GUIDE PRATIQUE DU **BLOGUEUR** ET DU **CYBERDISSIDENT**

REPORTERS SANS FRONTIÈRES

MARS 2008

REPORTERS SANS FRONTIERES
POUR LA LIBERTÉ DE LA PRESSE

GUIDE PRATIQUE **DU BLOGUEUR** ET DU **CYBERDISSIDENT**

REPORTERS SANS FRONTIÈRES

MARS 2008

REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE LA PRESSE

GUIDE PRATIQUE **DU BLOGUEUR** ET DU **CYBERDISSIDENT** **SOMMAIRE**

© 2008 Reporters sans frontières


le Mien

LES BLOGUEURS, **NOUVELLES SOURCES D'INFORMATIONS**

Les blogueurs inquiètent. Les gouvernements se méfient de ces hommes et ces femmes qui, sans être journalistes de métier, publient des informations. Pire, les blogueurs abordent parfois des sujets sensibles que les médias désormais qualifiés de "traditionnels" n'osent pas traiter. Les blogs sont devenus, dans certains pays, une source d'informations à part entière.

Près de 120 000 blogs se créent chaque jour sur la Toile. Certes, cette blogosphère ne renferme pas seulement des trésors d'audace et de vérité. Elle est aussi souvent source de confusions et de désinformation et tous les blogueurs ne se sentent pas l'âme de reporters. C'est pourquoi ce guide renferme des conseils pour créer un blog et le mettre à jour, sans autre prétention que celle de s'exprimer librement. Pour d'autres, il s'agit d'un combat pour attirer l'attention sur un sujet. La préoccupation première est alors de rendre sa publication visible (voir l'article de Jotman). Ce guide renferme des astuces pour être bien référencé sur la Toile (voir l'article d'Olivier Andrieu) ainsi que des recommandations plus "éditoriales" ("Faire sortir son blog du lot", de Mark Glazer).

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 blogueurs ?), c'est-à-dire fait "par le peuple et pour le peuple".

Les blogs sont plus ou moins maîtrisables pour qui veut les surveiller. Les gouvernements les plus en pointe en matière de nouvelles technologies ont recours aux techniques de filtrage ou de blocage les plus élaborés, empêchant toute visibilité sur la Toile. Mais les blogueurs ne se laissent pas faire. Leur sécurité devient une question essentielle. Avec une simple adresse IP, un blogueur peut être retrouvé et arrêté (voir "Comment bloguer de manière anonyme?").

Dans les pays où la censure est le mot d'ordre, les blogs sont parfois la seule source d'informations. Lors des événements de l'automne 2007, opposant les moines et la population à la junte militaire en Birmanie, les blogueurs ont été les principales sources

d'informations des journalistes étrangers. Leurs témoignages vidéos ont permis de constater l'ampleur de la protestation et la nature des revendications. Durant plus de deux mois, des marches ont été organisées dans les rues. Une répression massive s'est abattue sur les opposants, que seuls les Birmans étaient en mesure de montrer, tant il était difficile pour les rares journalistes étrangers qui parvenaient à entrer sur le territoire de revenir avec des images. Et les blogueurs ne pouvaient pas faire sortir leurs images sans contourner la censure imposée par le gouvernement sur Internet. Ce guide voudrait aider chaque blogueur à surmonter ces "trous noirs" de l'information. Sa deuxième partie est 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 blogueur devrait être capable de s'affranchir de la censure.

CLOTHILDE LE COZ
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, plus ou moins régulièrement
- 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 animé par une ou plusieur s personnes. Il peut également être anonyme.

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. Les commentaires peu vent être modérés
- 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.)

LEMONDEDUBLOG.COM

PETIT LEXIQUE DU BLOGGING

AGRÉGATEUR RSS
Logiciel ou service en ligne permettant au blogueur 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 dont le contenu peut être modifié facilement et rapidement par n'importe quel visiteur. Bien qu'il existe des points communs entre le blog et le Wiki, ce sont deux outils distincts.

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.

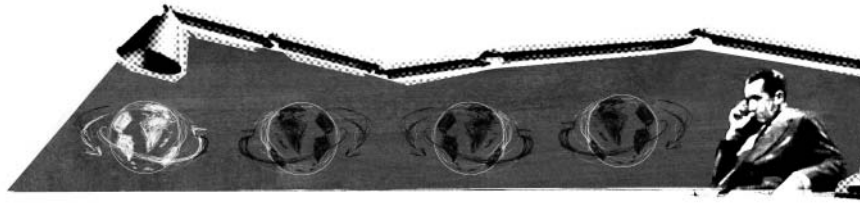
BLOGUEUR
Celui ou celle qui publie un blog.

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.

LEMONDEDUBLOG.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 : Wordpress »)

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.

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.

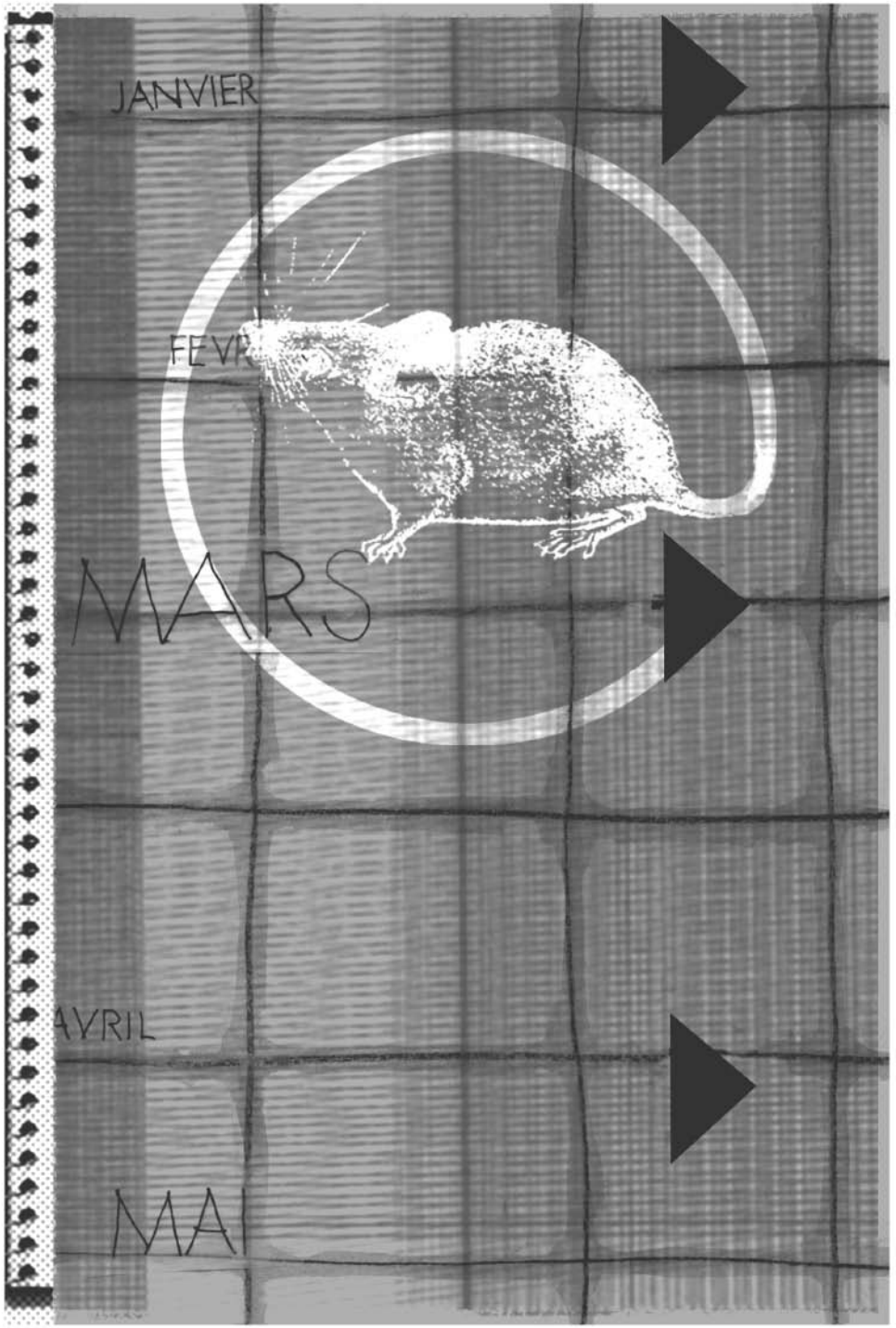
En matière d'outils à installer, les principaux blogiciels à considérer sont :

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

LEMONDEDUBLOG.COM

LeMondedublog.com est un blog quotidien consacré aux blogs, aux réseaux sociaux et au Web 2.0


BLOG
a M D i


JANVIER
FEVR
MARS
AVRIL
MAI

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

Pr sentation du syst me Wordpress (www.wordpress.com)

Wordpress est une plateforme de blogs très simple à utiliser, qui nécessite de télécharger un logiciel avant de créer un blog. Elle repose sur le modèle "blogware" (cf. Petit lexique du blogging"). C'est un projet "Open Source", ce qui signifie que des centaines d'internautes peuvent l'améliorer par leurs commentaires et suggestions diverses. Très facile d'accès, il est devenu l'un des logiciels de blogs les plus utilisés.

Il est cepedant indispensable de vous renseigner sur les fonctions de sécurité de cette plateforme. Pour en savoir plus, rendez-vous au chapitre "Comment bloguer de manière anonyme".

PAGE D'ACCUEIL DE WORDPRESS

A noter : Wordpress est disponible en plus de 120 langues (http://wordpress.com/languages/-). À chaque fois qu'un nouvel article est posté, la plateforme se met à jour automatiquement, grâce au flux RSS

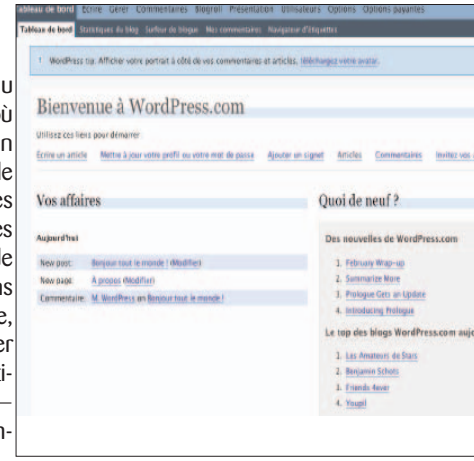
PAGE D'ENREGISTREMENT

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. Wordpress ne demande pas beaucoup d'informations (pseudonyme, mot de passe et adresse e-mail), ce qui permet de bloguer de manière anonyme si nécessaire. Une fois enregistré, l'internaute reçoit par e-mail les codes d'accès qui lui permettront de démarrer son blog, à l'adresse mail qu'il a indiqué à l'inscription.

CONNEXION AU SYSTÈME D'ADMINISTRATION

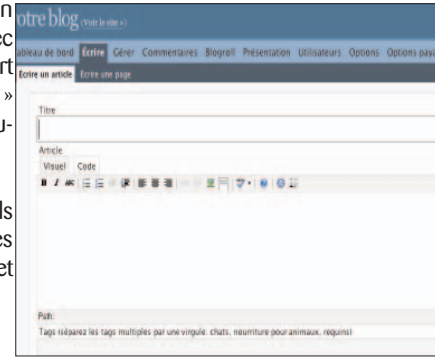
Le blog a une « face publique » qui est la page sur laquelle les visiteurs se rendent, et une « face privée » qu'on utilise pour sa mise à jour et son administration. On accède à la face privée en allant sur une page où l'on rentre le login et le mot de passe qu'on a reçus lors de la création du compte.

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'oeil de ce tout ce qui se passe sur le blog. On y trouve les messages, les commentaires et les « trackbacks » les plus récents. À 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 a mise en page Web.

Wordpress, comme la plupart des outils récents, permettent de modifier les polices des caractères, les tailles, les couleurs, et d'insérer des liens et des images.

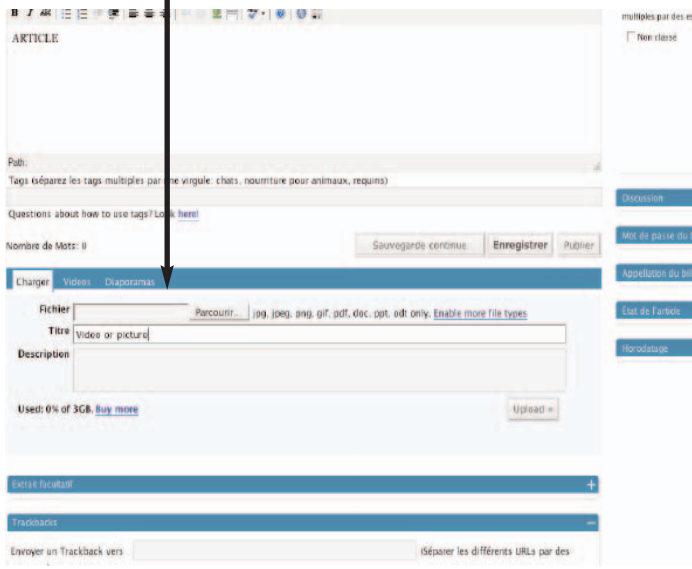
Les étapes pour poster un message :
1. se connecter au système d'administration
2. cliquer sur « écrire »
3. donner un titre à l'article et taper le contenu dans le corps de l'article
4. Mettre le texte en forme
5. assigner une catégorie au texte
6. cliquer sur enregistrer pour le sauvegarder. Votre article est dans les brouillons.
7. cliquez sur publier pour le mettre en ligne. Attention, si vous bloguez de manière anonyme, pensez à changez l'heure de publication avant de cliquer sur « publier ». Ainsi, peu importe l'endroit où vous êtes, on ne pourra pas vous taxer d'avoir publié cet article à ce moment. (rubrique « Post timestamp »)

LES « PINGS »

Un peu comme les « Poke » sur Facebook, les « pings » permettent à des sites Internet de signaler la mise à jour du vôtre. Ils sont importants pour augmenter la circulation sur un blog, car plusieurs sites Internet tiennent une liste des sites qui « pingent ». Cependant, ils peuvent être dangereux pour les blogueurs anonymes s'ils n'utilisent pas de logiciel qui modifient les adresses IP. Le principe est le suivant : signaler la mise à jour de votre blog en testant la présence de votre adresse IP sur le Réseau.

COMMENT PUBLIER UNE VIDEO

La publication de vidéo en ligne est de plus en plus fréquente et donne un aspect plus interactif à votre blog. Deux solutions s'offrent à vous. Soit vous disposez d'une vidéo sur votre ordinateur, que vous voulez publier. Soit il s'agit d'une vidéo disponible sur un site de partage de vidéos. Si c'est une vidéo que vous avez sur votre ordinateur, vous devez souscrire à la version payante de Wordpress et passer par WordPress.com Video Player. Si c'est une vidéo disponible sur une plateforme de publication de vidéos en ligne, cliquez sur vidéo et insérez le lien de la vidéo que vous avez choisi de publier sur votre blog.



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 « envoyer un trackbacks vers » et le «

trackback » sera automatiquement envoyé, quand le message sera enregistré, au site auquel on fait référence.

INSERER DES LIENS VERS VOS SITES PRÉFÉRÉS

Pour que les blogs de vos amis ou ceux que vous consultez régulièrement apparaissent sur le vôtre, cliquez sur « Blogroll » et ajoutez les adresses Internet des sites que vous voulez mettre en avant

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

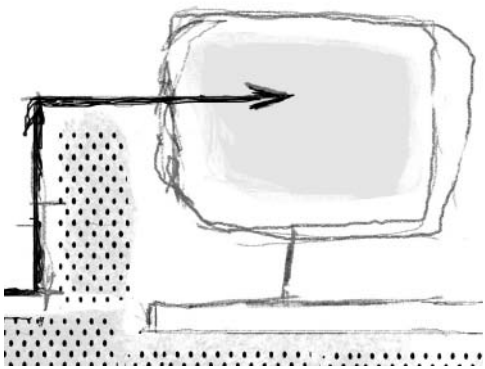
Civiblog Central Resources Blog :
http://central.civiblog.org/blog/BloggingResources

Comment bloguer :
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



les gens étaient affamés dans la rue, avec la police derrière eux

les gens étaient affamés dans la rue, avec la police derrière eux

QUELLE ÉTHIQUE POUR LES BLOGGERS ?

Tous les blogueurs 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

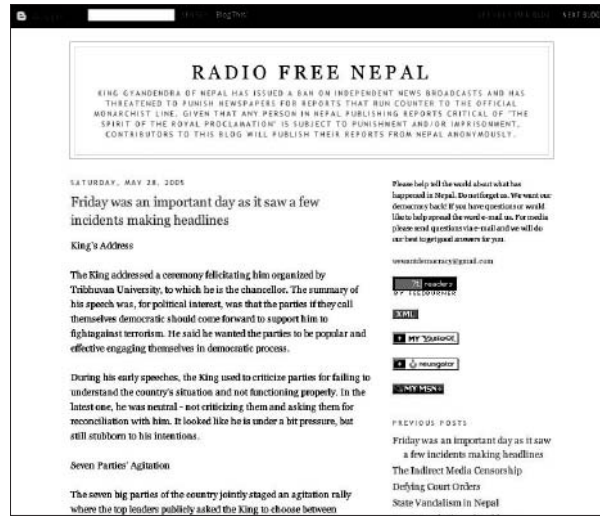
Les blogs étant des sites web à part entière, il est logique que l'on se pose à court terme la question de leur référencement sur les moteurs de recherche comme Google, Yahoo! Search ou MSN Search. En effet, un blog doit pouvoir obtenir une bonne visibilité sur ces moteurs pour les mots clés importants 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.

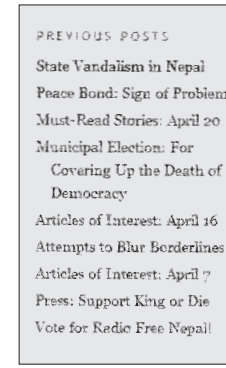
• Le titre du « post » est le plus souvent repris dans le titre de la page et dans son url (adresse). Exemple : pour le blog « Radio Free Nepal », qui est disponible à l'adresse http://freenepal.blogspot.com/, chaque « post » est disponible sur une page spécifique comme celle-ci (http://freenepal.blogspot.com/2005/04/state-vandalism-in-nepal.html)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



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) :

Pour limiter les résultats aux pages les plus pertinentes (total : 13), Google a ignoré certaines pages à contenu similaire. Si vous le souhaitez, vous pouvez relancer la recherche en incluant les pages ignorées.

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.

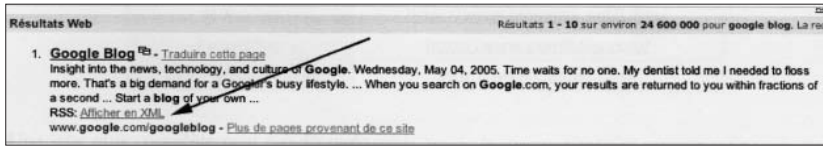
6. Ne proposez pas un titre trop long pour votre blog

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

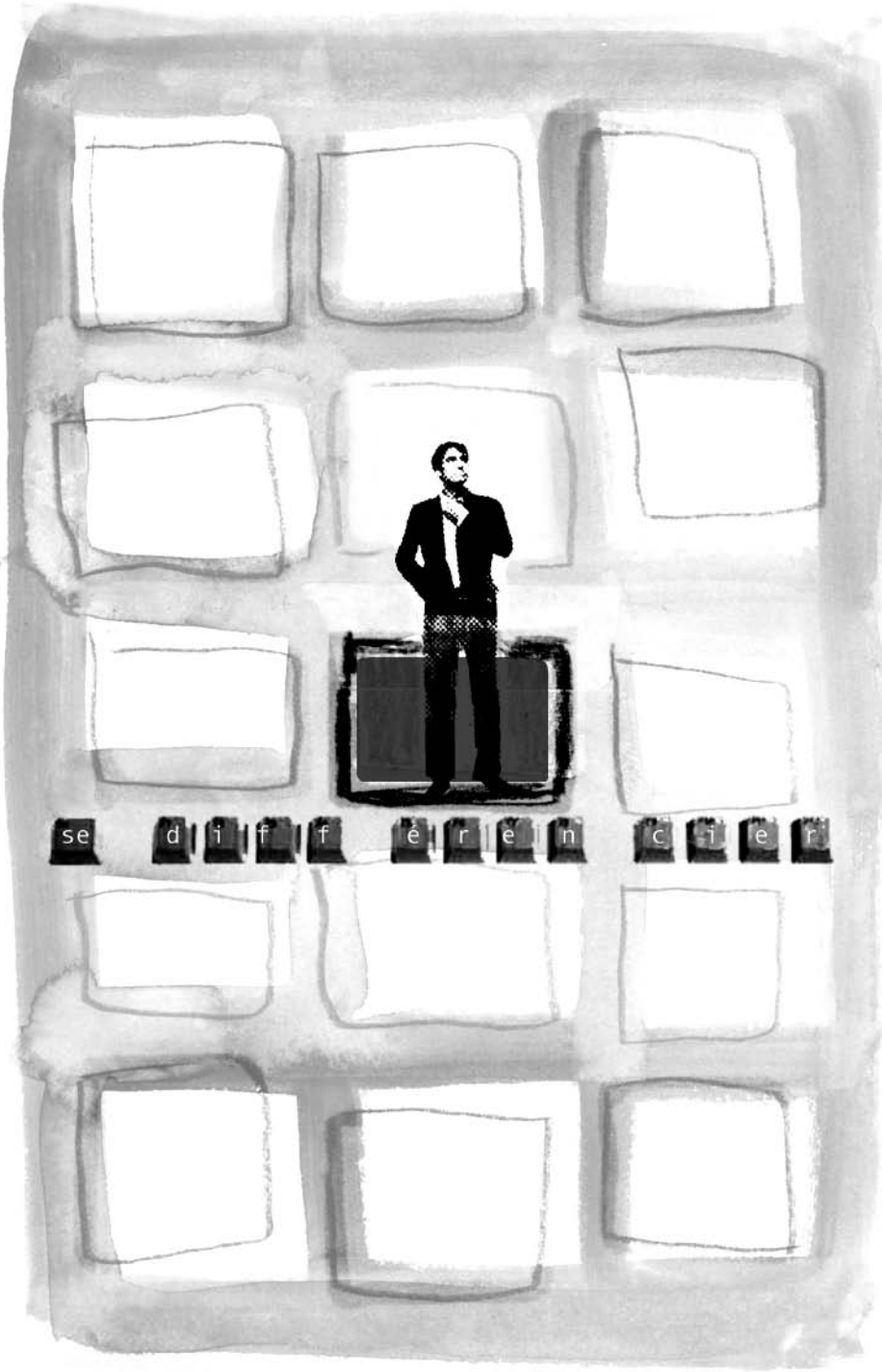
A explorer également, les annuaires de chaque prestataire de technologies, comme :
http://www.canalblog.com/cf/browseBlogs.cfm
http://www.dotclear.net/users.html
http://www.blogspirit.com/fr/communautes_blogspirit.html
Etc.

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.


se différencier

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.

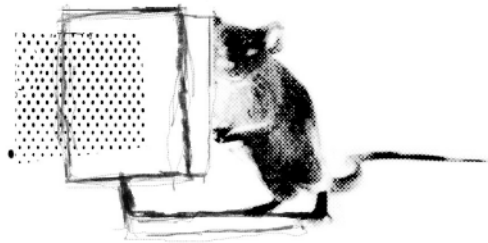
L'ACTUALISATION

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.

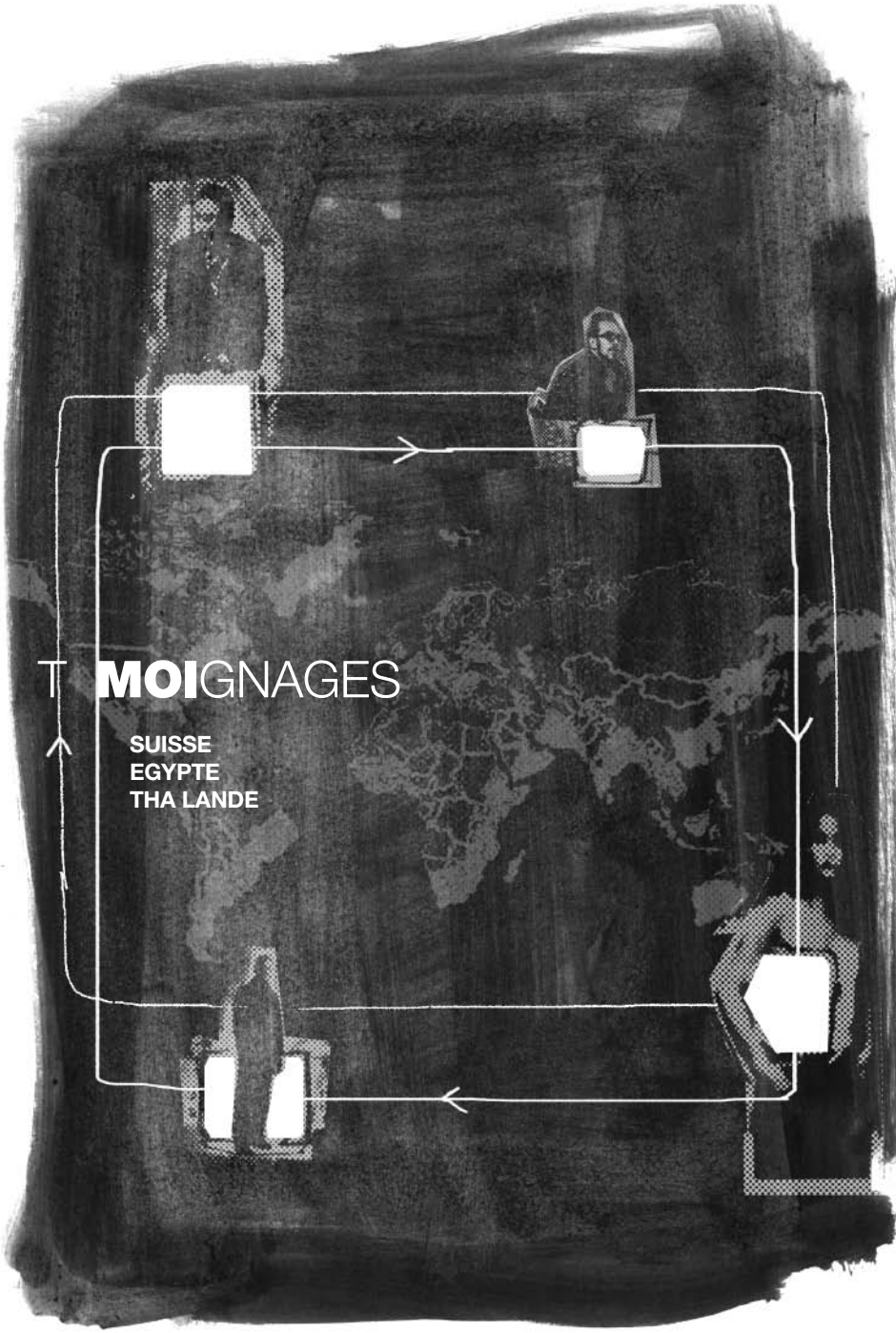


PARLER FRANCHEMENT

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.


T MOIGNAGES
SUISSE
EGYPTE
THA LANDE

SUISSE

˙ DES IMAGES POUR CONTOURNER LA CENSURE ¨

Picidae.net

Sur Internet, nous sommes habitués à côtoyer du texte. Alors nous avons choisi de prendre Internet en photos.

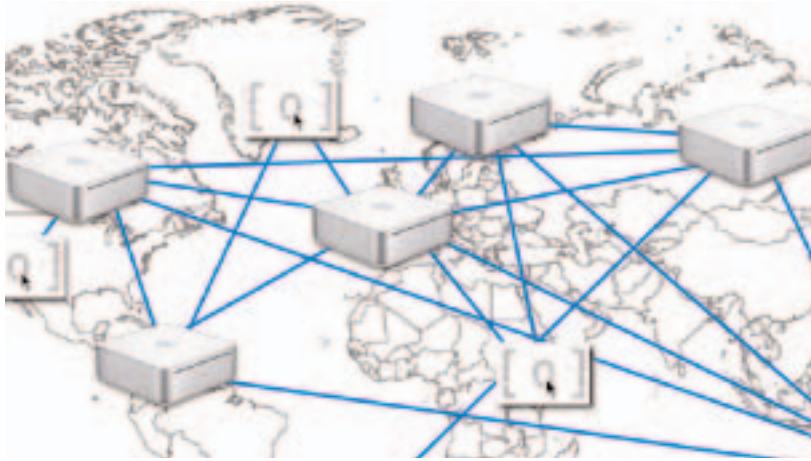
Ce signe symbolise Picidae. Choisissez : c'est un appareil photo stylisé ou une brèche dans un mur. "Picidae" vient du mot latin signifiant "le pic". Nous avons voulu faire référence aux pioches des Allemands de l'Est qui ont détruit le Mur de Berlin. Mais ce signe représente également le mode de fonctionnement de notre projet : prendre Internet en photos pour contourner la censure.

C'est d'abord un projet artistique. Regarder le monde à travers cette brèche, c'est se poser la question de savoir à quoi il ressemble derrière le mur. C'est une nouvelle manière de l'appréhender. Picidae est une nouvelle stratégie : trouver un moyen de contournement de la censure qui ne peut être filtré ou censuré. Cet outil se sert du Réseau tout entier et a été conçu pour reposer sur une communauté d'internautes. Comme Internet n'est pas centralisé, il permet des échanges en toute liberté. C'est pour cela que notre projet repose sur l'échange de données. Si l'accès à Internet est coupé pour certains, Picidae pourra donner d'autres points d'accès à ses utilisateurs et son activité ne sera jamais interrompue. C'est également une plateforme de communication, qui permet à chacun d'en améliorer la technique en faisant apart de ses commentaires.

Nous avons mis au point des serveurs "Pici", qui permettent à l'utilisateur de se connecter à Internet via un ordinateur qui n'est pas le sien. S'il fait appel à un serveur pici, un formulaire s'affiche et il peut y entrer une adresse web. Le serveur pici crée alors une image du site et vous la renvoie. Pour rendre le surf possible à partir de cette image, le serveur va analyser le site web, et intégrer un calque avec des zones cliquables à la place des liens. Tous les liens internet y sont reproduits (barre de menu, fonctions de recherche etc.). Il est donc possible de cliquer sur les liens de la même manière que sur un “vrai” site.

En prenant ces images, Picidae code les sites Internet ce qui ne laisse aucune chance de réussite au filtrage par "mot clé". Et pour que le mot "picidae" ne soit pas filtré, nous avons choisi un symbole, qui ne dépend d'aucune langue particulière. Cette image est universelle et peut déjouer le filtrage.
Pour empêcher la censure des requêtes des utilisateurs dans un serveur pici, les données entrées dans les formulaires sont cryptées avant d'être envoyées. Les systèmes de censure ne peuvent donc pas savoir ce que recherche une personne, ce qui permet de déjouer le contrôle des gouvernements.

Nous avons testé notre projet en Chine. Ce voyage au bout de l'Internet nous a montré à quel point la censure y est dissimulée. Les cybercafés sont surveillés et le réseau ultra-filtré. Les informations sur le Tibet, Taïwan, la critique politique ou les droits de l'homme sont



censurées. L'un des apects les plus importants de Picidae est de rendre la censure visible. Au travers des serveurs Pici basés à Zürich, nous avons pu accéder aux sites que nous voulions. Picidae est actuellement utilisé en Chine et en Europe et nous avons l'intention de l'exporter dans les pays arabes et en Afrique du Nord. Le système est libre et gratuit et ne demande aucune installation, login ou mot de passe.

Christoph Wachter et **Mathias Jud** sont les créateurs du projet.

Plus d'informations sur http://www.picidae.net
Serveur pici : http://pici.picidae.net/
Les proxies sont également disponibles à : contact@picidae.com :
Picidae est un système décentralisé et ne doit pas être accessible grâce à une base de données centralisée. Chaque point d'accès ou serveur fonctionne indépendamment des autres, et ne contient pas de nom ou de description, dans le but d'éviter la censure.

EGYPTE

˙ QUAND LA FRONTIØRE ENTRE LE JOURNALISTE ET LE MILITANT DISPARAºT ¨

Wa l Abbas

Le blogging a permis de repousser les limites de la liberté de la presse et celle de la liberté en général en Egypte. Certains considèrent même que les blogueurs ont réalisé en quelques jours ce que les organisations de défense des droits de l'homme n'ont pas réussi à faire en dix ans.

Fin 2004, les mouvements appelant au changement ont grossi leurs rangs à l'approche de l'élection présidentielle. Des manifestations ont été organisées, qui n'étaient pas couvertes par les médias traditionnels car elles demandaient le départ du Président. Les blogueurs ont donc pris le relais en publiant simplement des vidéos et des photos, pour rendre compte de la situation. J'ai même manqué d'être arrêté alors que j'essayais de prendre en photo des policiers qui s'en prenaient à eux.

Un jour, des avocats m'ont appris qu'un mandat d'arrêt avait été lancé contre moi car l'un des clichés que j'avais publiés sur mon blog montrait des agents de sécurité détruisant un drapeau de l'Egypte. Mais j'étais également accusé de faits que je n'avais pas commis : agression de forces de l'ordre, attaque d'employés, saccage d'établissements publics, etc. J'ai réussi à prouver qu'il n'y avait rien contre moi, mais ces accusations se sont répétées à chaque fois qu'une manifestation était organisée. Ironie de l'histoire : je n'ai pas assisté à la plupart des manifestations et j'étais même hors du pays quand elles ont eu lieu.

L'information relayée par les blogueurs émane des citoyens. Ils ont révélé la répression exercée lors de ces manifestations pacifiques, puis la falsification des résultats de l'élec-

tion et les actes de violences dans les commissariats contre des personnes qui ne faisaient l'objet d'aucune accusation. C'est là que la frontière entre le journaliste et le militant disparaît.

Quand j'ai relayé l'affaire "Imad Al-Kabir" (du nom d'un prisonnier) en publiant les vidéos montrant la torture des prisonniers dans les commissariats, j'ai eu l'information par des citoyens. C'est d'eux qu'elle émane. Cette affaire a été l'un des grands exploits de la blogosphère car ces vidéos, seulement publiées en ligne, ont servi de preuves lors du procès qui a condamné le policier Islam Nabih à trois ans de prison. Je suis cependant conscient du travail que les journalistes ont fourni pour découvrir l'identité des victimes de torture. Ce sont eux qui ont permis de déférer certains policiers devant les tribunaux.

Les médias traditionnels n'osent pas traiter ces sujets. Avant de diffuser les informations recueillies par les blogueurs, ils s'assurent qu'elles ne gêneront pas le gouvernement. Mais plusieurs journaux tentent parfois de s'approprier les enregistrements et les photos des blogueurs, souvent détenteurs d'exclusivité. La plupart du temps, ils n'en mentionnent pas la source. Plutôt que de subir cette situation, blogueurs et journalistes sont devenus collaborateurs. Une nouvelle forme de journalisme est née, qui allie les deux mondes.

Personnellement, je suis satisfait si le citoyen sait qu'un policier n'a pas le droit de l'agresser, si les victimes des tortures se mettent à parler, portent plainte et revendiquent leurs droits. Tout cela est nouveau pour l'Egypte car les services de sécurité ont réussi à cultiver la peur et les Egyptiens se sont habitués à souffrir en silence.

WAEL ABBAS

Wael Abbas est un des plus importants défenseurs des droits de l'homme en Egypte. Il vit au Caire et tient un blog (http://misrdigital.blogspirit.com) sur lequel il publié, début 2007, des vidéos dénonçant la torture de certains prisonniers dans les commissariats du Caire. Elles ont permis d'identifier les victimes et les auteurs de ces crimes mais également de sensibiliser la société sur les abus de pouvoir des policiers.


abcd efgh ijkl mop qrst
abcd efgh ijkl mop qrst

THAÏLANDE

˙ LE WEB N A PAS T PENS POUR LES BLOGUEURS ¨

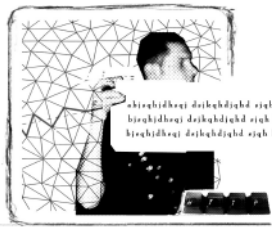
Jotman

J'ai plongé dans le monde des blogs à Bangkok, en 2006. Mon appareil photo à la main, j'étais assis dans un taxi qui me conduisait dans le quartier des tanks de l'armée chargés de surveiller les alentours des principaux bâtiments officiels. Il était un peu plus de minuit quand j'ai assisté aux vrombissements des motos qui menaient les généraux au pouvoir. A l'aube, les photos et les vidéos que j'ai publiées sur mon blog étaient parmi les premières du coup d'Etat thaïlandais à sortir des frontières et j'ai continué à bloguer en dépit des restrictions imposées sur la Toile par le régime militaire.

Évidemment, la Birmanie, la Chine et d'autres gouvernements pourront toujours bloquer l'accès à mon blog en traquant l'adresse URL, mais il pourrait être bloqué autrement. Les options de la plateforme que j'utilise, Blogger, sont quelque peu restreintes mais peu importe. A force de trop s'intéresser au design, on ne fait plus comprendre aux internautes qu'on a quelque chose à dire. Cette interface modeste me permet de me concentrer sur ce que j'écris.

Bloguer pour parler du quotidien peut revêtir différentes formes. Souvent, bloguer ressemble à "pinailler" – traquer les informations pour trouver la moindre imprécision ou un trésor de sagesse. Bloguer veut aussi dire informer – publier de l'information et montrer d'où elle vient. Lors de la crise birmane de septembre 2007, j'ai mesuré tout l'impact que mon blog pouvait avoir en rassemblant des informations sur la situation des blogueurs birmans et sur leur combat. Quand j'ai voulu vérifier les rumeurs concernant les blogueurs birmans et leurs conditions de vie, j'y suis allé. J'ai interviewé un bonze. Je me suis ensuite rapproché de la frontière thaïlandaise où je me suis entretenu avec plusieurs autres bonzes et des activistes démocrates. Mais bloguer c'est aussi publier un contenu original et multimédia. Parfois, un blog peut même être à l'origine d'un "scoop".

Les blogueurs traitent de sujets importants, mais n'ont pas assez d'audience. Le Web a beau être "grand comme le monde", il n'a pas été pensé pour les blogueurs. Il ne sait que chercher et répertorier l'information. Un moteur de recherche, quel pauvre outil pour attirer de nouveaux lecteurs! Rien à voir avec ce bon vieux journal qui expose des informations aux passants, qu'ils ne seraient sûrement pas allés chercher d'eux-mêmes. Sur Internet, chacun peut lire son journal idéal. Il n'y a plus de heureux hasard entre les lecteurs et l'information. Paradoxalement, à l'heure de la mondialisation, les événements sont toujours un peu plus liés les uns les autres mais les perspectives des lecteurs rétrécissent.



Il faudrait donc s'assurer que les blogs de qualité atteignent une audience plus large. Plusieurs étapes ont déjà été franchies au travers d'agrégateurs de blogs traduits en plusieurs langues (Global Voices, Wordpress etc). Wikipedia a également contribué à faire en sorte que les blogueurs acquièrent une certaine crédibilité. Mais même ce genre de site précurseur n'intéresse que les internautes aguéris ou spécialisés sur une région du monde. La société civile aurait tout à y gagner si elle y avait accès.

Les blogueurs trouvent souvent des informations intéressantes qui auraient également un intérêt pour ceux qui ne bloguent pas, qui ne sont ni spécialistes ni passionnés. Mais le Réseau fait en sorte de les cacher.

Jotman a voulu rester anonyme. Il a été l'une des principales sources d'informations sur la crise birmane et lauréat des BOB awards en 2007, un concours de blogs, auquel Reporters sans frontières s'est associé. Il a été récompensé pour son travail promouvant la liberté d'expression.

X

COMMENT BLOGUER **DE MANIÈRE ANONYME ?**

Un exercice pratique avec Tor et Wordpress

Il n'y a pas une seule et unique solution pour être un blogueur anonyme sur Internet. Lorsqu'on s'engage sur le chemin de l'anonymat, il faut prendre en compte les conditions de connexion du pays, sa compétence technique personnelle et son degré 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. Bloguer de manière anonyme est très contraignant et demande beaucoup de précautions. Ne le faites que si vous le devez réellement.

Dernier conseil, n'oubliez pas de signer vos messages sur le blog avec un pseudonyme !

Vous souvenez-vous de Sarah, qui, dans notre précédente édition, apprenait le B.A.BA du blogging anonyme ? Voici quelques petits rappels…

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 WordPress
Blogger : outil de blog gratuit de Google
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.

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 les autorités vérifieront l'adresse IP utilisée pour poster des messages sur le blog, elles découvriront que cela a été fait d'un cybercafé où les ordinateurs sont utilisés par beaucoup de monde et il leur sera difficile de l'identifier.
Cette stratégie a des inconvénients. Si le cybercafé 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 sur un poste public, parce que le veilleur se souviendra certainement de qui il s'agit. Elle devra changer souvent de cybercafé. En effet, si les autorités découvrent que tous les messages le concernant proviennent de l'Internet café « Chez Jojo, bières et snacks », dans la rue principale, elles risquent 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. Les autorités auront 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"). 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, par exemple, elle se connecte d'abord au proxy, qui lui-même se connecte à Hotmail. 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 les autorités ont les moyens d'accéder aux données enregistrées par tous les FAI du pays, elles risquent de découvrir que l'ordinateur de Sarah était l'un des seuls à avoir accédé à ce proxy particulier. Elle ne peuvent pas prouver que Sarah a utilisé le proxy pour aller sur un outil de blog. Mais elles peuvent 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.

Voici aujourd'hui comment résoudre les problèmes que Sarah a rencontrés jusqu'à maintenant au travers d'un exemple simple : naviguer avec Tor et bloguer avec WordPress.

ETAPE N°1 : CACHER SON ADRESSE IP

Chaque ordinateur a une adresse qui permet de l'identifier. Avant de publier quoi que ce soit, il est indispensable de la cacher, sans quoi l'identité du blogueur peut être dévoilée. Sarah craignait pour son identité car son FAI avait accès à son adresse IP, directement associée à son domicile ou son bureau.

Dans ce cas

1. Installez Firefox

Téléchargez ce logiciel sur le site de Mozilla (http://www.mozilla.org) et Installez le sur l'ordinateur que vous utilisez pour bloguer.

Pourquoi Firefox plutôt qu'Internet Explorer ? Explorer connaît des failles dans sa sécurité qui ne garantissent pas l'anonymat le plus sûr en toutes circonstances (http://www.schneier.com/blog/archives/2005/12/internet_explor.html).

2. Installez TOR

Téléchargez Tor à l'adresse suivante : http://www.torproject.org/
S'il est censuré dans votre pays, voici les sites miroirs par lesquels vous pourrez y accéder (http://www.torproject.org/mirrors.html.en) :
http://tor.cybermirror.org/
http://tor.zdg-gmbh.eu/
http://tor.anonymity.cn/

Installez la dernière version du logiciel sur votre bureau et suivez les instructions.

Tor est un logiciel assez sophistiqué qui repose sur la connexion à trois serveurs proxies. Ils recomposent ensemble chaque page que vous voulez consulter, ce qui empêche le serveur d' identifier l'adresse IP de votre ordinateur car il ne la reconnaît pas (cf . « Choisir sa technique pour contourner la censure»).
De plus, Tor contient un logiciel qui garantit une sécurité plus importante : privoxy, qui bloque aussi l'accès aux cookies et aux publicités.

3. Installez le bouton « TOR »

Cette fonction permet de savoir en un clic si Tor est actif ou pas. Firefox est indispensable pour l'installer facilement.

Attention, si vous bloguez d'un cybercafé, il est nécessaire de passer par XeroBank Browser (xB Browser) ou Tor on a Stick (ToaSt) et d'utiliser un ordinateur sur lequel vous pouvez sauvegarder des fichiers. Sur votre clé USB, copiez le fichier xB-Browser.exe, qui vous donnera accès à Tor de n'importe quel ordinateur, en utilisant Windows. Quittez le navigateur installé par défaut sur l'ordinateur du cybercafé dans lequel vous êtes et connectez-vous à Internet via ce fichier, qui lancera un nouveau navigateur utilisant Tor. Xerobank est une version spéciale de Firefox sur laquelle Tor et privoxy sont déjà installés. Le stocker sur une clé USB vous permet de contourner la censure à partir d'ordinateurs sur lesquels vous ne pouvez pas installer de logiciels. Donc, même si le cybercafé relève l'identité de l'internaute à l'entrée, son anonymat est assuré.

Pour savoir si Tor fonctionne, activez-le et allez voir sur le site si le message « Your IP is identified to be a Tor Exit » s'affiche. Dans ce cas, vous êtes connectés à Internet via Tor.

ETAPE N°2 : CRÉER UN COMPTE MAIL DIFFICILEMENT IDENTIFIABLE

Même en utilisant Tor, vous ne devez pas utiliser votre messagerie personnelle pour bloguer car toute information qui vous est liée à vous pourrait mener à vous identifier. Vous devez créer un compte spécial et vous assurer que RIEN ne peut permettre de vous identifier (nom, adresse etc). Sur ce compte déjà existant, l'adresse de votre ordinateur, quand il ne passait pas par Tor, est retenue par votre fournisseur d'accès.

1. Choisir une boîte de messagerie

Gmail et Hushmail, Vaultletsoft peuvent vous permettre de rester anonmyme, mais également d'autres webmails tels que fastmail.fm. Yahoo! et Hotmail sont également des options à considérer, si vous utilisez Tor.

Sur Hotmail et Yahoo !, vous pouvez être identifié si vous n'utilisez pas Tor car ces boîtes gardent en mémoire l'adresse IP de l'ordinateur à partir duquel vous vous connectez.

Hushmail permet d'avoir un haut degré de sécurité car cette boîte ne stocke pas votre

adresse IP. Cependant, c'est un service payant et si vous y créez un compte gratuit, vous devrez l'utiliser régulièrement afin qu'il ne soit pas supprimé.

Gmail est une bonne solution car ce service gratuit ne donne pas accès à l'adresse IP d'où provient le mail. Il est possible d'avoir une adresse sécurisée.

2. Créer un compte anonyme

N'utilisez aucune donnée personnelle. Prenez les noms les plus courants et créez un mot de passe de 8 caractères au minimum, incluant au moins un chiffre ou caractère spécial. Important : choisissez le même nom pour ce compte que pour votre blog !

3.Tester le fonctionnement du compte

Envoyez un mail à partir de ce nouveau compte quand Tor est activé. Comme Tor change ses codes toutes les dix minutes, vous ne pourrez envoyer des mails qu'à dix minutes d'intervalle.

ETAPE N°3 : CRÉEZ VOTRE BLOG ANONYME SUR WORDPRESS

Cette étape demande beaucoup plus de précautions que pour la création d'un blog sans couvert d'anonymat.

ACTIVEZ TOR OU XEROBANK

Allez sur le site Internet de la plateforme de Wordpress. Créez un nouveau blog en utilisant l'adresse et le nom du compte mail que vous venez de créer (cf. « présentation de Wordpress).
Wordpress vous enverra un lien pour activer votre compte sur votre mail « d'anonymat » et vous tiendra au courant des activités de la plateforme.
Toujours en utilisant Tor, connectez-vous à votre blog et changez votre profil afin de choisir un autre mot de passe que celui accordé par Wordpress. Ajoutez autant d'informations que vous voulez mais n'oubliez pas qu'elles ne doivent pas permettre de vous identifier. Ne mettez pas de photo de vous ou de votre entourage par exemple.

ETAPE N°4 : POSTER DES ARTICLES

Ne rédigez pas d'article en ligne ! Non seulement cela vous permet de ne pas les perdre si la connexion Internet est coupée ou le navigateur capricieux, mais aussi d'écrire ce que vous voulez, sans la pression d'un gérant de cybercafé ou de policiers autour de vous. Effacez ensuite ces contenus de votre ordinateur.

Connectez vous via Tor et mettez votre article en ligne en utilisant les fonctions « copier » et « coller ». N'oubliez pas d'ajouter le titre et les catégories (cf. « comment être bien réfé-

rencé » et « présentation de Wordpress ») avant d'enregistrer votre article.

Avant de « publier en ligne », changez la fonction d'horodatage (« timestamp ») et publiez votre article à une heure postérieure à l'heure réelle. C'est également une façon de protéger votre identité car l'heure à laquelle vous êtes connecté est un signe qui peut permettre de vous retrouver (cf. l'article "présentation de Wordpress"). Certains gérants de cybercafés sont tenus d'enregistrer l'heure de connexion de tous leurs clients.

ETAPE N°5 : ASSUREZ VOS ARRIÈRES

Effacez tous les brouillons d'articles, même s'ils sont stockés sur une clé USB. Il n'est pas suffisant de les mettre à la « corbeille ». Veillez à utiliser des logiciels du type Ccleaner (www.ccleaner.com) ou Eraser (www.heidi.ie/eraser) si vous êtes sous Windows. « Secure empty trash » si vous êtes sur Mac.
Effacez également tout l'historique de votre navigation sous Firefox avant d'éteindre votre ordinateur, par l'intermédiaire de la fonction « Clear private data when closing firefox » dans le menu « Préférences »> « Vie privée ».

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

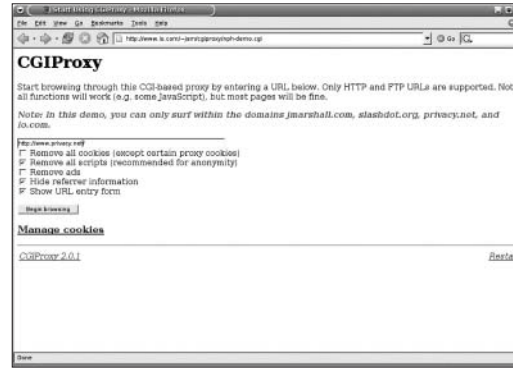
Il est extrêmement important de connaître la sanction pénale à laquelle s'exposent les utilisateurs s'ils sont surpris en train d'utiliser une technologie de contournement. Les options seront différentes en fonction de la sévérité de la sanction. Si la sanction pénale encourue est limitée, les internautes 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://psiphon.civisec.org

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.

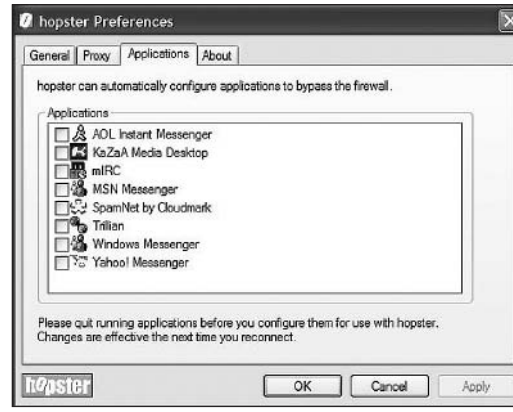
La recherche et l'emploi de proxies ouverts n'est pas recommandée. Ces serveurs sont souvent utilisés en raison de leur disponibilité, mais, s'ils sont efficaces pour contourner les mesures de filtrage, ils n'assurent pas la sécurité de l'utilisateur.

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.

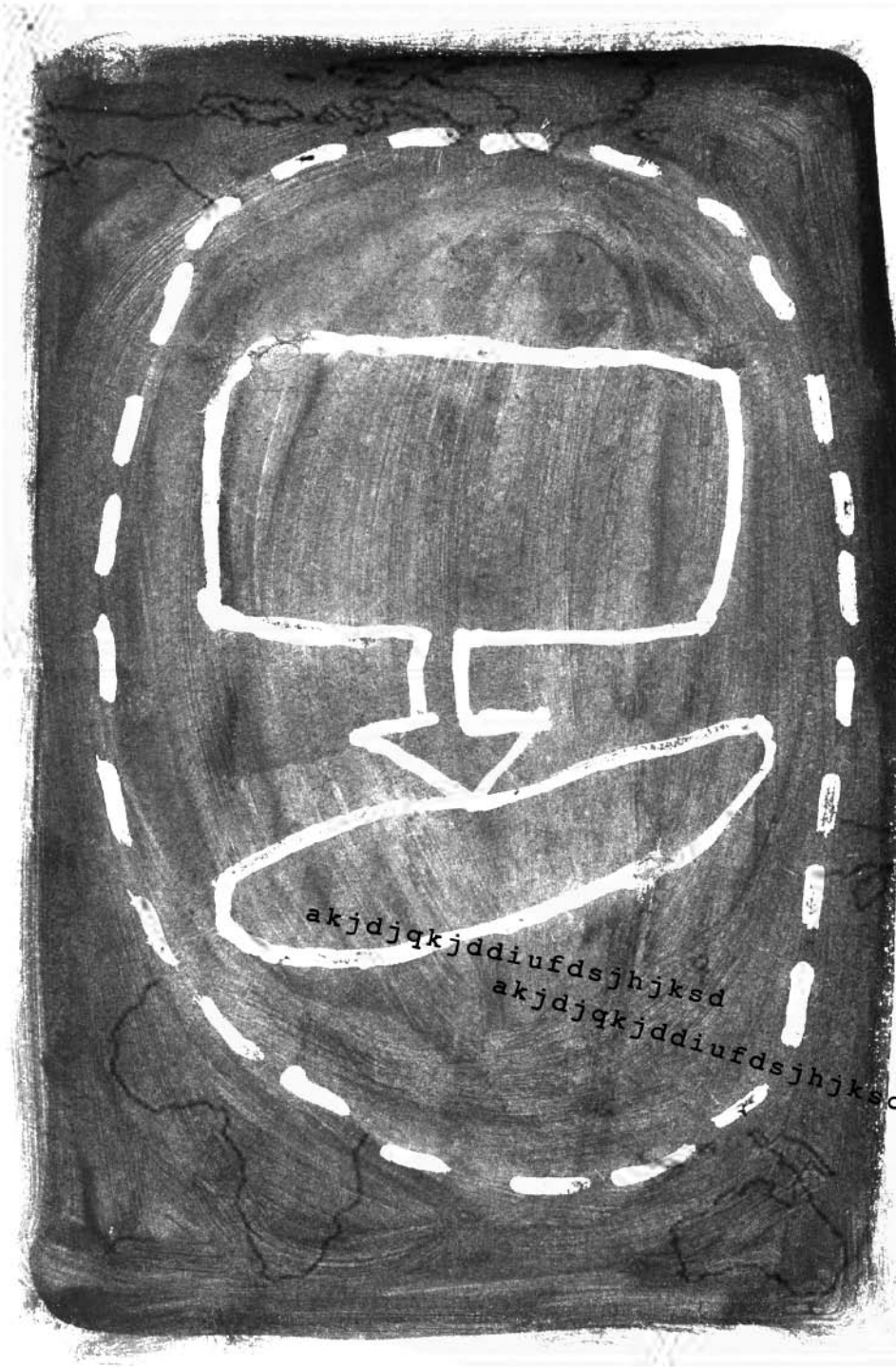
Toutefois, la clé publique étant échangée sur Internet sans protection particulière, il est recommandé de vérifier la validité de celle-ci auprès de son propriétaire. Pour ce faire, chaque clé publique possède une courte suite de caractères, appelée empreinte digitale, qu'il est facile d'échanger de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


akjdjqkjddiufdsjhjksd
akjdjqkjddiufdsjhjksd

LES CISEAUX D OR **2008**

Les pays les plus répressifs sur Internet font preuve de minutie et de créativité. La censure sur la Web est un savant mélange entre le filtrage et la surveillance. De plus en plus de gouvernements tentent de réaliser pour contrôler l'information qui circule sur leur réseau, souvent sous couvert de combattre la cybercriminalité

CHAMPION TOUTES CATÉGORIES : LA CHINE

Le Parti communiste chinois (PCC) et l'Etat ont déployé des ressources humaines et financières colossales pour empêcher l'émergence d'une véritable liberté d'expression sur Internet. Les sites d'informations ont notamment été placés sous la tutelle éditoriale d'organes de propagande, au niveau national et local. Avec 48 cyberdissidents derrière les barreaux, la Chine exerce une répression systématique envers les blogueurs. Le gouvernement veut garder le contrôle sur l'information et censure le Net grâce à un mélange subtil entre filtrage et dissuasion. Plusieurs milliards de dollars auraient déjà été consacrés à la censure d'Internet. Depuis l'été 2007, deux "cyberpoliciers" s'affichent sur les écrans des ordinateurs des cybercafés afin de signifier aux internautes qu'il sont surveillés. Le pays est en passe de devenir le plus grand marché du secteur de l'Internet au monde, devant les Etats-Unis, et attire de plus en plus d'entreprises étrangères, qui, pour certaines, acceptent de censurer leur réseau.

MEILLEUR RÉPRESSEUR : L'IRAN

Internet occupe une place de plus en plus importante dans la société, ce qui déplaît fort au président Mahmoud Ahmadinejad qui ne supporte pas que sa politique soit malmenée. Le gouvernement s'est donc doté d'un outil légal pour censurer le Web. Depuis 2006, tous les sites Internet doivent s'enregistrer auprès des autorités et les fournisseurs d'accès doivent vérifier que des contenus "interdits" ne sont pas publiés par leurs serveurs. Les sites de partage de photos FlickR et de vidéos YouTube sont inaccessibles car certains documents qu'ils contiennent sont jugés "immoraux" par les autorités. La

Toile reste cependant le vecteur de l'expression de la société et permet par exemple aux femmes de revendiquer leurs droits. Les journalistes en ligne, qui publient des articles pour des revues féminines, sont régulièrement convoquées au tribunal de Téhéran pour des interrogatoires. En 2007, les autorités ont interpellé une dizaine de blogueurs et blogueuses en raison de leurs activités sur Internet.

MEILLEUR SECOND RÔLE : L'ENTREPRISE AMÉRICAINE YAHOO !

Grâce à sa collaboration, les autorités chinoises ont pu mettre au moins quatre cyber-dissidents en prison. Shi Tao, journaliste de 37 ans pour Dangdai Shang Bao (Les Nouvelles du commerce contemporain), a été condamné à dix ans de prison en 2005 pour "divulgation illégale de secrets d'Etat à l'étranger", sur la base de renseignements fournis par l'entreprise américaine au gouvernement. Il a été reconnu coupable d'avoir diffusé, sur des sites basés à l'étranger, une note interne transmise à sa rédaction par les autorités qui mettait en garde les journalistes contre les dangers d'une déstabilisation sociale et les risques liés au retour de certains dissidents à l'occasion du quinzième anniversaire du massacre de la place Tiananmen. L'entreprise américaine est engagée dans deux procédures judiciaires pour l'aide qu'elle a procurée aux autorités. Lors d'une audience devant le Congrès américain dans le cas Shi Tao, son président Jerry Yang, s'est publiquement excusé pour le « malentendu » qui a conduit le journaliste en prison et a décidé de créer un fonds humanitaire dédié à aider les familles des cyberdissidents.

MEILLEUR ESPOIR : LE ZIMBABWE

Le Web n'est pas assez consulté sur le territoire pour que le gouvernement exerce une censure massive de la Toile. Cependant, les internautes sont ouvertement épiés par le pouvoir, qui se focalise sur les e-mails. En août 2007, le gouvernement a adopté une loi qui l'autorise à surveiller toutes les communications, qu'elles soient téléphoniques ou électroniques. La demande peut même être faite "à l'oral" dans le cas d'une "urgence ou de circonstances exceptionnelles". Publier un article critique envers le gouvernement sur Internet est extrêmement risqué pour son auteur. Étroitement contrôlée par le gouvernement de Robert Mugabe, l'entreprise nationale de télécommunications TelOne s'occupe de la censure du Réseau. La société peut demander aux fournisseurs d'accès à Internet de surveiller les communications en ligne sur simple requête. Le texte de l'accord leur demande également de "prendre les mesures nécessaires" afin d'empêcher la diffusion de contenus illégaux sur le Net.

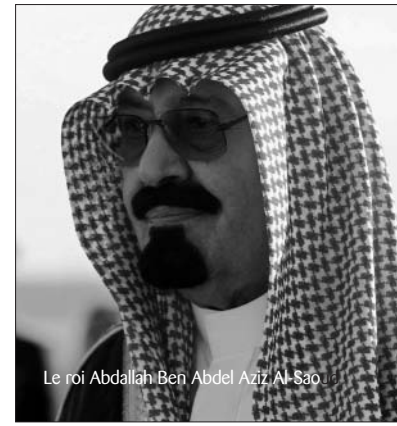

Le président Robert Mugabe

MEILLEUR SCÉNARIO ORIGINAL : BIRMANIE

De fin août à mi-octobre 2007, la Birmanie a connu le soulèvement le plus important depuis les manifestations étudiantes de 1988 dont la répression avait fait 3000 morts. Les moines se sont révoltés contre les conditions de vie des Birmans, entraînant avec eux des milliers de manifestants dans les rues. Devant cette "révolution safran", le gouvernement a volontairement isolé le pays pour qu'aucun témoignage ne sorte des frontières. Du 28 septembre au 16 octobre 2007, les deux fournisseurs d'accès ont coupé les connexions Internet sur ordre de la junte militaire. Durant ces deux semaines de black-out, Internet n'a été accessible que durant quelques heures et tous les cybercafés ont été fermés. Pour les Birmans, les seuls moyens de s'informer étaient les télévisions par satellites ou les radios étrangères.

MEILLEUR FILTRAGE : ARABIE SAOUDITE

Contrairement à la Chine ou à l'Iran, les filtres saoudiens indiquent clairement que les autorités censurent le Web. Beaucoup de sites, qui traitent de la vie sociale sont inaccessibles. Près de 400 000 pages Web sont bloquées dans le royaume en raison de leur contenu "immoral", lié par exemple à l'homosexualité ou aux droits des femmes. Une commission doit également mettre en place des labels de qualité pour «protéger la société saoudienne » de ces contenus. Il a même été décidé de renforcer la loi pour combattre le terrorisme, la fraude, la pornographie, la diffamation ou la violation des valeurs religieuses. Le 10 décembre 2007, le blogueur Fouad al-Farhan a été arrêté et conduit à la prison de Djeddah pour avoir publié un commentaire sur les avantages et les inconvénients d'être musulman.


Le roi Abdallah Ben Abdel Aziz Al Saoud

MEILLEUR CENSEUR : LE VIÊT-NAM

Le Viêt-nam a un taux de pénétration d'Internet supérieur à celui de la Chine. Depuis 2001, tous les internautes qui utilisent le réseau vietnamien sont responsables du contenu qu'ils créent, diffusent ou archivent. En 2006, les fournisseurs d'accès ont reçu la consigne d'installer un logiciel qui permet de conserver, pendant un an, les données de leurs clients. Le filtrage des contenus politiques dépend du ministère de l'Intérieur. L'Etat est actionnaire de tous les fournisseurs d'accès et peut donc aisément les contrôler. Sept cyberdissidents sont derrière les barreaux pour avoir usé de leur droit à la liberté d'expression sur Internet. Grâce à sa « cyberpolice » présente dans les cybercafés depuis 2002, le

pays est sur la même voie que son grand frère chinois.

MEILLEUR DÉCOR : CUBA

Depuis l'escapade de Reporters sans frontières sur cette île de rêve en 2006, la situation d'Internet s'est encore aggravée en matière d'accès au Réseau. Au centre de La Havane, on ne compte plus qu'un cybercafé ouvert. Les Cubains n'ont en grande partie accès qu'à un Intranet (messagerie, navigateur et actualités) car l'accès au réseau international est très cher. Le gouvernement n'hésite pas à réprimer les voix les plus critiques. Les connexions privées à Internet sont considérées comme illégales et un internaute peut être condamné à cinq ans de prison pour ne pas avoir respecté cette règle. Mais il peut également être condamné à vingt ans de prison pour avoir publié un article "contre-révolutionnaire" sur des sites étrangers.

REPORTERS SANS FRONTIÈRES
Secrétariat international
47, rue Vivienne – 75002 Paris, France
Tél. : 33 1 44 83 84 84
Fax : 33 1 45 23 11 51

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

Conception graphique orginale : Nuit de Chine
Illustrations additionnelles : Marion Brosse pour Nuit de Chine

Copyright : Reporters sans frontières 2008

Soutenez la campagne de Reporters sans frontières à l'approche des Jeux olympiques de Pékin en 2008
http://www.rsf.org

GUIDE PRATIQUE DU **BLOGUEUR** ET DU **CYBERDISSIDENT**

Les blogueurs inquiètent. Les gouvernements se méfient de ces hommes et ces femmes qui, sans être officiellement journalistes, publient des informations. Pire, ils abordent souvent des sujets sensibles que les médias désormais qualifiés de "traditionnels" n'osent pas traiter. Les blogs sont devenus, dans certains pays, une nouvelle source d'informations.

Cette nouvelle version du guide et du cyberdissident est disponible en français et en anglais, sur le site http://www.rsf.org. Ce guide rassemble des conseils et des astuces techniques pour lancer son blog dans de bonnes conditions et contourner la censure sur Internet. Il explique notamment comment bloguer anonymement et propose les témoignages de blogueurs d'Egypte et de Birmanie notamment.

REPORTERS SANS FRONTIÈRES

www.rsf.org

REPORTERS SANS FRONTIERES
POUR LA LIBERTÉ DE LA PRESSE