

Tunisie : La censure sur Internet Un combat d'arrière garde



Août 2009

Publignet fermé à Tunis

Avertissement

Ce rapport a pour but de faire l'état des lieux de la censure qui se pratique officiellement sur Internet en Tunisie. Il a été réalisé par des non experts pour des non experts ; l'Observatoire souhaitait essentiellement révéler le dispositif réglementaire de la censure, les techniques de censure utilisées et surtout aider les défenseurs tunisiens à s'outiller pour comprendre et se protéger contre différentes formes d'attaques qu'ils subissent sur leur courriers électronique ou sur leur capacité à surfer librement sur le Web. Nous cherchons également à favoriser une citoyenneté active, permettant de prévenir les effets négatifs de la marginalisation, notamment des jeunes qui sont la population qui utilise le plus Internet.

Table des matières

Table des matières.....	3
I- Résumé exécutif.....	5
II- Recommandations.....	8
III- Introduction « médias dans une société fermée ».....	9
Un paysage médiatique pauvre malgré le pluralisme de façade	10
IV- Internet et les mécanismes de la censure.....	11
Un réseau moderne qui couvre l'ensemble du pays.....	11
Internet, le media alternatif.....	12
<i>Un dispositif réglementaire répressif</i>	<i>12</i>
Arrêté du ministre des communications du 22 mars 1997	13
Arrêté du ministre des communications du 9 septembre 1997	13
Loi n° 98-38 du 2 juin 1998 relative au Code de la Poste	13
Loi n° 2001-1 du 15 janvier 2001, portant promulgation du code des télécommunications	14
Loi n°2000-83 du 9 août 2000, relative aux échanges et au commerce électroniques.	14
Loi du 10 décembre 2003 sur le terrorisme	14
Loi N° 2004-5 du 3 février 2004 relative à la sécurité informatique.....	14
Loi d'orientation n° 2007-13 du 19 février 2007,.....	14
Décret n°2008-2638 du 21 juillet 2008	15
Décret n° 2008-2639 du 21 juillet 2008	15
<i>Une cyberpolice à la mesure de l'extension du réseau.....</i>	<i>16</i>
Les techniques de censure	17
Le filtrage de contenu	17
Surveillance et interception de la messagerie.....	18

Qui est censuré et qu'est ce qu'on censure ?.....	21
V- Les publinets sous surveillance étroite	24
Profil des usagers de publinets	24
Contrôle étroit et réduction du parc par fermeture administrative.....	24
Fichage des usagers.....	25
La justice à la rescousse quand la cyberpolice échoue	26
VI- La surveillance hors du territoire tunisien	27
<i>Attaques des sites web dissidents hébergés à l'étranger</i>	27
Surveillance des connexions de dissidents résidents à l'étranger	29
Infiltration de la blogosphère dissidente	30
VII- Conclusion	31

I- Résumé exécutif

La Tunisie a été révélée au monde comme l'un des pays qui pratique une censure à large échelle sur Internet et de façon systématique, lors de la tenue du Sommet mondial sur la société de l'information (SMSI) en novembre 2005.

Dans cette société fermée, le défi de la communication reste le problème majeur. Non satisfaites de verrouiller la presse et les médias audiovisuels, les autorités ont fait la chasse à ce nouvel outil de communication qu'est Internet. Une armada d'agents est mobilisée au ministère des Communications pour traquer les internautes et surveiller leur navigation.

Le paysage médiatique reste pauvre malgré le pluralisme de façade. La liberté d'éditer des journaux ou de diffuser des contenus TV ou radio libres est totalement confisquée. Aucune nouvelle autorisation de publier n'a été accordée à des médias indépendants depuis 1987.

La Tunisie se prévaut d'avoir été le premier pays arabe et africain à se connecter à la toile. Elle est officiellement le pays d'Afrique du Nord qui connaît la connectivité la plus importante avec 4,12 % de taux de pénétration. Elle est aussi le **seul pays africain qui interdit le raccordement par satellite aux particuliers** et la téléphonie fixe demeure le monopole de l'opérateur officiel, [Tunisie Télécom](#).

Dès l'année 1999 Internet est investi par les jeunes et les dissidents qui y trouvent une fenêtre sur le monde et un **espace alternatif où la parole citoyenne pouvait librement s'exprimer**.

Surprises par ces débordements inattendus, les autorités publiques vont de leur côté développer des mesures réglementaires et logistiques appropriées pour maintenir la toile dans les filets de la censure. Elles créent un véritable corps de police de l'information qui « veille » à la santé intellectuelle des Tunisiens.

La Tunisie est le pays de la région qui a très tôt développé une **réglementation sur Internet la plus exhaustive et la plus sévère**. Toutes ces lois ne sont pas mauvaises en soi, mais elles ont ceci en commun, elles donnent un **pouvoir exorbitant et discrétionnaire à l'administration publique** tout en limitant la marge de recours laissée au citoyen.

De grands moyens ont été investis pour contrôler le trafic du web. Les autorités ont mis en place une architecture où le contrôle se fait à plusieurs niveaux et assure le filtrage à l'épine dorsale du réseau faisant de l'Internet en Tunisie un vaste **intranet** à l'échelle du pays.

Ce type de censure pose évidemment de sérieux problèmes relatifs aux **libertés individuelles** et à la **protection de la vie privée** qui est normalement protégée par l'article 9 de la Constitution ainsi que la loi, portant sur « la protection des données à caractère personnel ».

Le contrôle du net est total grâce à ce verrouillage centralisé, opéré formellement par le fournisseur en gros de l'Internet (ATI) ; **en réalité, l'ATI n'est qu'un paravent ; c'est un autre organisme directement rattaché au ministère de l'intérieur et à la présidence de la république** qui opère ce contrôle en toute opacité.

Le filtrage du contenu - par le biais de logiciels de filtrage comme [Websense](#) et [Smartfilter](#) - constitue l'essentiel des techniques de censure des sites. Mais la surveillance et l'interception de la messagerie mobilise l'essentiel de leur énergie. C'est la technologie **Deep Packet Inspection** (DPI) qui est actuellement utilisée pour la surveillance de la messagerie ou la téléphonie internet VoIP.

Coupure de la connexion, Blocage des ports, disparition du courrier et blocage de l'attachement, sont devenus monnaie courante pour les défenseurs de droits humains et journalistes indépendants qui ont fait l'expérience d'une nouvelle méthode d'interception du courrier qui ne cherche plus à se cacher et à opérer discrètement. Cette situation a poussé 3 ONG à lancer en septembre 2008 un cri d'alarme dans un communiqué commun.

Qui est censuré et qu'est ce qu'on censure ? La manie de surveillance n'épargne personne : Des opposants et ONG indépendantes aux ministres en passant par les opérateurs économiques, les membres du parti au pouvoir, les syndicats, les universitaires, ou les représentations diplomatique.

Les contenus censurés sont les sites de droits humains, les sites d'information, les sites politiques d'opposition, les sites de pornographie, les outils de contournement et de navigation anonymes ; les traducteurs automatiques, certaines encyclopédies en ligne comme *Wikipedia* (certaines pages), les sites d'hébergement de vidéos tels *YouTube* et *Dailymotion* et les réseaux sociaux comme *Facebook*.

Les Publinets sont des centres publics d'Internet où des particuliers peuvent accéder à Internet. Ces derniers sont étroitement contrôlés et soumis à un cahier de charge contraignant. Le gérant doit « veiller à ce que le contenu visité par l'utilisateur doit être conforme aux normes autorisées par l'ATI » ; et « à contrôler à distance le contenu du courrier électronique de ses clients ».

Depuis le début de l'année 2009, les autorités ont remis en service l'obligation pour les usagers de s'identifier avant de surfer; un nouveau programme appelé **Publisoft** est imposé par l'ATI à tous les publinets; ils peuvent ainsi identifier en temps réel quel utilisateur a essayé de visiter quel site.

Ce contrôle étroit a conduit à une réduction du parc publinet par fermeture administrative qui a été réduit de moitié en l'espace de 4 ans. Aujourd'hui, l'ATI n'affiche plus sur sa page statistique le nombre de publinets en Tunisie.

La cyberpolice ne se contente pas de surveiller les Tunisiens en Tunisie, elle met tout en œuvre pour étendre également sa main mise sur l'activité des Tunisiens hors du territoire national. Elle multiplie les attaques contre les sites web dissidents hébergés à l'étranger (tous le sont parce que les FSI tunisiens refusent d'héberger ce type de contenu), elle surveille leur mails et leur connexions en recourant aux services de tiers et envoie ses espions infiltrer la blogosphère.

Une chose est sûre, des ressources considérables sont investies dans la surveillance de l'Internet, réparties entre le budget du ministère des Communications, du ministère de l'Intérieur, de l'ATCE et de la présidence de la république. Pour de nombreux observateurs ces ressources gagneraient à être investies dans des projets productifs et permettraient ainsi de résorber au moins 1/3 du chômage des jeunes diplômés tunisiens.

L'observatoire relève également le rôle négatif des partenaires européens dans l'appui inconditionnel à cette politique du régime tunisien qui se fait au nom de la sécurité, de la lutte contre le terrorisme et de la stabilité dans la région.

II- Recommandations

L'OLPEC demande à l'Etat tunisien de veiller

- 1- Au respect de ses engagements internationaux et notamment les instruments relatifs à la liberté d'expression (art.19 de la Déclaration universelle des droits de l'homme ainsi que du Pacte relatif aux droits civils et politiques)
- 2- A ce que toute législation touchant à la circulation de l'information sur Internet doit être fondée sur le principe de la liberté d'expression telle que définie par l'article 19 de la Déclaration universelle des droits de l'Homme.
- 3- Au respect de l'article 9 de la Constitution tunisienne qui prévoit que « *L'inviolabilité du domicile, le secret de la correspondance et la protection des données personnelles sont garantis* » et à ce que la messagerie des citoyens ne soit plus interceptée.
- 4- A faire cesser toute forme de censure et tout filtrage des contenus en ligne relatifs à la liberté d'expression et à ce que la question de la « gouvernance d'Internet » ne serve pas de prétexte pour réglementer de manière abusive les contenus d'Internet.
- 5- A abroger toutes les lois liberticides et notamment celles qui rendent un prestataire technique d'Internet responsable des contenus visités par les usagers et lever toutes les restrictions imposées aux Publinets.
- 6- A agir pour que toute décision concernant la légalité ou l'illégalité d'un site Web, ne puisse être prise que par une autorité judiciaire qui doit garantir les principes d'équité et d'indépendance.
- 7- A mettre les technologies de l'information au service du développement du citoyen et à cesser de criminaliser la navigation.
- 8- A ce que la liberté de publier des contenus écrits, audio ou vidéo sur Internet ne soit pas restreinte par aucune mesure réglementaire ou administrative.
- 9- A ce que l'accès à internet soit un espace public mondial ouvert et accessible à tous sans discrimination ni restriction.
- 10- A favoriser cet accès par tous les moyens y compris par voie satellitaire.

III- Introduction « médias dans une société fermée »

La Tunisie a été révélée au monde comme l'un des pays qui pratique une censure à large échelle sur Internet et de façon méthodique, lors de la tenue du Sommet mondial sur la société de l'information (SMSI) en novembre 2005. Au cours de ce sommet, le cadre international et extraterritorial du Sommet tenu sous l'égide de l'ONU n'a pas été respecté. La censure a été largement pratiquée dans l'enceinte du site ; Un rapport D'*Amnesty International* a été censuré et interdit de distribution. Des journalistes étrangers ont été agressés¹ ; Des sites Internet à contenu critique continuaient à être bloqués. Et surtout, la transmission directe du discours inaugural du président de la Confédération, Samuel Schmid, coorganisateur du sommet, a été interrompue sur la chaîne nationale tunisienne au moment où il prononçait ces mots : « *l'ONU compte encore parmi ses membres des Etats qui emprisonnent des citoyens au seul motif qu'ils ont critiqué leurs autorités sur Internet ou dans la presse...J'attends donc que la liberté d'expression et la liberté de l'information constituent des thèmes centraux au cours de ce sommet.* »

Catherine Trautmann, députée européenne qui conduisait la délégation du Parlement européen au sommet déclarait le 13 décembre 2005, lors de la séance plénière consacrée à l'évaluation du SMSI au Parlement européen « *Je déclare inacceptables les incidents graves qui ont entouré le sommet et porté atteinte à la liberté de la presse, à la liberté d'expression et de réunion, mais aussi aux personnes, ainsi que les événements qui ont visé notre délégation, en particulier le sabotage de l'atelier sur les droits de l'homme. Ils sont contraires aux engagements souscrits par la Tunisie dans les conclusions du sommet, de même que dans l'accord d'association, dont ils rompent ainsi la réciprocité.* ».

Après ces déclarations, une amnésie frappe les partenaires institutionnels européens et la Tunisie reprend sa place de « *pays modèle dans la coopération euro-méditerranéenne*² » applaudie pour ses performances en matière de droits humains par le président français, Nicolas Sarkozy qui déclare : « *L'espace des libertés progresse* » lors de sa visite en Tunisie en avril 2008.

Pourtant tous les rapports publiés par les ONG tunisiennes ou internationales³ continuent de pointer le rétrécissement de cet espace. Dans cette société fermée, le défi de la communication reste le problème numéro un.

¹ Agression à l'arme blanche dont avait été victime le journaliste de *Libération*, Christophe Boltanski, les journalistes de la *RTBF* ont eux aussi eu leur part de violences et leur cassette fut confisquée ; l'équipe de *TV5* décidait de plier bagage en réaction à une surveillance policière trop collante.

² Romano Prodi, l'ancien président de la Commission européenne, lors de sa visite officielle en Tunisie, le 1^{er} avril 2003

³ <http://cpj.org/reports/2008/09/tunisia-oppression.php>; <http://cpj.org/reports/2009/04/10-worst-countries-to-be-a-blogger.php>; http://www.rsf.org/article.php3?id_article=30272; http://campaigns.ifex.org/tmg/IFEXTMGreport_April2007_The_Siege_Holds.pdf;

Non satisfaites de verrouiller la presse et les médias audiovisuels, les autorités ont fait la chasse à ce nouvel outil de communication qu'est Internet. Une armada d'agents (plus de 400) est mobilisée au ministère des Communications pour traquer les internautes et surveiller leur navigation.

Un paysage médiatique pauvre malgré le pluralisme de façade

Dans un pays où le culte de la personnalité a atteint un niveau tel que l'encensement au quotidien du chef de l'Etat par les médias prend l'allure d'un véritable rituel, on comprend que Ben Ali entende faire des médias un outil de propagande qui loue ses réalisations et ne souffre aucune critique.

Et aux partenaires occidentaux, il vend un paysage médiatique « libéralisé et pluriel » avec 265 journaux et magazines, 2 TV et 3 radios privées. La réalité de cette façade, c'est que sur ces 265 journaux, il n'existe que 3 organes de partis d'opposition (subissant tous des restrictions) et zéro organe indépendant ; ces derniers ont été éradiqués dès 1990 peu après son accession au pouvoir. Quant aux chaînes de TV et radios privées, elles sont toutes la propriété des proches de Ben Ali, leurs licences ayant été accordées dans des conditions d'opacité totale.

La liberté d'éditer des journaux ou de diffuser des contenus TV ou radio libres est totalement confisquée. Aucune nouvelle autorisation de publier n'a été accordée à des médias indépendants depuis 1987, date de l'accession au pouvoir de Ben Ali. Seul un organe de parti d'opposition « [Muwatinoun](#) » a vu le jour en 2007. L'exemple de ce qui est arrivé à [Radio Kalima](#) en janvier dernier est éloquent sur la capacité de tolérance des pouvoirs publics d'une quelconque voix critique. Alors que cette radio émettait sur Internet et sur satellite à partir de l'étranger, ses bureaux ont été encerclés par la police⁴, ses journalistes arrêtés, son matériel confisqué, l'appartement qui hébergeait le studio mis sous scellés et sa rédactrice en chef, poursuivie pour « utilisation illégale de fréquences⁵ », l'instruction est encore en cours.

Quant aux journalistes, ils sont régulièrement harcelés et soumis à une pression telle que l'autocensure s'installe et domine leur production lorsqu'ils travaillent dans les médias officiels ou proches du pouvoir ; Ceux qui travaillent pour des médias étrangers sont systématiquement harcelés, privés de leur carte de presse, parfois agressés physiquement ou emprisonnés.

La tentative de putsch que vient de subir le syndicat national des journalistes (SNJT⁶) est la meilleure illustration de la volonté de main mise du pouvoir sur ce secteur et son intolérance à toute voix critique, fût-elle modérée.

⁴ <http://cpj.org/blog/2009/02/tunisias-radio-kalima-raided-shuttered-staffers-ha.php>

⁵ Cf la note juridique élaborée par les avocats de radio Kalima : <http://www.olpec-marsed.org/fr/News-file-article-sid-8.html>

⁶ <http://mena.ifj.org/en/articles/ifj-condemns-orchestrated-campaign-against-union-of-journalists-in-tunisia?format=print> ; <http://campaigns.ifex.org/tmg/>

IV- Internet et les mécanismes de la censure

Un réseau moderne qui couvre l'ensemble du pays

La Tunisie se prévaut d'avoir été le premier pays arabe et africain à se connecter à la toile. Ainsi dès 1991, la Tunisie est connectée à Internet à travers l'Institut Régional des Sciences Informatiques et des Télécommunications (IRSIT). En 1993, un réseau national de recherche et de technologie (RNRT) est créé pour connecter les centres de recherche Tunisiens. En 1996, l'Agence Tunisienne d'Internet (ATI) est créée pour développer la technologie réseau en Tunisie et servir d'opérateur Internet. Agissant sous la tutelle du Ministère des Technologies de la Communication, l'Agence Tunisienne d'Internet est le fournisseur en gros d'accès Internet en Tunisie.

Il faudra attendre la fin de l'année 1997, pour que les particuliers puissent disposer de deux fournisseurs privés à Tunis avec lesquels ils peuvent souscrire un abonnement Internet ; ils sont actuellement 5 répartis sur l'ensemble du territoire et s'ajoutent aux six fournisseurs de Services Internet déjà existants pour le secteur public.

La Tunisie est officiellement le pays d'Afrique du Nord qui connaît la connectivité la plus importante avec 4,12 % de taux de pénétration. Selon les statistiques du ministère des Communications, le taux de pénétration d'Internet dans les ménages était de 3,36 en 2007.

Le réseau national en câbles à fibres optiques couvre l'ensemble du pays, sous forme de boucles SDH articulées autour de commutateurs multiservices. Les connexions internationales sont assurées par des liaisons en câbles optiques sous-marins reliés à l'Europe, ainsi que des liaisons satellitaires.

Notons cependant que la Tunisie est le **seul pays africain qui interdit le raccordement par satellite aux particuliers**⁷ et l'usage d'une connexion satellitaire pour les particuliers est puni par la loi.

La téléphonie fixe demeure le monopole de **Tunisie Télécom**. Le réseau fixe, entièrement numérisé depuis 1999, compte 1,2 millions d'abonnés, soit une densité téléphonique de 25 lignes pour 100 habitants. L'ADSL en Tunisie est proposé sous forme d'une offre conjointe entre Tunisie Télécom et les fournisseurs des services Internet privés pour des débits allant de 256Ko à 2048Ko.

La Tunisie a connu un développement de son parc informatique ces dernières années, qui est passé à 472 000 unités en 2004.

En Avril 2009, l'ATI annonçait **305.960** abonnés⁸, dont **262.986** à haut débit et **2.960.000** utilisateurs Internet pour une population de 10 millions d'habitants qui connaît un taux d'alphabétisation de 74,30% ;

⁷ Cf http://www.rfi.fr/actufr/articles/075/article_42639.asp

⁸ <http://www.ati.tn/fr/index.php?id=90&rub=27>

Outre les abonnements particuliers, des centres Internet publics appelés « Publinets » ont vu le jour dès la fin 1998 ; En 1999, la Tunisie comptait 200 centres Publinets et l'Etat projetait de créer fin 2001, 400 nouveaux centres.

Internet, le media alternatif

Dès l'année 1999 Internet est investi par les jeunes et les dissidents qui y trouvent une fenêtre sur le monde et un espace alternatif où la parole citoyenne pouvait librement s'exprimer. Le net tunisien connaît une vraie effervescence.

Le premier qui a fait beaucoup de bruit a été le site *Takriz*, un webzine hébergé aux USA, Lancé en 1998 par deux étudiants ; au départ une simple liste de diffusion qui connaît un vrai succès et devient en 2000 un forum très fréquenté par les jeunes qui bousculent les tabous sous le couvert de l'anonymat. En août 2000, l'ATI bloque le site qui ne tarde pas à disparaître quelque temps après.

En Août 1999, le Conseil national pour les libertés en Tunisie (CNLT) qui venait d'essayer un refus d'enregistrement en tant qu'ONG, lance son site et son forum (hébergé au Canada) ; lui aussi sera un lieu de débat très fréquenté ; le site sera également bloqué peu de temps après son lancement.

A partir de l'étranger, des sites d'opposants exilés fleurissent ; Mai 2000 [Tunisnews](#) lance sa liste de diffusion qui atteindra sa vitesse de croisière et connaîtra un grand succès dès 2003.

En Octobre 2000, le magazine [Kalima](#) voit le jour, après un refus d'autorisation. Il sera également bloqué quelques semaines après son lancement.

En juillet 2001, Zouhair Yahyaoui lance [TUNeZINE](#). Ce site fera date et cristallisera la révolte des jeunes en dehors de tout cadre politique ou associatif. Zouhair Yahyaoui est arrêté en juin 2002 dans le publinet où il opérait, condamné à 2 ans de prison ferme pour « propagation de fausses nouvelles », il ne sera libéré qu'en novembre 2003. Zouhair décèdera en mars 2005 après avoir subi un harcèlement incessant de la police. Le site s'arrêtera quelques temps après sa mort, d'autres initiatives tenteront de faire revivre cette expérience qui a marqué toute une génération comme [réveil tunisien](#) et plus tard [Nawaat](#) en 2004.

Ces sites seront en quelque sorte le creuset où va se déployer une renaissance de la société civile tunisienne maintenue sous une chape de plomb une décennie durant.

Surprises par ces débordements inattendus, les autorités publiques vont de leur côté développer des mesures réglementaires et logistiques appropriées pour maintenir la toile dans les filets de la censure. Elles créent un véritable corps de police de l'information qui « veille » à la santé intellectuelle des Tunisiens.

Un dispositif réglementaire répressif

La censure de l'Internet est menée dans le cadre d'un large éventail de lois et de règlements administratifs. La Tunisie est le pays de la région qui a très tôt développé une réglementation sur

Internet la plus exhaustive et la plus sévère. Toutes ces lois ne sont pas mauvaises en soi, mais elles ont ceci en commun, elles donnent un pouvoir exorbitant et discrétionnaire à l'administration publique tout en limitant la marge de recours laissée au citoyen, qui est souvent impuissant à agir contre les abus de pouvoir d'une administration omnipotente et se sachant dans l'impunité totale. Nous en citons quelques unes de ces réglementations.

Arrêté du ministre des communications du 22 mars 1997,
« portant approbation du cahier des charges fixant les clauses particulières à la mise en œuvre et l'exploitation des services à valeur ajoutée des télécommunications de type Internet ».

Ce texte est le plus draconien de l'arsenal juridique relatif à l'Internet, car il rend le FSI (fournisseur de service Internet) responsable du contenu visité par ses clients et doit communiquer à l'opérateur public (ATI) la liste nominative de ses abonnés.

En effet l'article 9 stipule : « Le directeur désigné par le fournisseur de services conformément à l'article 14 du décret n° 97-501 du 14 mars 1997 susvisé, et dont le nom doit être communiqué à l'opérateur public concerné, **assume la responsabilité du contenu des pages et des serveurs Web qu'il est appelé à héberger** dans ses serveurs conformément aux dispositions du code de la presse sus visé. » et ajoute: « Le directeur est tenu d'assurer une surveillance constante du contenu des serveurs exploités par le fournisseur de services, pour ne pas laisser perdurer des **informations contraires à l'ordre public et aux bonnes mœurs.** » ! Par ailleurs le provider est tenu de « communiquer à l'opérateur public concerné la liste nominative écrite, dûment signée et actualisée, de tous ses abonnés au début de chaque mois. » Art.8.

Arrêté du ministre des communications du 9 septembre 1997
Cet arrêté fixe les conditions d'utilisation du cryptage dans l'exploitation des services à valeur ajoutée des télécommunications. Il oblige les FSI à obtenir une autorisation du ministère des communications pour l'utilisation de cryptage: « Tout fournisseur ou utilisateur de service à valeur ajoutée des télécommunications désirant recevoir ou transmettre des informations cryptées sur le service est tenu d'obtenir préalablement une autorisation l'habilitant à mettre en œuvre et à utiliser le cryptage (Art. 2); L'autorisation est octroyée à titre personnel et ne peut être transférée à un tiers qu'avec l'autorisation du ministre chargé des communications » (art.4).

Loi n° 98-38 du 2 juin 1998 relative au Code de la Poste
Le code de la poste autorise l'administration postale à confisquer tout courrier postal ou électronique pour « trouble à l'ordre public », il énonce dans son article 20 « Ne sont pas admis les envois qui ne répondent pas aux conditions prévues par les conventions internationales ratifiées et par les textes législatifs et réglementaires en vigueur ou les envois qui sont de nature à porter atteinte à l'ordre et à la sécurité publics ». et dans son article 21 : « Au cas où les envois prévus à l'article 20 du présent code sont trouvés, ils ne seront ni remis aux destinataires ni retournés à l'expéditeur, l'autorité compétente procède à leur confiscation conformément à la législation en vigueur ».

Loi n° 2001-1 du 15 janvier 2001, portant promulgation du code des télécommunications

L'Instance Nationale des Télécommunications est assimilée à une juridiction et connaît des litiges relatifs: - à l'interconnexion et à l'accès aux réseaux ; - aux conditions de l'utilisation commune entre les exploitants des réseaux des infrastructures disponibles. (Art. 67) et ses séances ne sont pas publiques (art. 69). Ce code organise les normes de cession des concessions de communication -jusqu'ici monopole d'état - aux privés, et place en passant toute activité d'émission, de réception ou d'exploitation de tout matériel de communication, sous contrôle des Ministres de la défense et de l'intérieur (art 52 et 56). Une « Agence nationale des fréquences » est créée, ainsi qu'un « Conseil national des communications ». Désormais l'exploitation d'une radio libre sans autorisation de l'Agence est passible d'une peine de cinq ans de prison ferme (art 82). Alors que jusqu'ici les radios n'étaient pas soumises à autorisation préalable. Est punie de la même peine toute personne qui se connecte à un réseau satellitaire (pour tout usage, même téléphonique par exemple) sans avoir reçu l'agrément de l'Agence (art 82) ou utilise les moyens ou les services de cryptologie (art.87).

Loi n°2000-83 du 9 août 2000, relative aux échanges et au commerce électroniques.

Qui crée « l'agence nationale de certification électronique » ;

Loi du 10 décembre 2003 sur le terrorisme

Loi n° 2003-75 du 10 décembre 2003, relative au soutien des efforts internationaux de lutte contre le terrorisme et à la répression du blanchiment d'argent. « Sont soumis au même régime que l'infraction qualifiée de terroriste, les actes d'incitation à la haine ou au fanatisme racial ou religieux quels qu'en soient les moyens utilisés. » (Article 6). Ce qu'il convient de relever c'est que depuis 2004, c'est la loi qui est la plus sollicitée pour sanctionner les infractions liées à la navigation sur Internet et l'accès à des sites prohibés.

Loi N° 2004-5 du 3 février 2004 relative à la sécurité informatique

Elle crée « l'Agence nationale de la sécurité informatique » qui fixe les règles générales de protection s réseaux et des systèmes informatiques et confie à l'agence la tâche d'auditer les systèmes informatiques.

Loi d'orientation n° 2007-13 du 19 février 2007,

relative à l'établissement de l'économie numérique ; cette loi porte essentiellement sur la capacité de l'Etat, les collectivités locales, les établissements et les entreprises publics peuvent conclure des conventions de partenariat par voie de négociation directe.

Art. 3. – L'Etat, les collectivités locales, les établissements et les entreprises publiques peuvent, dans le domaine de l'économie numérique, confier à une ou plusieurs entreprises économiques, l'accomplissement de la totalité ou d'une partie de leurs activités ou la participation à la réalisation des projets économiquement importants.

Art. 4. - Dans le cadre du partenariat entre le secteur public et le secteur privé dans le domaine de l'économie numérique, les conventions sont conclues par voie de négociation avec mise en concurrence sur la base des principes de l'égalité de traitement des participants et de la transparence des procédures.

Décret n°2008-2638 du 21 juillet 2008

fixant les conditions de fourniture du service téléphonie sur protocole internet.

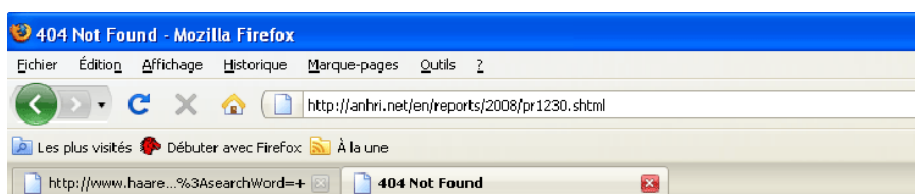
Décret n° 2008-2639 du 21 juillet 2008,

fixant les conditions et les procédures d'importation et de commercialisation des moyens ou des services de cryptage à travers les réseaux de télécommunications.

Une cyberpolice à la mesure de l'extension du réseau

La Tunisie a investi de grands moyens pour contrôler le trafic du web. Elle a mis en place une architecture où le contrôle se fait à plusieurs niveaux et assure ainsi le filtrage à l'épine dorsale du réseau (backbone).

Dès le départ les pouvoirs publics tunisiens ont fait de l'Internet en Tunisie un vaste intranet à l'échelle du pays. Normalement, lorsqu'une requête est faite par un individu sur son poste, celle-ci est transmise via des relais, jusqu'à atteindre sa cible. En Tunisie, ce circuit est interrompu au niveau d'un grand firewall qui va fermer le circuit et la requête suit un autre chemin. Elle va passer par un filtre qui va analyser la requête et décider si elle doit poursuivre son chemin ou pas ; si elle est autorisée, elle est transmise à un relais externe qui se trouve hors du territoire et renvoyer la réponse en chargeant la page demandée. Si la requête fait partie de la liste noire, un message d'erreur va s'afficher signalant que la page n'a pas été trouvée. C'est le fameux message **Error 404** (page not found), message d'erreur qui remplace le message de blocage que les internautes tunisiens ont ridiculisé en le rebaptisant « Ammar 404 »⁹.



Not Found

The requested URL /anhri.net was not found on this server.

Ce type de censure pose évidemment de sérieux problèmes relatifs aux libertés individuelles et à la protection de la vie privée qui est normalement protégée par l'article 9 de la Constitution qui prévoit que « L'inviolabilité du domicile, le secret de la correspondance et la protection des données personnelles sont garantis » ainsi que la Loi organique n° 2004-63 du 27 juillet 2004, portant sur « la protection des données à caractère personnel » qui stipule dans son article 1er : « Toute personne a le droit à la

⁹ http://www.letemps.com.tn/pop_article.php?ID_art=19839

protection des données à caractère personnel relatives à sa vie privée comme étant l'un des droits fondamentaux garantis par la constitution et ne peuvent être traitées que dans le cadre de la transparence, la loyauté et le respect de la dignité humaine et conformément aux dispositions de la présente loi. »

Ces dispositions sont en totale contradiction avec la réalité de la tutelle qu'exerce la cyberpolice sur les citoyens tunisiens en décidant à leur place ce qu'il convient de visiter et ce qui est illicite. Le contrôle du net est total grâce à ce verrouillage centralisé opéré formellement par le fournisseur en gros de l'Internet (ATI) ; **en réalité, ce n'est même pas l'ATI qui opère ce contrôle, mais un autre organisme directement rattaché au ministère de l'intérieur et à la présidence de la république qui sévit en toute opacité et l'ATI lui sert de paravent.**

Cette situation n'était pas pour plaire aux sociétés étrangères implantées en Tunisie qui souhaitent avoir la possibilité d'utiliser le VPN, (Virtual Private Network= réseau privé virtuel) et d'être reliées à l'entreprise mère et de partager leurs ressources en utilisant le chiffrement et l'authentification pour préserver le réseau virtuel des utilisateurs non-autorisés.

Il a fallu attendre 2005 pour que les entreprises étrangères puissent utiliser le VSAT, un réseau privé de communications par satellite pour transmission de données, entre leur siège social et ses succursales ; Le réseau VSAT, acquis depuis 2001 par Tunisie Télécom au prix de plusieurs centaines de milliers de dollars n'a jamais été mis en service et il a été délibérément gelé ; c'est finalement Divona qui a eu le privilège de l'exploiter, dans le cadre de la privatisation du secteur des télécommunications. Divona est détenue par Planet, principal fournisseur d'accès Internet détenue par Cyrine Mabrouk, la fille du président Ben Ali.

Les techniques de censure

Le filtrage de contenu

Il est techniquement aisé de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. C'est une technique basée sur le [SQUID](#) . Cela consiste à faire passer toutes les requêtes de pages Web par un point de contrôle qui est chargé d'autoriser ou non la demande. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de **liste blanche**, lorsqu'il s'agit d'une liste de sites interdits on parle de **liste noire**. Enfin l'analyse des réponses des serveurs conformément à une liste de critères (mots-clés, ...) est ce qu'on appelle filtrage de contenu.

Les autorités tunisiennes ont utilisé deux outils, [Websence](#) et [Smartfilter](#) pour opérer ce filtrage. La base des données d'adresses web (URL) est mises à jour quotidiennement. D'autres logiciels chinois sont utilisés actuellement.

- Les **keyloggers** ou enregistreurs de frappe au clavier ont pour fonction d'enregistrer furtivement absolument tout ce qui est tapé sur un clavier d'ordinateur, et de transmettre ces données à la source. Les keyloggers peuvent être installés à distance via un réseau, par le biais d'un troyen ou d'un virus, et ne nécessitent donc pas un accès physique à la machine pour la récupération des données collectées. La plupart des keyloggers enregistrent également le nom de l'application en cours, la date et l'heure à laquelle elle a été exécutée ainsi que les frappes de touches associées à cette application.
- **Troyens et virus** : Ils envoient également des troyens équipés d'un programme de type backdoor. De la même manière qu'un virus il est souvent dissimulé dans un fichier exécutable et peut emprunter les noms de vos fichiers. Une fois exécutés, ces troyens mettent en place une backdoor qui permet d'accéder à votre ordinateur aussi longtemps que vous êtes connectés à l'internet.

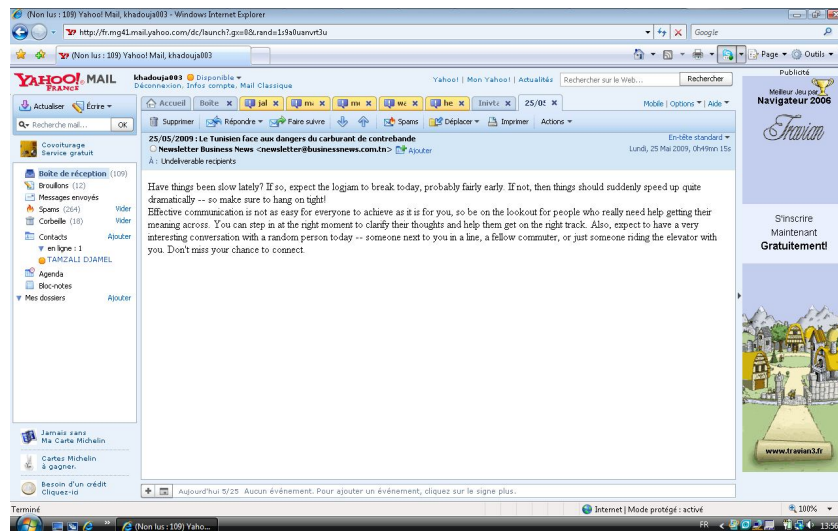
Surveillance et interception de la messagerie

C'est la technologie **Deep Packet Inspection (DPI)** qui est actuellement utilisée pour la surveillance de la messagerie ou la téléphonie internet VoIP (Voice over Internet Protocol).

Il s'agit d'un **détournement de trafic** ; ce dispositif est capable en temps réel de collecter les données (enregistrement des données aux fins d'examen) et de capturer à 10 gigabits par seconde. Le principe consiste à piquer des messages spécifiques ciblés sur la base d'une adresse e-mail, adresse IP, ou, dans le cas de la VOIP, d'un numéro de téléphone.

Pour ce faire, la cyberpolice va créer une adresse de surveillance ; pour chaque courriel qui entre et qui est destiné à la personne à surveiller, le logiciel va faire une copie du courriel entrant ou sortant et l'envoyer dans la boîte de surveillance.

- **Disparition du courrier et blocage de l'attachement**: Depuis 2008, les défenseurs de droits humains et journalistes indépendants ont fait l'expérience d'une nouvelle méthode d'interception du courrier qui ne cherche plus à se cacher et à opérer discrètement. Lorsque la boîte email est ouverte, elle affiche la liste des courriers entrants, dès que la personne clique sur le message voulu, le message disparaît et il est remplacé par un spam qui parle de la météo ou vous invite à un RV galant ou vous insulte en vous traitant de non patriote. D'autre part, lorsque vous envoyez un courrier et que vous cherchez à attacher un fichier, l'attachement est annulé. Il arrive également que le courrier soit envoyé, mais n'arrive jamais au destinataire.



Exemple de message original qui a disparu au profit d'un spam dans le courrier d'une dirigeante de l'ATFD

- Cette situation a poussé 3 ONG, la Ligue tunisienne de défense des droits de l'homme , l'Association tunisienne des femmes démocrates et l'Association des femmes tunisiennes pour la recherche sur le développement, à lancer en septembre 2008 un cri d'alarme: *« Nous sommes sérieusement handicapés dans notre travail depuis des mois. Nos mails sont devenus inaccessibles et quand ils le deviennent ils sont invisibles, illisibles et avalés. Malgré les différentes vérifications et réclamations auprès des différents services de l'Internet et des Telecom, les blocages des mails de nos associations et des mails personnels perdurent : il ne s'agit ni de problèmes techniques ni de problèmes de connexion mais bel et bien d'un contrôle de la société civile tunisienne autonome. Nous déplorons cette forme pernicieuse de censure qui bloque nos activités au quotidien. Nous faisons appel à tous nos partenaires pour prendre en considération cette situation de verrouillage et être compréhensifs des retards répétitifs de nos feed-back ».*
- **Coupure de la connexion** : Une autre méthode, expérimentée par la quasi-totalité des ONG indépendantes et notamment par L'OLPEC et le CNLT, c'est la coupure pure et simple de la connexion Internet par l'opérateur public Tunisie Télécom, bien que l'abonné soit en règle du point de vue paiement. Ainsi ces deux ONG qui partagent le même bureau ont pu obtenir discrètement un relevé de la fiche de réclamation traitée par leur FAI (voir fiche en annexe); cette fiche montre l'historique des réclamations effectuées par l'abonné durant neuf mois de l'année 2008. Sur ces 9 mois, il y a eu 16 réclamations pour cause d'interruption de trafic ; Le fournisseur d'accès envoie à Tunisie Télécom ses rapports où il signale « Modem Synchro et pas d'accès internet » ou « Pas de synchronisation » ; l'opérateur public de téléphonie fixe soit il s'abstient de rétablir la connexion, soit il la rétablit pour la couper à nouveau après quelques jours parfois.

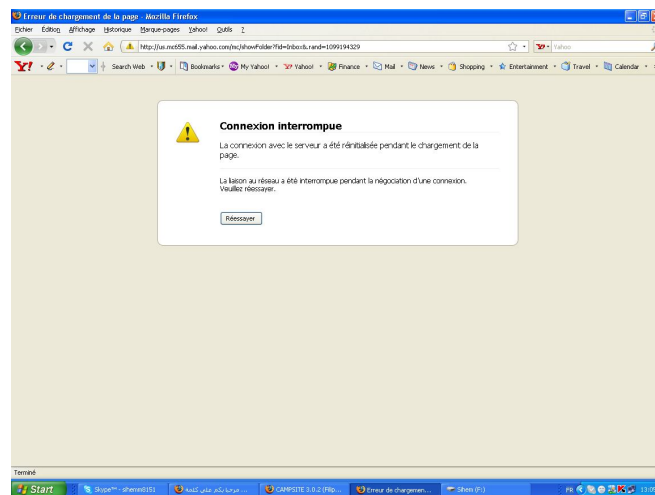
Fiche réclamation

Réclamation(s) traitée(s)

Référence réclamation	Numéro de téléphone	FSI	DTIR	Centre de gestion	Central	CCL
182671	71240907	Modem synchro et pas accès internet(15/07/2008 12:41:21) Connexion établie au moins une fois. Merci de vérifier cette ligne.4525		17/07/2008 07:44:11 Débit vérifié : oui Ports vérifiés : oui Ping : réussi Autres observations : Autres : TEST OK		
				06/02/2008 08:45:26		

Partie d'une fiche de réclamation (voir suite en annexe)

- **Blocage des ports** : Certains défenseurs ou opposants ont également fait l'expérience d'une page blanche avec une connexion internet qui fonctionne correctement. Peu de pages sont accessibles ou parfois aucune page ne s'affiche alors que l'icône témoin affiche un débit normal. Il s'agit en fait du blocage de certains ports ou de tous les ports sur des connexions de personnes ciblées. Par ailleurs, l'accès aux ports FTP (20, 21 ou 22) est fermé et soumis à autorisation, de même les ports alloués au trafic sécurisé (443 par exemple).



- Une autre méthode consiste à attribuer à un groupe de personnes (des personnalités de l'opposition et des ONG indépendantes) une adresse IP fixe après avoir identifié leur MAC adresse, et ainsi ils vont subir un contrôle spécifique d'un service spécialisé, c'est le cas de Ahmed Bouazzi, universitaire et membre dirigeant du PDP, qui a lancé le 25 mai 2009 une alerte sur le détournement de sa connexion Internet., voici un extrait de sa déclaration : « Depuis le milieu de janvier 2009, ma connexion s'est ralenti drastiquement, j'ai cessé de pouvoir

télécharger mon courrier électronique, utiliser le chat, accéder au service FTP, accéder au paiement sécurisé et même de pouvoir accéder à Facebook. Mes réclamations auprès de mon fournisseur de services internet m'ont révélé que ma connexion n'était plus branchée chez lui, et je me suis rendu compte qu'elle était plutôt rattachée à un autre fournisseur inconnu qui me fixait mon adresse IP au numéro 41.231.48.2 qui n'appartient à aucun fournisseur connu. Or, je paie un abonnement Internet à la société Tunisie Telecom aux termes duquel elle me connecte à mon fournisseur d'accès internet et me garantit un débit de 2 Mégabits/s ; la société en question ne me fournit pas ce pourquoi j'ai payé, pire, elle détourne d'une manière illégale ma connexion chez un fournisseur clandestin afin qu'il me ferme la majorité des services internet ordinaires...Suite à ces attaques, j'ai écrit au PDG de Tunisie Telecom, ensuite au ministre des technologies de communications, sans résultat. Je me suis trouvé alors dans l'obligation de demander justice auprès des tribunaux ; mon avocat a déposé une plainte contre Tunisie Telecom auprès du procureur de la République au palais de justice de Tunis le 13 mai dernier.»

Qui est censuré et qu'est ce qu'on censure ?

La manie de surveillance n'épargne personne ; Des opposants et ONG indépendantes aux ministres en passant par les opérateurs économiques, les membres du parti au pouvoir, les dirigeants des organisations nationales, les syndicats, les universitaires, les responsables régionaux, les ambassades, les différents corps de police et également des sondages aveugles chez de simples citoyens.

Jusqu'à fin 2007, les représentations diplomatiques se plaignaient de la surveillance, de l'interception de leurs courriels et du blocage de certains sites qu'ils ont l'habitude de consulter. Mais depuis, ils ont pu eux aussi souscrire des abonnements VSAT qui leur évite de passer par le chemin obligé de l'ATI et se connecter à Internet via le satellite.

Dans son discours officiel ou ses documents de propagande, le gouvernement affirme « *La liberté d'accès à l'Internet est une réalité en Tunisie....Des sites web parmi les plus critiques à l'endroit du gouvernement, y compris les sites d'organisations des droits de l'homme, sont accessibles aux citoyens tunisiens.* »¹⁰

Pourtant de nombreuses études et rapports révèlent le contraire. En 2006, une mission d'enquête de [IFEX](#) avait rencontré le ministre des Communications qui a reconnu qu'un blocage des sites est opéré sur les sites pornographiques ou terroristes uniquement. Dans son rapport de 2007¹¹, le TMG de IFEX affirme que « *Ces représentants nous ont en effet confirmé qu'un blocage systématique de l'Internet avait lieu, mais ont indiqué que le blocage des sites politiques ou d'information s'expliquait par le contenu terroriste ou haineux des sites visés. Or, les officiels du gouvernement se sont montrés incapables*

¹⁰ ATCE <http://www.tunisiemedias.com/references/internet.html>

¹¹ http://campaigns.ifex.org/tmq/IFEXTMGreport_April2007_The_Siege_Holds.pdf

de nommer quelque processus judiciaire ou réglementaire que ce soit, qui permettrait légitimement à de telles affirmations d'être contestées légalement. »

Le blocage des sites peut ne pas être total, mais partiel ; ainsi, un site peut être accessible, mais seule la page rapportant une information sur la Tunisie est bloquée, ce qui permet aux autorités d'affirmer que le site n'est pas bloqué et effectivement, cela n'est pas totalement faux, ni totalement vrai.

Un rapport publié en 2005 par *l'Opennet initiative* (ONI)¹² recense quatre types de contenus bloqués; les sites de droits humains, les sites politiques d'opposition, les sites de pornographie et les outils de contournement et de navigation anonymes ; Aujourd'hui, il faudra y rajouter les traducteurs automatiques, certaines encyclopédies en ligne comme *Wikipedia* (pas toutes les pages), les sites d'hébergement de vidéos tels *YouTube* et *Dailymotion* et plus récemment les réseaux sociaux comme *Facebook*.

Il convient de s'arrêter un instant sur le phénomène *Facebook* qui connaît une explosion et devient un véritable phénomène de société en Tunisie ; En août 2008, il a été bloqué, puis rouvert après 15 jours sur intervention expresse du président Ben Ali et après une vague de protestation¹³ qui a touché toute la société, y compris les sphères dirigeantes ; après sa fermeture, *Facebook* a vu ses membres doubler en l'espace d'un mois (passés de 28.000 à plus de 60.000), il continue de connaître une évolution exponentielle et pousse certains proches du pouvoir, comme le fameux Imed Trabelsi - qui vient d'être inculpé par le procureur d'Ajaccio¹⁴ de complicité de vol d'un yacht - à utiliser cette plateforme pour faire de la publicité pour l'ouverture de sa grande surface « Bricorama ».

A ce propos, il est utile de lire ce commentaire ironique, à lire au second degré, d'un journaliste paru sur un site officieux lors du blocage de *Facebook* en septembre 2008, pour comprendre l'ampleur de ce phénomène : « *Il faudrait donc, peut-être, penser à limiter drastiquement l'usage des e-mails aux seuls professionnels. Mieux : on pourrait ouvrir des bureaux spécialisés où des écrivains assermentés enverront à notre place les missives les plus urgentes. De quoi créer des emplois et résorber le chômage des diplômés d'arabe et de français...Que l'on sacrifie toute la Toile du net mondial, s'il le faut, si notre sérénité est à ce prix.*¹⁵ »

Cet épisode où la question de la censure de l'Internet a été mise sur la place publique, a été par ailleurs exploité par certains thuriféraires du régime pour appeler à plus de surveillance sur le net et à l'adoption de mesures réglementaires encore plus restrictives, comme l'a fait Borhane Bsaies, qui travaille pour l'*ATCE*, l'agence de propagande officielle « ...pour éviter les malentendus et les surenchères, il est urgent de réglementer davantage le secteur notamment en lien avec la surveillance et le blocage qui doit être exercé... il est de notre droit et de notre devoir de contrôler cette autoroute...et de la réglementer à

¹² <http://opennet.net/studies/tunisia>

¹³ [Tous contre la censure de Facebook en Tunisie](#)

¹⁴ <http://www.kalima-tunisie.info/fr/News-file-article-sid-13.html>

¹⁵ <http://www.webmanagercenter.com.tn/management/article.php?id=46326>

travers une loi qui définit clairement les normes d'utilisation et de navigation sur le net ...et mettre fin à l'anarchie qui y prévaut et qu'il convient de sanctionner. »¹⁶

¹⁶ http://www.assabah.com.tn/pop_article.php?ID_art=14204

V- Les publinets sous surveillance étroite

Les Publinets sont des centres publics d'Internet où des particuliers peuvent accéder à Internet. Ces derniers sont étroitement contrôlés et soumis à un cahier de charge contraignant. L'article 12 alinéa 5 du **décret 2481 du 10 décembre 1998 du ministère des communications fixant le cahier de charges des publinets** énonce que « l'enregistrement ou l'impression des documents téléchargés ou envoyés doivent passer obligatoirement par le gérant du publinet ou le technicien qui le remplace et que le poste ne doit pas comporter de lecteur de disquette »; il énonce également que le gérant doit « veiller à ce que le contenu visité par l'utilisateur doit être conforme aux normes autorisées par l'ATI » ; et qu'il « doit veiller à contrôler à distance le contenu du courrier électronique de ses clients ».

Au moment de leur lancement, les publinets ont été pris d'assauts par les jeunes tunisiens assoiffés d'échanges avec le monde extérieur. Cet engouement faisait pièce au déficit médiatique et modifiait le comportement des jeunes.

Profil des usagers de publinets

Selon une étude réalisée par Sami Ben Sassi¹⁷ en 2004 sur la fréquentation des publinets, il ressort que la durée moyenne d'utilisation d'un poste informatique relié à Internet est de 1 heure et 40 minutes. 18% des internautes de l'échantillon restent connectés moins d'une heure, 67 % entre 1 et 2 heures, 15 % plus de 2 heures. L'échantillon comprend 40 % de salariés, 56 % d'étudiants et scolaires et 4 % de personnes sans emploi. 64 % des personnes interrogées ont un niveau universitaire entre bac + 1 et bac +5, 3 % ont fait plus de 5 ans d'études supérieures, 29 % ont un niveau secondaire, 4 % primaire. Le taux moyen de retour au Publinet est 4 fois par semaine. 62 % des personnes interrogées se rendent régulièrement au même Publinet. Le coût moyen d'une heure d'Internet est de 1,35 dinars (1 dollar). Parmi les personnes interrogées 24 % ont moins de 20 ans, 64 % ont entre 20 et 30 ans, 12 % ont plus de 30 ans. La personne la plus jeune a 6 ans la plus âgée 50 ans. L'âge moyen de l'échantillon est de 24 ans. L'échantillon est composé à 70 % de garçons et à 30 % de filles. 83 % des personnes habitent à une distance inférieure ou égale à 1 km du Publinet où elles ont été interrogées. 20 % des individus déclarent avoir une activité de recherche sur Internet, 44 % déclarent avoir une activité de communication directe (chat) et 28 % n'utilisent que leur boîte email, 4 % déclarent jouer, 4 % déclarent ne pouvoir discerner leur activité principale sur le net.

Contrôle étroit et réduction du parc par fermeture administrative

Les jeunes sont rôdés aux techniques de contournements et parviennent à passer outre les mailles des filets ; de nombreux procès pour « terrorisme » n'ont pour éléments de preuves que des téléchargements effectués au nez et à la barbe des censeurs.

¹⁷ *Les publinets de Tunis, Une analyse microéconomique*, NETSUDS, n° 2, août 2004

Les autorités s'en inquiètent et le Ministère des communications multiplie les tours de vis et met la pression sur les gérants de publinets, sensés être responsables des contenus visités par leurs clients, mais ils sont débordés ; Les contrôles des inspecteurs qui relèvent régulièrement les historiques sur les postes n'y suffisent plus ; En 2004 on installe alors des mouchards sur les routeurs des serveurs reliés directement à l'ATI ; La technique la plus usitée consiste à activer la gestion des logs sur le routeur à l'entrée du lien. Lorsque cette fonction sur le routeur est activée, chaque connexion demandée par chaque utilisateur sera inscrite dans un fichier. On y retrouvera le numéro IP de l'utilisateur, la date, l'heure et le site que cet usager demande à voir.

Là encore, ces contrôles ne suffisent pas, les jeunes accèdent malgré cela aux sites prohibés. Les autorités adoptent alors une politique délibérée de restriction du parc publinet. De nombreux centres publinets sont alors fermés ; Il leur est reproché d'avoir laissé accéder des opposants ou des dissidents ; le prétexte invoqué sera par exemple l'absence d'accès aménagé pour handicapés, comme ce fut le cas à Médenine. D'autres gérants de publinets comme à Sfax (cas Slim Boughdhir) ou Zarzis (cas Abdallah Zouari), sont encouragés à aggraver physiquement ces usagers qui protestent contre l'interdiction d'accès qui leur est faite ou la font consigner par huissier notaire ; Mais c'est la victime qui sera poursuivie en justice pour entrave à activité commerciale ou diffamation, comme ce fut le cas pour Abdallah Zouari.¹⁸

En 1999 la Tunisie comptait 200 Publinets et l'Etat prévoyait de créer 400 nouveaux centres à la fin 2001. En juin 2002 en Tunisie il n'existait que 306 Publinets ; La moitié du parc se trouvant dans le grand Tunis. En 2009, le président de la chambre nationale syndicale des publinets, M. Samir Sahnoun lance un cri d'alarme « les **gérants des publinets sont de plus en plus nombreux à mettre la clé sous la porte. Sur les 400 professionnels qui opéraient il y a quatre ans dans le secteur, ils ne sont plus aujourd'hui qu'à peine 200 voire moins** »¹⁹; Aujourd'hui, l'ATI n'affiche plus sur sa page statistiques le nombre de publinets dont le parc s'est considérablement réduit.

Fichage des usagers

Depuis le début de l'année 2009, les autorités ont remis en service l'obligation pour les usagers de s'identifier avant de surfer; un nouveau programme appelé **Publisoft** est imposé par l'ATI à tous les publinets ; ils peuvent ainsi identifier quel utilisateur a essayé de visiter quel site; Ce programme consiste à obliger le client à s'inscrire en donnant sa carte d'identité ; ses données personnelles sont ainsi entrées dans l'application et le client reçoit en retour un username et un password qu'il gardera en permanence et sera valable dans tous les publinets ; il ne peut accéder au WEB que s'il entre ces données. Ce programme est directement relié à l'ATI qui sait ainsi en temps réel qui est l'utilisateur et où il se trouve et sur quels sites il est en train de naviguer;

¹⁸ http://www.rsf.org/article.php3?id_article=7866

¹⁹ Tunisia Today



De nombreux gérants de publinets ont rechigné à appliquer ce software, mesurant son impact négatif sur la fréquentation de leur clientèle qui va hésiter par deux fois à surfer sous l'œil vigilant de la cyberpolice. Ils ont parfois prétexté l'alourdissement des machines qu'un tel programme provoquait pour se défausser. Dans un premier temps, lors des contrôles de routine, les inspecteurs s'appliquaient à installer eux mêmes sur le serveur ce software ; et dans un deuxième temps, c'est la fermeture pure et simple qui attend le gérant, comme ce fut le cas de plusieurs publinets dans la capitale et notamment celui de la Marsa où la fermeture avait eu lieu violemment par des policiers et sous les yeux des clients en mars 2009 (voir photo en cover).

La justice à la rescousse quand la cyberpolice échoue

C'est souvent via Internet que la chasse à l'apprenti terroriste s'organise ; Il est très fréquent que dans les affaires où comparaissent des jeunes accusés de terrorisme, les pièces à convictions sont constitués d'informations téléchargées sur clés USB ou CD-Rom(cf rapport du CNLT « [Justice préventive](#) » ou le rapport du CRLDHT et ALT sur la [torture en Tunisie](#)).

VI- *La surveillance hors du territoire tunisien*

Nous avons vu que la volonté de contrôle est totale dans le territoire tunisien, mais la cyberpolice ne se contente pas de surveiller les Tunisiens en Tunisie, elle met tout en œuvre pour étendre également sa main mise sur l'activité des Tunisiens hors du territoire. Elle multiplie les attaques contre les sites web dissidents hébergés à l'étranger (tous le sont parce que les FSI refusent d'héberger ce type de contenu), elle surveille leur mails et leur connexions et envoie ses espions infiltrer la blogosphère.

Attaques des sites web dissidents hébergés à l'étranger

Il est pratiquement rare de trouver un site web ou un blog dissident à l'étranger qui n'a pas subi une attaque informatique qui a détruit ses archives ou l'a rendu inaccessible pour quelques jours. Durant l'année écoulée plusieurs sites ont ainsi été attaqués ; nous en citerons à titre d'exemple, le site d'informations le plus populaire [Tunisnews](#), de même [Kalimatunisie](#), [Tunisawatch](#), ou les sites d'opposition comme [PDPinfo.org](#) et [CPRtunisie](#) ou certains blogs comme [Reveiltunisien](#) ou [Nawwaat](#).

Ces attaques ne sont pas évidemment signées, mais toutes les victimes s'accordent à dire qu'il s'agit d'attaques commanditées par les services tunisiens ; Pour avoir écrit cela dans un [article](#) après l'attaque du site de Kalima en octobre 2008, Naziha Rjiba, la vice présidente de l'OLPEC, a été convoquée le 23 octobre et interrogée par le procureur de la république, le dossier est encore ouvert.

L'une des plus importantes opérations de hacking a été opérée contre deux sites tunisiens opposants [www.ennahdha.org](#) et [www.pdpinfo.org](#) hébergés tous deux à l'étranger, à très courte intervalle en février 2008 par le même hacker qui avait réussi à implanter dans les deux sites des [shells](#) insérés dans des dossiers. (voir screenshots en annexe)



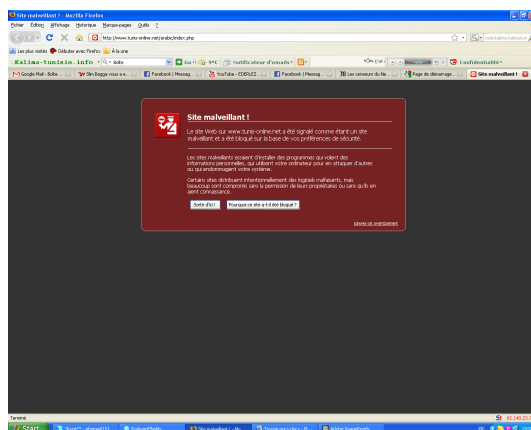
site du PDP



site d'Ennahdha



Un autre type d'attaque très virulent consiste à envoyer un trojan qui s'infiltré à travers un website vers l'utilisateur qui le visite et se démultiplie ; le but est d'attaquer tous les visiteurs qui visitent cette page ; les computers des victimes vont alors servir de source d'attaque d'autres usagers. Google et les moteurs de recherche vont alors signaler ce site comme malveillant et cette information sera transmise à la base des données des antivirus (Norton, Kaspersky...etc.) qui vont le définir comme un site malveillant et leurs clients vont le bloquer indirectement. Le 29 mai 2009, le site Tunis-online a subi ce genre d'attaque



[spoofing](#) ; Ces renifleurs ou « sniffeurs » sont des logiciels qui peuvent récupérer les données transitant par le biais d'un réseau local. Ils permettent une consultation aisée des données non-chiffrées et peuvent ainsi servir à intercepter des mots de passe ou toutes données qui transitent en clair. L'usurpateur peut non seulement voir les données qui transitent mais également les stocker pour les analyser ultérieurement ; comme il peut bloquer le passage de certaines données et jouer le rôle de censeur qui filtre le trafic vers et à partir de cette adresse IP.

Dans le cas du ARP spoofing ou ARP poisoning, le hacker se substitue en quelque sorte à la victime et récupère les données qui sortent de son ordinateur ou qui lui sont destinées, après avoir identifié son MAC adresse (son empreinte informatique) à travers son adresse IP. « C'est une technique utilisée pour attaquer tout réseau local utilisant le protocole de résolution d'adresse [ARP](#), les cas les plus répandus étant les réseaux Ethernet et Wi-Fi. Cette technique peut permettre à l'attaquant de détourner des flux de communication transitant sur un réseau local commuté, lui permettant de les écouter, de les corrompre, mais aussi d'usurper [une adresse IP](#) ou de [bloquer du trafic](#). Cette usurpation d'adresse IP se fait en envoyant un paquet ARP forgé par l'attaquant vers une machine A, afin qu'il envoie ses paquets à l'attaquant C, alors qu'ils étaient destinés à la victime B. De même, l'attaquant C envoie un [paquet ARP](#) forgé vers la victime B afin qu'elle envoie ses paquets à l'attaquant C au lieu de les envoyer à la machine A. Enfin, l'attaquant doit router les paquets de A vers B et inversement pour que la connexion entre la machine A et la victime puisse continuer. L'attaquant, en détournant le flux, peut ainsi voir les données qui transitent en clair entre les deux machines. » (Wiki).

A titre d'exemple, Sihem Bensedrine a subi ce genre d'attaque sur son ordinateur en Autriche et ne pouvait plus accéder à sa boîte email ou certaines pages web censurées en Tunisie comme [RSF](#) ou le quotidien algérien [ElWatan](#) durant plusieurs mois entre septembre 2008 et février 2009.

Infiltration de la blogosphère dissidente

Une autre technique utilisée pour harceler et discréditer les dissidents, consiste à infiltrer les forums et les sites qu'ils créent ou fréquentent en se faisant passer pour un opposant très critique et parfois insultant à l'égard des représentants du pouvoir. Une fois payé le ticket d'entrée, ils s'acharnent sur les personnalités dissidentes en vue en les diffamant et les discréditant. Cette méthode est très usitée par les *Mukhabarat* tunisiens (services secrets) qui parviennent à recruter à l'étranger des plumitifs qui exécutent la sale besogne pour eux. Ils interviennent dans les forums dissidents, mais ils ont également leurs sites propres ; Voici quelques sites dédiés à cette tâche. [Biladi](#) ; [samibenabdallah](#) ; [Kalima-horra](#) ;

VII- Conclusion :

L'absence de transparence dans la gestion des finances publiques ne nous permet pas de mesurer avec précision le budget investi en Tunisie et à l'étranger par les pouvoirs publics en vue de contrôler Internet et de bloquer toute information qui peut refléter une image négative sur les pratiques des responsables politiques tunisiens.

Mais ce qui est sûr c'est que des ressources considérables sont investies dans la surveillance de l'Internet, réparties entre le budget du ministère des Communications, du ministère de l'Intérieur, de l'ATCE et de la présidence de la république. Pour de nombreux observateurs ces ressources gagneraient à être investies dans des projets productifs et permettraient ainsi de résorber au moins 1/3 du chômage des jeunes diplômés tunisiens.

Il faudrait également relever le rôle des partenaires européens dans l'appui inconditionnel à cette politique du régime tunisien qui se fait au nom de la sécurité, de la lutte contre le terrorisme et de la stabilité dans la région.

Mais ce qu'il convient surtout de souligner, c'est que cette bataille où toute une armada de ressources humaines et matérielles est mobilisée pour fermer l'Internet aux usagers et contrôler leur messagerie en violant leur vie privée, est une bataille perdue d'avance et un combat d'arrière garde, car les moyens technologiques pour contourner la censure se développent aussi rapidement que ceux utilisés pour installer les mailles de la censure, rendant celle-ci inopérante.