces ports. Un contournement réussi peut donc nécessiter l'emploi d'un proxy qui a été configuré pour fonctionner sur un port non standard.

http://www.web.freerk.com/proxylist.htm

### LES SERVEURS PROXIES : PROBLÈMES DE SÉCURITÉ

La configuration des serveurs proxies est extrêmement importante, car elle conditionne la sécurité et l'anonymat de la connexion. En l'absence de cryptage, les serveurs proxies peuvent transmettre des informations sur l'utilisateur au site de destination, ces données pouvant notamment servir à identifier l'adresse IP de son ordinateur. En outre, toute la communication entre vous et le serveur proxy est en clair et ainsi peut être facilement interceptée par les autorités de filtrage. Toute information passant par les serveurs proxies peut également être interceptée par le propriétaire de ce serveur.

La recherche et l'emploi de proxies ouverts n'est pas recommandée. Ces serveurs sont souvent utilisés en raison de leur disponibilité, mais, s'ils sont efficaces pour contourner les mesures de filtrage, ils n'assurent pas la sécurité de l'utilisateur.

De même que les proxies en ligne, les serveurs proxies sont peu sûrs. Des scripts et cookies nocifs peuvent être transmis à l'utilisateur et, même s'ils sont utilisés avec une technologie de cryptage, les serveurs proxies peuvent faire l'objet d'attaques MITM et de prises d'empreinte HTTPS. Il faut également noter que certains navigateurs donneront accès à des informations sensibles quand ils se connectent à un serveur sock, un type particulier de serveur capable de manipuler d'autres types de trafics que le trafic Web. Quand on effectue une requête sur un site Internet, le nom de domaine est traduit en adresse IP ; certains navigateurs font cela localement si bien que la conversion se fait avant le passage par le serveur proxy. La requête de l'adresse IP sera alors prise en charge par les serveurs DNS (Domain Name System) situés dans le pays qui met en œuvre le filtrage, ce qui est dangereux pour l'utilisateur (2).

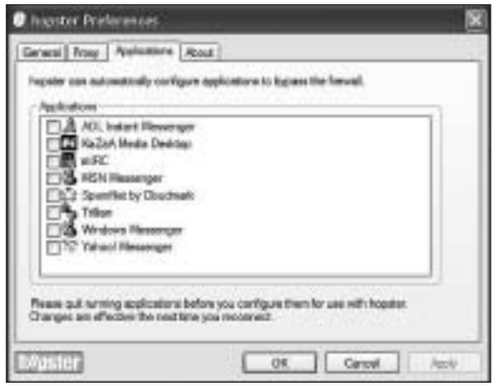
**2** Voir le site Tor pour plus d'informations : http://tor.eff.org/cvs/tor/doc/CLIENTS





*Récapitulatif :*
*Le recours à un serveur proxy accessible ouvert, c'est-à-dire accessible au public, n'est pas une option très sûre et ne doit être utilisée que par des personnes vivant dans des environnements où les risques d'interception des communications sont faibles. C'est une solution pratique pour les internautes qui ont des besoins temporaires de contournement ou d'anonymisation et qui n'ont pas besoin de transmettre des informations sensibles.*

### LE TUNNELING



Un logiciel de « tunneling »

Le tunneling, également connu sous le nom de « redirection de port », permet d'encapsuler un paquet d'informations non sécurisées ni cryptées à l'intérieur d'un protocole de cryptage. L'utilisateur situé dans un endroit soumis à la censure peut télécharger un logiciel client qui crée un « tunnel » vers un ordinateur situé dans un endroit non filtré. Les services normaux de l'ordinateur de l'utilisateur sont disponibles mais fonctionnent au travers d'un tunnel crypté qui passe d'abord par un ordinateur « ami », qui transmet ensuite les requêtes de l'utilisateur ainsi que leurs réponses. Il existe toute une série de produits de tunneling à disposition. Les internautes qui ont des contacts dans un pays non filtré peuvent mettre au point des services privés de tunneling. Ceux qui n'ont pas de contacts doivent passer par des services commerciaux de tunneling, habituellement payants et disponibles sur abonnement mensuel.

Les utilisateurs de services gratuits de tunneling doivent savoir qu'ils incluent souvent de la publicité. Les requêtes pour les publicités sont des requêtes http en clair qui peuvent être interceptées par les autorités, qui ont ainsi la possibilité de déterminer quel utilisateur a recours à un service de tunneling. En outre, de nombreux services de tunneling reposent sur l'utilisation de serveurs sock qui ne dissimulent pas les noms de domaines auxquels accède l'utilisateur.

http://www.http-tunnel.com/
http://www.hopster.com/
http://www.htthost.com/

**Avantages :**
*Les applications de tunneling assurent un transfert crypté sur le réseau.*
*Elles sont habituellement capables de transmettre de façon sécurisée de nombreux protocoles et pas seulement le trafic Web.*

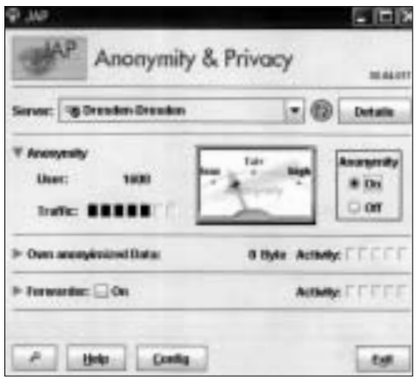
*Il existe des services commerciaux que les utilisateurs peuvent acheter s'ils n'ont pas de contacts dans des pays non soumis au filtrage.*

**Inconvénients :**
Les services commerciaux de tunneling sont connus de tous et peuvent être filtrés.
Ils ne peuvent pas être utilisés à partir de points d'accès publics, où les utilisateurs n'ont pas la possibilité d'installer le logiciel, comme les cybercafés ou les bibliothèques.
L'utilisation d'applications de tunneling peut demander des compétences techniques supérieures aux autres méthodes de contournement.

Les applications de tunneling s'adressent davantage à des utilisateurs compétents techniquement et qui ont besoin des services de contournement sécurisés (mais pas anonymes). Ces outils permettent d'utiliser des services autres que le seul trafic Web. Ils sont en revanche difficilement utilisables pour ceux qui utilisent des points d'accès publics au Réseau (cybercafé, bibliothèque, etc.). Les services commerciaux de tunneling sont une excellente ressource pour les internautes qui n'ont pas de contacts à l'étranger.

## SYSTÈMES DE COMMUNICATIONS ANONYMES

Les technologies de contournement et les systèmes de communications anonymes sont semblables et souvent entremêlés. Ils ont toutefois des objectifs différents. Les systèmes de communications anonymes veillent essentiellement à assurer la confidentialité de l'utilisateur en masquant son identité aux sites qu'il visite. De plus, les systèmes les plus évolués emploient différents systèmes de routage pour garantir que l'identité de l'utilisateur est masquée du système de communications anonymes lui-même. Les systèmes de contournement ne se concentrent pas forcément sur l'anonymat. Ils cherchent à fournir à l'utilisateur les moyens d'envoyer et de recevoir des informations sur le Web de la manière la plus sécurisée possible. Le contournement de la censure nécessite une technologie de communication sécurisée, mais celle-ci ne garantit pas nécessairement un anonymat complet.



Les systèmes de communications anonymes

Les systèmes de communications anonymes sont souvent utilisés pour contourner les filtres. L'un des avantages de ces systèmes est qu'ils se basent sur plusieurs réseaux auxquels il est possible de se connecter alternativement pour contourner la censure. Un autre est évidemment de pouvoir surfer sur le Net de façon anonyme.





Le logiciel d'anonymisation doit être installé sur l'ordinateur de l'utilisateur et certains demandent un certain degré de compétence technique. Le recours à ces systèmes est par ailleurs limité aux ordinateurs sur lesquels l'utilisateur a les autorisations appropriées d'installer ce type de logiciel. Les personnes qui accèdent à Internet via des terminaux publics, des bibliothèques ou des cybercafés seront très probablement incapables d'utiliser cette technique. Cette technologie peut également ralentir de manière significative votre connexion au Réseau.

Les internautes cherchant à contourner la censure s'apercevront également que les autorités en charge du filtrage prennent désormais des mesures pour bloquer l'utilisation des systèmes de communications anonymes. Si ces systèmes utilisent un port statique, le logiciel de filtrage peut être facilement configuré pour en bloquer l'accès. Plus le système de communications anonymes est connu et plus important est le risque qu'il soit bloqué. De plus, pour combattre des systèmes qui utilisent une technologie point à point, les autorités de filtrage peuvent simplement en refuser l'accès à leurs internautes. Les autorités de filtrage peuvent aussi mettre en place un nœud de connexion qui leur soit propre et tenter de contrôler l'utilisateur. Enfin, dans certains pays où Internet est contrôlé, l'utilisation de tels systèmes peut attirer l'attention sur les utilisateurs (3).

**Avantages :**
Les systèmes de communications anonymes assurent à la fois la sécurité et l'anonymat.
Ils ont généralement la capacité de transmettre de façon sécurisée de nombreux protocoles, et pas uniquement le trafic Web.
Ils sont parfois maintenus par une communauté d'utilisateurs et de développeurs qui peuvent fournir une assistance technique.

**Inconvénients :**
Les systèmes de communications anonymes ne sont pas spécifiquement conçus pour le contournement. Ils sont largement connus et peuvent être facilement filtrés.
Ils ne peuvent pas être utilisés à partir de points d'accès publics, où les utilisateurs ne peuvent pas installer de logiciel, tels qu'un cybercafé ou une bibliothèque.
Ils peuvent nécessiter un niveau assez élevé d'expertise technique.

• Tor est un réseau de tunnels virtuels qui permet à des personnes ou des groupes d'améliorer la confidentialité et la sécurité de leurs communications électroniques. Tor offre une base pour toute une série d'applications qui permettent à des organisations ou à des individus de partager des informations sur des réseaux publics sans compromettre la confidentialité de leurs communications.

**3** Pour plus d'informations sur les attaques potentielles contre les systèmes de contournement, reportez-vous à la « liste des faiblesses possibles des systèmes destinés à contourner la censure sur Internet », de Bennett Haselton (« List of possible weaknesses in systems to circumvent Internet censorship »), disponible à l'adresse suivante : http://peacefire.org/circumventor/list-of-possible-weaknesses.html. Et la réponse de Paul Baranowski : http://www.peek-a-booty.org/pbhtml/downloads/ResponseToLopwistcic.pdf

• http://tor.eff.org/
JAP permet de naviguer sur le Net de façon anonyme. Au lieu de se connecter directement à un serveur Web, les utilisateurs font un détour en se connectant de façon cryptée via plusieurs intermédiaires appelés « mixes ».

• http://anon.inf.tu-dresden.de/index_en.html
Freenet est un logiciel libre qui permet de publier et d'obtenir des informations sur Internet sans crainte de la censure. Il se base sur un réseau entièrement décentralisé où ceux qui publient ou utilisent les informations restent anonymes.
http://freenet.sourceforge.net/

*Récapitulatif :*
*Les systèmes de communications anonymes conviennent à des utilisateurs disposant de compétences techniques, qui ont besoin à la fois d'un service de contournement et d'anonymat, et qui utilisent d'autres services Internet que le simple trafic Web. Cette solution n'est pas adaptée pour ceux qui se connectent à partir de points d'accès publics.*

## CONCLUSION

La décision d'utiliser une technologie de contournement doit être prise sérieusement, en analysant soigneusement ses besoins, ses ressources et les risques inhérents aux différents outils. Les utilisateurs ont à leur disposition une grande variété de techniques. Cependant, l'utilisation de ces technologies pour un contournement stable et efficace de la censure dépend de toute une série de facteurs, parmi lesquels le niveau de compétence technique de l'utilisateur, les risques potentiels en termes de sécurité et les contacts disponibles à l'étranger. En outre, des Etats peuvent prendre des contre-mesures pour bloquer efficacement les technologies de contournement.

Les clés d'une possibilité de contournement stable et réussie sont la confiance et l'efficacité. Les systèmes de contournement doivent viser des utilisateurs spécifiques ou être facilement adaptables à leurs besoins. Ils doivent être sûrs, configurables et cachés. Un lien de confiance doit être établi entre le fournisseur de contournement et l'utilisateur, en tenant compte de l'environnement légal et politique dans lequel l'utilisateur travaille. Il faut également se tenir informé des limitations de chaque technologie de contournement.

**NART VILLENEUVE**

Nart Villeneuve est directeur de la recherche technique à Citizen Lab, un laboratoire interdisciplinaire basé au Centre Munk pour les études internationales, à l'université de Toronto (Canada). En tant que développeur de programmes et enseignant, il travaille actuellement sur l'initiative OpenNet (ONI : OpenNet Initiative), documentant les pratiques de surveillance et de filtrage de contenus Internet dans le monde. Il travaille également sur l'évaluation des technologies de contournement. Il s'intéresse par ailleurs à l'activité des hackers (l'hacktivisme), au cyberterrorisme et à la sécurité d'Internet. Nart Villeneuve a été récemment diplômé par l'université de Toronto dans le cadre du programme d'études sur la paix et les conflits (Peace and Conflict Studies).

Remerciements : Michelle Levesque, Derek Bambauer et Bennett Haselton.





# ASSURER LA CONFIDENTIALITÉ DE SES E-MAILS

La plupart des Etats ont aujourd'hui les moyens d'intercepter les communications électroniques. Les « cyberpolices » des pays répressifs ne se privent pas de cette possibilité pour identifier et arrêter les opposants politiques. De nombreux internautes ont ainsi été condamnés pour avoir envoyé ou parfois simplement transféré un e-mail. Aux Maldives, un dissident politique a été condamné à 15 ans de prison, en 2002, pour avoir correspondu par e-mail avec Amnesty International. En Syrie, un internaute est emprisonné depuis février 2003 pour avoir transféré un bulletin d'information électronique.

D'où ces quelques conseils pour assurer la confidentialité de vos échanges sur Internet.

Utiliser le compte e-mail proposé par un fournisseur d'accès Internet (AOL, Wanadoo, Free, etc.), ou par une entreprise, n'assure aucune confidentialité à vos échanges. Les propriétaires des réseaux sur lesquels transitent vos données peuvent intercepter très facilement vos communications. Lorsque les autorités d'un pays enquêtent sur un internaute, c'est par le biais de son fournisseur d'accès qu'elles accèdent, le plus souvent, à ses e-mails.

Un compte de type « webmail » (Yahoo , Hotmail…) est plus sûr puisqu'il n'utilise pas les serveurs d'un fournisseur d'accès local. Pour lire les messages d'un webmail, il faut par conséquent en forcer l'accès ou intercepter les e-mails alors qu'ils circulent sur le Réseau, ce qui est plus difficile techniquement. Malheureusement, cette protection est toute relative : si une police spécialisée ou un pirate informatique veut pénétrer votre webmail, il y parviendra.

La cryptographie (ou l'art d'écrire « caché ») est la principale technique utilisée pour assurer de manière effective la confidentialité de vos communications électroniques. Il existe deux méthodes de cryptographie.

## LA CRYPTOGRAPHIE CLASSIQUE

Alice et Bertrand, qui veulent échanger des messages secrets, conviennent entre eux d'un code de cryptage et de décryptage (une clé). Ensuite, ils s'échangent des messages en utilisant la clé dans un sens pour le cryptage, puis dans l'autre pour le décryptage.

Cette technique a toutefois un inconvénient. Si une troisième personne intercepte les messages dans lesquels Alice et Bertrand échangent leur clé de cryptage, elle pourra lire et même émettre de faux e-mails à destination de ces deux personnes. Par conséquent, pour que cette technique soit parfaitement sûre, il faut qu'Alice et Bertrand échangent leurs clés sans que celles-ci puissent être interceptées, en se rencontrant par exemple.

## LA CRYPTOGRAPHIE ASYMÉTRIQUE

Pour remédier à ce problème, il est préférable d'utiliser la cryptographie dite asymétrique. Deux clés sont alors nécessaires : une clé pour encrypter, une autre pour décrypter. La clé pour encrypter (appelée clé publique) peut être échangée sans danger sur Internet car elle ne permet pas de décrypter un message. La clé pour décrypter (clé secrète), elle, ne doit jamais être communiquée.

Avec la cryptographie asymétrique, Alice possède une paire de clés qui lui est propre (clé publique qu'elle diffuse et clé secrète qu'elle conserve). Alice envoie sa clé publique à Bertrand, qui l'utilise pour encrypter ses messages à destination d'Alice. Seule Alice, à l'aide de sa clé secrète, peut ainsi décrypter les messages de Bertrand. Doté lui aussi d'une paire de clés, Bertrand envoie sa clé publique à Alice, qui peut dès lors répondre à ses messages en toute confidentialité.

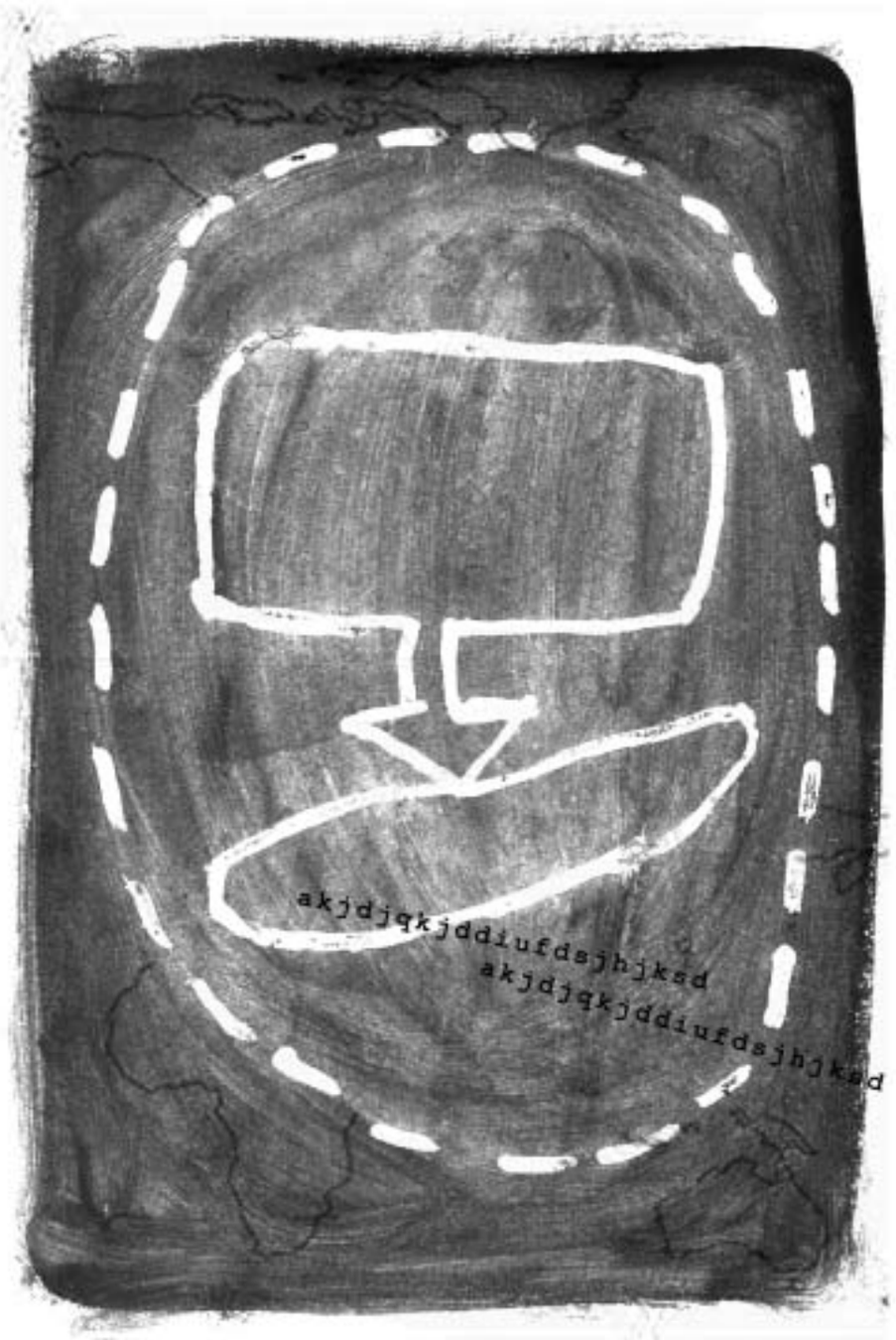
Toutefois, la clé publique étant échangée sur Internet sans protection particulière, il est recommandé de vérifier la validité de celle-ci auprès de son propriétaire. Pour ce faire, chaque clé publique possède une courte suite de caractères, appelée empreinte digitale, qu'il est facile d'échanger de vive voix ou par téléphone.

Une clé non vérifiée est peut-être une fausse clé émise par une troisième personne mal intentionnée, rendant le cryptage totalement inutile. Il est important de comprendre que toute la fiabilité de la cryptographie asymétrique repose sur la protection de la clé secrète, mais aussi de la vérification de la clé publique du correspondant.

OpenPGP (« Open Pretty Good Privacy ») est le standard de cryptographie asymétrique. La solution logicielle la plus utilisée pour créer, utiliser une paire de clés et gérer les clés publiques de ses correspondants est GnuPG (« GNU Privacy Guard »). Cette solution est utilisable aussi bien avec votre mailer (type Thunderbird ou Outlook) qu'avec un webmail ou encore une messagerie instantanée.
Téléchargez le logiciel GNUPG sur : http://www.gnupg.org/
Téléchargez le logiciel spécifique pour Windows : http://www.winpt.org/

**LUDOVIC PIERRAT**

Ludovic Pierrat est ingénieur en informatique. Il est directeur de la Wa Company, une entreprise de conseil et de réalisation en technologies de l'information.





# LES CHAMPIONS DE **LA CENSURE DU NET**

La plupart des régimes autoritaires de la planète cherchent aujourd'hui à contrôler les informations auxquelles accèdent leurs internautes. Ils parviennent de mieux en mieux à purger le Web de celles qui les dérangent, le plus souvent grâce à des technologies achetées à des entreprises américaines. Si l'on établissait un classement des censeurs du Réseau, la Chine serait sans conteste la championne du monde. Mais la compétition s'est faite plus rude ces dernières années. En matière de censure, chacun des pays de cette liste – qui est loin d'être exhaustive – a son style et sa tactique, mais tous n'ont qu'une idée en tête : garder le contrôle du jeu.

## LA CHINE : CHAMPIONNE DU MONDE !

La Chine a été l'un des premiers Etats répressifs à comprendre qu'elle ne pourrait pas se passer d'Internet et qu'il lui faudrait donc parvenir à le maîtriser. C'est un des rares pays à avoir réussi à aseptiser son Réseau, le purgeant de toute information critique du régime, tout en le développant. Quelle est la recette miracle de ce géant de la censure ? Un savant mélange d'investissement, de technologie et de diplomatie.
Pékin a investi des dizaines de millions de dollars pour s'équiper des meilleures technologies de filtrage et de surveillance du Réseau. Son système de filtrage est basé sur une liste noire de sites, mise à jour en permanence. L'accès aux publications « subversives » – un concept extensif allant de la pornographie à la critique politique, en passant par les sites pro-tibétains ou favorables à l'indépendance de Taïwan – est ensuite bloqué au niveau des grands nœuds de connexion (backbones) du Net chinois. Mais les capacités de censure des autorités vont bien au-delà de la simple liste noire. Le pouvoir est également en mesure de bloquer automatiquement les sites où sont repérés certains mots-clefs suspects – par exemple massacre + tiananmen.
La Chine a ensuite mis en place des systèmes lui permettant de censurer quasiment en temps réel les outils de discussion sur le Net. En alliant une cyberpolice pléthorique – on parle de dizaines de milliers de « cyberflics » – à des logiciels de censure sophistiqués, elle a réussi à vider les forums de discussion, très actifs il y a quelques années, de toute contestation politique. Un message appelant, par exemple, à des élections libres, dispose d'une durée de vie d'une demi-heure maximum. Les blogs ont également attiré l'attention du ministère de l'Industrie de l'Information (MII). Ce dernier a ainsi passé un accord avec

les outils de blog basés en Chine pour qu'ils censurent leurs utilisateurs. Résultat, un « post » sur le Dalaï Lama apparaîtra criblé de trous, le logiciel de censure remplaçant par un espace vide tout mot jugé « illégal ».
Mais comment la Chine a-t-elle pu se doter d'un arsenal technologique aussi efficace, alors qu'elle ne disposait il y a 10 ans d'aucune entreprise majeure dans le domaine d'Internet ? Avec l'aide des grandes entreprises américaines du secteur, Cisco en tête. Pour avoir leur part du juteux marché chinois – déjà plus de 100 millions d'internautes –, ces sociétés ont fermé les yeux sur l'usage qui était fait de leur technologie. Certaines ont même vraisemblablement collaboré directement à l'installation des systèmes de filtrage et de surveillance chinois. Pékin a même réussi à faire plier les grands moteurs de recherche étrangers. Yahoo ! a accepté il y a déjà plusieurs années de faire disparaître de sa version chinoise tous les résultats de recherche qui déplaisent au pouvoir. Google, qui s'y était longtemps refusé, semble aujourd'hui s'engager sur la même voie.
Enfin, la justice chinoise est sans pitié envers les éditeurs de sites qui ne respectent pas les consignes du Parti. Plus de 60 cyberdissidents sont actuellement emprisonnés pour avoir voulu diffuser une information indépendante sur le Réseau. Certains d'entre eux purgent des peines de plus de 10 ans.
Bref, avant de s'aventurer à créer un blog en Chine, mieux vaut se renseigner sur les consignes de sécurité à respecter. Chez ce champion du monde de la censure, les bloggers se doivent d'être malins et prudents.

## LE VIÊT-NAM : « DUR SUR L'HOMME »

En matière de contrôle du Réseau, le Viêt-nam suit très scrupuleusement l'exemple chinois. Toutefois, bien qu'encore plus rigide d'un point de vue idéologique, il ne dispose pas des capacités économiques et technologiques de son voisin. Le pays s'est doté d'une cyber-police, il filtre les contenus « subversifs » sur la Toile, surveille les cybercafés.
S'il existe toutefois un domaine dans lequel ce pays n'est pas à la traîne par rapport à la Chine, c'est bien la répression envers les cyberdissidents et les bloggers. Trois d'entre eux sont détenus depuis plus de trois ans pour avoir osé s'exprimer en faveur de la démocratie sur Internet.


Le président Ben Ali

## LA TUNISIE : LE MODÈLE

Le président Ben Ali, dont la famille dispose d'un monopole sur l'exploitation du Réseau, a mis en place un système très efficace de censure d'Internet. Toutes les publications de l'opposition tunisienne sont bloquées, de même que de nombreux sites d'information – comme le quotidien français *Libération*. Les autorités cherchent par ailleurs à dissuader les internautes d'utiliser des webmails, plus difficiles à surveiller que les comptes mails classiques (par Outlook, etc.). Accéder à Yahoo ! mail à partir d'un cybercafé tunisien peut prendre 20 minutes, et souvent se terminer par un message du type « délai de connexion dépassé » ou « page non trouvée ». Quant au site de Reporters sans frontières, inutile de le chercher sur le Web tunisien.
Malgré cela, la Tunisie reçoit les louanges de la communauté internationale pour sa gestion d'Internet. C'est en effet ce pays qui a été désigné par l'Union internationale des télécommunications (UIT), organisation du système des Nations unies, pour accueillir le Sommet mondial sur la société de l'information (SMSI), en novembre 2005. La Tunisie comme modèle de développement du Net… L'idée fait froid dans le dos.

## L'IRAN : CAPABLE DU PIRE… COMME DU PIRE

La censure du Réseau n'est pas l'apanage des régimes communistes d'Asie. Les systèmes de filtrage iraniens se sont également nettement améliorés ces dernières années. Le ministère de l'Information se targue aujourd'hui de bloquer l'accès à des centaines de milliers de sites. Les mollahs iraniens s'attaquent en priorité aux contenus touchant de près ou de loin à la sexualité mais ne tolèrent pas non plus les sites d'information indépendants.
Si Téhéran est capable du pire en matière de censure, il détient également le record de bloggers interpellés et emprisonnés de l'automne 2004 à l'été 2005 : près d'une vingtaine d'entre eux sont passés par les geôles du pays pendant cette période ; trois d'entre eux s'y trouvaient encore au 1er septembre 2005.


Fidel Castro

## CUBA : LA LÉGENDE

On savait le régime cubain expert en matière d'écoutes téléphoniques, on le découvre également performant en matière d'Internet. Le modèle chinois, développer Internet tout en le contrôlant, étant trop coûteux, Fidel Castro a choisi une méthode plus simple pour assurer son emprise sur ce médias : il a tout simplement tenu à l'écart du Réseau la quasi-totalité de sa population. A Cuba, accéder au Réseau est un privilège auquel très peu ont droit et qui nécessite une autorisation expresse du Parti unique. Même si on parvient à se connecter à la Toile, le plus souvent de manière illégale, c'est de toute façon à un Internet ultra-censuré qu'on accède. Bien peu savent pourtant que Cuba est l'un des pays les moins connectés du monde au Réseau, et que l'information en ligne y est aussi sévèrement contrôlée que dans les médias traditionnels. Pourquoi cet aveuglement ? Peut-être en raison du mythe encore tenace lié à la révolution cubaine.


Le roi Abdallah Ben Abdel Aziz Al-Saoud

### L'ARABIE SAOUDITE : DROIT AU BUT

En Arabie saoudite, la censure du net est affichée et revendiquée par les autorités. Pas de « page introuvable », comme en Chine, lorsqu'on tente d'accéder à un site interdit, mais un message clair indiquant que le site a été bloqué par les filtres officiels. L'agence gouvernementale chargée d'« assainir » le Web, l'Internet Service Unit (ISU), est fière d'annoncer qu'elle bloque près de 400 000 sites. Elle a même mis en place un formulaire en ligne permettant aux internautes de proposer de nouvelles pages Web à censurer. Selon les termes de l'ISU, l'objectif du filtrage est de « préserver les citoyens de contenus offensant ou violant les principes de la religion islamique et les normes sociales ».
On note d'ailleurs que, là encore, c'est une entreprise américaine, Secure Computing, qui a vendu à l'Arabie saoudite son système de filtrage.

### L'OUZBÉKISTAN : LE FEINTEUR

« Il n'existe aucune possibilité de censurer l'Internet du pays », a déclaré, en juin 2005, le ministre de l'Information ouzbek. Une telle affirmation fait sourire dans un pays où tous les sites d'opposition sont inaccessibles et où les journalistes en ligne sont régulièrement victimes de menaces et d'agressions.

**JULIEN PAIN**
Responsable du bureau Internet et Libertés de Reporters sans frontières





**REPORTERS SANS FRONTIÈRES**
Secrétariat international
5, rue Geoffroy-Marie – 75009 Paris, France
Tél. : 33 1 44 83 84 84
Fax : 33 1 45 23 11 51

Site Internet : **www.rsf.org**

Rédactrice en chef : Sylvie Devilette / devilette@rsf.org
Communication : Anne Martinez-Saiz / communication@rsf.org

Conception graphique : Nuit de Chine
Illustrations additionnelles : Marion Brosse pour Nuit de Chine
ndc@nuitdechine.com

ISBN : 2-915536-35-X

Achevé d'imprimer en août 2005
Inmprimé en France

Diffusion librairie : Dif'Pop'
21 ter, rue Voltaire – 75011 Paris
Tél. : 01 40 24 21 31. Fax : 01 40 24 15 88

Avec le soutien
du
**ministère français des Affaires étrangères**
et de
**la Caisse des dépôts et consignations**

**www.rsf.org**