L'internet, une nouvelle menace pour la liberté d'expression ?

Premier auteur : Cécile DOLBEAU-BANDIN
Adresse du premier auteur :
49 avenue de Seine
92 500 Rueil-Malmaison
☎ 01 47 08 57 76
✉ cdolbeau@wanadoo.fr

Résumé :

Cet article traite des excès et des dangers que fait naître l'internet sur la presse en ligne. Nous faisons une synthèse des moyens technologiques et juridiques mis en place par les régimes autoritaires et démocratiques pour contrôler et censurer l'information en ligne. Nous rappelons aussi les dangers auxquels s'exposent quotidiennement les professionnels des médias en ligne pour faire leur métier.

Summary:

This article deals with excesses and risks created by the internet on press on-line. We give an overview of the technological and legal means used by authoritarian and democratic political regimes to control and censor the on-line information. We also remind risks daily ran by professionals of on-line media to do their job.

Mots clés : l'internet, presse en ligne, cyberdissidents, liberté d'expression, vulnérabilité,

L'internet, une nouvelle menace pour la liberté d'expression ?

« *Quand l'homme commence à redouter sa propre pensée, à se défiler et à fuir ses propres mots, par crainte de la censure, alors là il a perdu sa liberté*. »
Zoé Valdés

Introduction

Cette intervention vient en réponse au président du jury de ma thèse : Mohamed Hamdame, directeur et professeur à l'Institut de presse et des sciences de l'information (IPSI) à Tunis. Pour cet intellectuel tunisien, qui connaît bien la répression et la pression exercées par les autorités de son pays vis-à-vis des médias traditionnels, l'internet est un espace de discussion et une source d'information indépendante. Mais il s'interroge : « *le support papier étant saisi à la douane, est-ce que des procédés techniques sont utilisés par le pouvoir politique pour freiner la diffusion du journal mis en ligne ?* » Ainsi, nous étudions les excès et les dangers que fait naître l'internet sur la citoyenneté et les espaces publics, plus exactement sur le cas de la presse en ligne.

Dans certains pays où les médias traditionnels sont censurés, l'internet offre un nouvel espace d'expression aux dissidents et aux journalistes : détournement de la censure des médias traditionnels, publication d'une information et d'opinions indépendantes quitte à déplaire à un gouvernement, circulation d'informations que les médias traditionnels ne relaient pas...

Les dissidents et les journalistes hors-ligne deviennent des dissidents et des journalistes « internétiques ». Ils peuvent ainsi jouer un rôle actif au regard de l'information en ligne en réagissant (forums de discussions…), en participant (blogs, wikis, sites indépendants…), en téléphonant par l'internet ou utilisant un *proxy*[1] pour contourner les interdits. L'internet leur permet de recevoir, d'écrire et de faire partager des informations en s'affranchissant *a priori* du contrôle des autorités locales.

Seulement, leur espoir de liberté d'expression numérique se heurte le plus souvent à la censure du pouvoir. L'internet dérange, voire fait peur aux régimes répressifs. Les gouvernements autoritaires renforcent leur emprise sur le réseau (fermetures de sites d'information, perquisitions policières, procès, amendes, emprisonnements, harcèlements, menaces, intimidations, coups et blessures…). Les démocraties, elles aussi, glissent peu à peu dans la surveillance des communications numériques et le développement de lois liberticides. Ainsi, l'internet devient à la fois un espace d'expression et une menace supplémentaires pour le journalisme et les journalistes.

[1] Un serveur mandataire ou proxy est un serveur informatique qui a pour fonction de relayer des requêtes entre un poste client et un serveur. Le relais proxy permet de se connecter au réseau au travers de serveurs basés à l'étranger.

Nous découpons ce travail en deux parties :

1. Dans un premier temps, nous faisons une synthèse des moyens technologiques et juridiques mis en place par les régimes autoritaires et démocratiques pour contrôler, voire interdire l'information en ligne.

2. Dans un second temps, nous relatons les risques qu'encourent les journalistes et les dissidents « internétiques ».

Ce qui nous intéresse ici, c'est l'insécurité numérique et la vulnérabilité des cyberdissidents et des journalistes « internétiques ».

Un muselage technologique et juridique

Selon les pays, l'internet est soumis à des législations différentes et des restrictions plus ou moins importantes. Pour contrôler les internautes et censurer le réseau, les dictatures trouvent de multiples parades et réussissent à contrôler, à museler et à purger le web, le plus souvent grâce à des systèmes technologiques. De ce fait, le raffinement de l'internet apporte des moyens considérables de contrôle et une surveillance de l'information qu'il est bien difficile d'empêcher ou de détourner.

Nous faisons ici un rapide panorama de ces technologies plus ou moins sophistiquées :

- Les filtres qui rendent inaccessibles les contenus et permettent de contrôler l'accès aux données diffusées sur le web. Ce filtrage repose sur le blocage d'une liste de noms de domaines ou d'URL et associé à des systèmes basés sur la recherche de mots-clés permettant de barrer les contenus de façon dynamique. Quand les usagers 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. Les blogs qui dérangent sont aussi bloqués (Arabie Saoudite) ;

- Les logiciels qui permettent de lire les courriels en reprenant des mots clés (démocratie, révolution, coup d'état, nom d'un dissident connu…) susceptibles de porter atteinte à la sécurité de l'état ;

- Les « miroirs modifiés » copient les sites controversés puis les modifient afin de miner ou d'affaiblir les prises de positions interdites : ceux qui se connectent reçoivent des copies falsifiées ;

- Le blocage IP (*Internet Protocol*), par routeur et plus récemment par la redirection DNS, permet aux gouvernements de bloquer les contenus du web. Le navigateur peut afficher ce message « *host was not found* » ou « *connection time out* » laissant croire que le serveur est en panne. En Thaïlande, l'accès aux sites de jeu ou de politique est bloqué par un filtrage IP ;

- Le pare-feu ou *firewall* est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment l'internet). Il filtre l'accès aux sites jugés indésirables et permet de repérer ce qui circule sur le réseau. C'est un système analogue que la Chine met en place face à l'internet étranger ;

- Certains fournisseurs d'accès, à la demande des autorités locales, connectent leurs serveurs à un superordinateur central le plus souvent installé dans les locaux du ministère de l'intérieur (Chine, Tunisie…) ;

- Certaines pages ou certains éléments qui dérangent sont supprimées (Arabie Saoudite) ;

- Des hackers créent des virus et des programmes informatiques de toutes sortes pour bloquer les publications indésirables ;

- L'ensemble des cafés-internet ou publinets est contrôlé voire surveillé par l'état (Tunisie, Birmanie…) et des logiciels espions (implantés sur les disques durs lors de téléchargement de logiciels gratuits) sont installés sur les ordinateurs des cybercafés (Cuba) permettant ainsi d'épier les usagers. Lorsqu'un internaute saisit des mots interdits dans un courriel, il reçoit un message d'alerte lui indiquant que son texte est considéré comme une menace pour la sécurité de l'état. Quelques secondes plus tard, son navigateur web se referme automatiquement.

Les autorités peuvent aussi interdire l'accès au web à la majorité de la population (Turkmenistan), proscrire les connexions à haut débit (Iran), posséder un monopole sur les télécommunications du pays (Bélarus), obliger les propriétaires d'ordinateurs à se déclarer sous peine de se voir imposer une peine de prison (Birmanie), restreindre le contenu accessible sur le réseau des fournisseurs d'accès autorisés (Chine), fermer ou rediriger des sites de discussion abordant des thèmes politiques ou sociaux sur des forums de loisirs, réglementer l'achat de matériel (Cuba)…

Il existe aussi une police « internétique » chargée de traquer et d'arrêter les cyberdissidents et les journalistes « internétiques ». Les cyberpolices interceptent les communications numériques, identifient et arrêtent les opposants au régime. Pour surveiller un journaliste web, elles utilisent des machines qui épient, produisent des rapports et bloquent automatiquement les conversations et les publications subversives. Ainsi, les gouvernements répressifs ont tendance à vouloir « retoucher » l'internet pour en faire un instrument de contrôle et de censure en mettant en place des technologies bloquant l'accès de certains contenus et en instaurant une surveillance à très grande échelle.

On peut penser que ces procédés sont réservés uniquement aux régimes autoritaires. Mais depuis quelques années dans les pays démocratiques, la censure de sites, la surveillance des communications numériques et des lois liberticides se développent. En octobre 2001, les États-Unis adoptent le *Patricot Act*, suivis de près par la plupart des pays occidentaux. Cette

loi antiterroriste permet au FBI de connecter le système Carnivore[2] sur le réseau d'un fournisseur d'accès pour épier le mouvement des messages numériques et garder le suivi de la navigation d'un individu suspecté d'être en contact avec une force étrangère.

La France se dote aussi d'un arsenal juridique : la loi française sur la sécurité quotidienne (LSQ, novembre 2001) et la loi sur la confiance dans l'économie numérique (LEN, 13 mai 2004). L'un des objectifs de ces deux textes est de faciliter l'obtention par la police d'informations personnelles sur les internautes. De ce fait, les actions de ces derniers peuvent être retranscrits instantanément grâce au numéro d'identification de leur poste, leur adresse IP, enregistrés et conservés. L'internaute laisse des empreintes et éparpille de nombreuses données sur son identité, ses goûts ou ses habitudes.

Le comité des ministres du Conseil de l'Europe adopte en mai 2003 une déclaration sur la liberté des communications sur l'internet. Ce texte précise que ce nouveau média doit profiter des mêmes protections que les médias traditionnels et admet l'éventualité de filtrer certains sites suite à une décision judiciaire. Ces états démocratiques justifient cette mise sous tutelle juridique par le fait qu'ils doivent démanteler les réseaux terroristes, lutter contre le développement des contenus xénophobes, des contenus pédophiles, des contenus antisémites, faire baisser la cybercriminalité… Mais ils oublient que ceci doit être effectué dans un cadre juridique précis et respectueux des libertés individuelles.

Comme le souligne Robert Ménard, secrétaire général de Reporters sans frontières (RSF) :

« *Que notre sécurité se paie de certains empiètements sur nos libertés ne devrait pas nous choquer* a priori. *Mais à deux conditions. Le législateur doit encadrer toutes ces mesures, ce ne fut pas toujours le cas. La police doit agir sous le contrôle des magistrats, on l'a parfois oublié.* »[3]

Dans ce sens, les états démocratiques doivent s'atteler au dossier de l'internet en cherchant des voies nouvelles pour réguler le réseau sans nuire aux libertés individuelles des citoyens.

La vulnérabilité des journalistes et des dissidents « internétiques »

Je montre ici de quelle manière la censure de la presse en ligne relève de la vulnérabilité et quelle forme elle prend. La désobéissance civile numérique n'est pas sans risques pour le journalisme et les journalistes. Les menaces et les pressions des régimes autoritaires sont inquiétantes et constituent un vrai péril quant à la liberté d'expression sur l'internet : les cyberdissidents et les journalistes « internétiques » des régimes répressifs sont trop souvent en danger.

---

[2] Carnivore est le nom du logiciel de surveillance que le FBI pouvait installer, jusqu'en 2002, chez les fournisseurs d'accès. Il permettait de surveiller la circulation des messages et de conserver l'historique des consultations d'un individu soupçonné de contact avec une puissance non américaine.

[3] RSF. *Guide pratique du blogger et du cyberdissident*. Éditions RSF, Paris, 2006. P. 1.

Pour cette dernière partie, je me base essentiellement sur *la liste des 13 ennemis d'internet* publiée par RSF[4] en 2006. L'Arabie Saoudite, le Belarus, la Birmanie, la Chine, la Corée du nord, Cuba, l'Égypte, l'Iran, l'Ouzbékistan, la Syrie, la Tunisie, le Turkmenistan et le Viêt-nam figurent sur cette liste où la liberté d'informer *via* l'internet n'est pas un droit.

La publication d'informations ou de propos en faveur de pays démocratiques, la diffusion sur des blogs personnels d'opinions subversives, d'articles sécessionnistes ou critiques à l'encontre du gouvernement, l'utilisation des forums de discussion pour faire de la propagande anti-gouvernementale ou pour demander plus de démocratie, l'outrage aux dirigeants du pays ou la simple appartenance à la presse libre et indépendante mettent en danger ces dissidents et ces journalistes « internétiques »

Mais que risquent-ils ? Je fais ici un rapide bilan de ce qu'ils encourent : censure, fermeture de site ou de blog, vol ou confiscation du matériel informatique, poursuites judiciaires, convocations par la police, surveillance, perquisitions, brutalités policières, harcèlement, menaces sur l'entourage, intimidations, agressions, incarcérations, assassinat…

En 2004, 74 cyberdissidents[5] se trouvent emprisonnés. En 2007, ils ne sont plus que 66 derrière des barreaux. Mais cette « légère amélioration » ne doit pas faire oublier que les pressions exercées sur ces internautes et les arrestations demeurent. Les peines d'emprisonnement sont plus ou moins longues selon les pays : de plusieurs mois pour des blogueurs cubains, iraniens ou des internautes vietnamiens ou égyptiens à plusieurs années (neuf ans de prison pour des journalistes web chinois, plus de vingt ans en Tunisie). Des journalistes ou les dissidents cubains ont été condamnés à vingt ans de prison pour des articles contre-révolutionnaires publiés sur des sites étrangers et à cinq ans pour s'être simplement connectés de manière illégale à l'internet. Ces arrestations, amplement médiatisées, sont aussi le moyen de faire peur et de faire taire ces journalistes web.

Certains régimes répressifs ont aussi recours à la force pour bâillonner ces cyberdissidents. Ils peuvent être torturés et détenus dans des conditions inhumaines. Dans certains pays (Syrie, Tunisie…), les menaces corporelles restent le moyen le plus utilisé par les autorités pour empêcher les journalistes d'exercer leur métier. En Tunisie et à Cuba, les services de sécurité harcèlent les blogueurs indépendants et les responsables de sites d'opposition.

Des journalistes sont tués dans l'exercice de leur fonction. En Ukraine, un collaborateur en ligne de Vlasti.net est retrouvé pendu à la poignée de son réfrigérateur en décembre 2003. Il se donnait pour mission de dénoncer les pratiques frauduleuses des autorités et des hommes politiques. En novembre 2000, le rédacteur en chef du Pravda.com est retrouvé mort (décapité et mutilé). Il était connu pour son regard critique du pouvoir ukrainien et pour son combat en faveur de la liberté de la presse.

L'internet, en touchant un large public, est souvent la seule arme anti-censure. Seulement, les journalistes et les dissidents « internétiques », maillons indispensables de la liberté de la presse en ligne, sont vulnérables.

---

[4] En 2006, trois pays sont retirés de la liste des ennemis de l'internet : la Libye, les Maldives et le Népal.
[5] RSF. *Internet sous surveillance, les entraves à la circulation de l'information sur le réseau*. Éditions RSF, Paris, 2004. P. 3.

Comme le souligne Alain Frachon, journaliste au *Monde* :

« *Il faut le savoir : se connecter, c'est exposer et écrire en ligne. C'est aussi s'exposer.* »[6]

Conclusion

Nous comprenons bien au vu de cet acte que les principales difficultés des journalistes en ligne et des dissidents sont à la fois nombreuses, graves et préoccupantes. Face à ces contrôles, à ces menaces et à ces censures, les dissidents et les journalistes « internétiques » s'organisent pour les contourner et protéger leur anonymat.

De nombreuses « technologies de contournement » apparaissent afin de leur permettre de déjouer ces méthodes de contrôle et de filtrage. En général, ces technologies 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. Le codage de leurs courriels (cryptographie) ou l'utilisation de *Skype*[7] facilite également les communications entre les journalistes et leurs sources.

Ils peuvent aussi bénéficier du soutien, de la protection et de l'aide d'ONG et d'associations de journalistes dont RSF, IFEX (International Freedom of expression exchange), CPJ (Comnittee to protect journalist), FIJ (Fédération internationale des journalistes)… Le but de ces organisations internationales est de défendre les droits des journalistes et de contribuer au développement dans le monde entier de la liberté des médias traditionnels et en ligne.

Par exemple, elles proposent de contourner la censure en hébergeant des journaux qui ne peuvent être édités dans leur pays et donne la parole à des journalistes contraints au silence, établissent des sites pour défendre les droits de l'homme, publient des informations notamment sur la liberté d'expression, accordent des aides matérielles ou financières à un journaliste ou à un média en difficulté ainsi qu'aux familles de reporters emprisonnés, essayent d'agir pour améliorer la sécurité des journalistes…

Les journalistes en ligne, ainsi que les personnes qui écrivent sur l'internet, doivent bénéficier du droit fondamental à la liberté d'expression et de droits complémentaires à la confidentialité de leurs communications et de leurs sources tout en respectant les codes de déontologie qui existent.

---

[6] FRACHON Alain. Les nouveaux verrous. *Le Monde 2*, n°104, Paris, 2006, P.10,

[7] Il permet de téléphoner gratuitement uniquement entre deux ordinateurs ou terminaux équipés de *Skype* et connectés à l'internet, grâce à un microphone et des haut-parleurs ou un téléphone branché sur l'ordinateur. Il est aussi équipé d'une messagerie instantanée permettant aux usagers de communiquer textuellement et de se transmettre des fichiers.

Références bibliographiques

a. Ouvrages

RSF. *Internet sous surveillance, les entraves à la circulation de l'information sur le réseau*. Éditions RSF, Paris, 2004.

RSF. *Guide pratique du blogger et du cyberdissident*. Éditions RSF, Paris, 2006.

b. Articles

BEN EDELMAN. Sur Internet filtré, les choses ne sont pas ce qu'elles paraissent. *Internet sous surveillance, les entraves à la circulation de l'information sur le réseau.* Éditions RSF, Paris, 2004. P.4.

BOLLON Patrice et CHAMPAGNE Antoine. Attention, Internet sous surveillance. *Le Monde 2*, n°104, Paris, pp. 21-25, 2006.

FRACHON Alain. Les nouveaux verrous. *Le Monde 2*, n°104, Paris, pp. 10, 2006.

STRIEGLER Bernard. Internet, enjeu d'une lutte de société. *Le Monde 2*, n°104, Paris, pp.26-27, 2006.

c. Sites

CHARLES Gilbert. « Journalistes sous surveillance ». www.lexpress.com, Paris, 2004.

FIGAROL Nadège. « Presse indépendante en ligne, un bastion pour la liberté d'informer ». www.CFDT.fr, Paris, pp.1-2, 2003.

RSF. « Bienvenue dans l'ère des dictatures web 2.0 ». www.RSF.org, Paris, pp.1, 2007.

RSF. « Liste des 13 ennemis d'Internet ». www.RSF.org, Paris, pp.1-5, 2006.

SAMARCQ Nicolas. « La cybercriminalité sous surveillance ». www.brmavocats.com, Paris, pp. 1-3, 2004.

UNESCO. « Conclusions de la conférence sur les nouveaux médias et la liberté de la presse ». www.portal.unesco.org, Paris, pp.1, 2007.

WOLTON Dominique. « Journalisme et liberté d'information à l'heure de la mondialisation ». www.cnrs.fr, Buenos Aires, pp. 1-2, 2005.