Member of IFEX www.ifex.org

Observatoire

pour la Liberté de presse, d'édition et de création

Tunisie

OLPEC

www.olpec-marsed.org

Tunisia: Internet Censorship

A Rearguard Battle

Publinet closed by police in Tunis

Foreword

The purpose of this report is to provide an overview of state-sanctioned Internet censorship in Tunisia. It was written by non-experts, for non-experts, with the aim of exposing the regulatory and technical mechanisms of censorship, but more importantly, of assisting Tunisian rights defenders by providing them with the tools necessary to understand and protect themselves against the various forms of attack they regularly come under when accessing their e-mail or surfing the Net. But it is our hope too that it might foster a sense of citizenship as a rampart against marginalisation, particularly among young people, the largest users of the Internet.

Table of Contents

I - Executive summary

Tunisia was exposed to the entire world as a country in which large scale Internet censorship is methodically practised at the World Summit on the Information Society (WSIS) in November 2005.

Freedom to publish or broadcast has been completely appropriated by government. No new license to publish has been issued to an independent media outlet since 1987, the year Ben Ali came to power. *Muwatinoun,* the country's sole opposition paper, was launched in 2007.

Tunisia prides itself on being the first Arab and African country to be connected to the Net. Today, Tunisia boasts the largest connectivity figures in North Africa with a penetration rate of 4.12%, up from 3.36% in 2007, according to Ministry of Communications' figures. Landlines remain the monopoly of **Tunisia Telecom**. It is worth noting however, that Tunisia is **the only African country that forbids satellite connection for private citizens**[1] and where such satellite use is punishable under the law.

By 1999, dissidents and young people were flocking to the Internet in droves, drawn by the window it offered to the outside world and the alternative forum it presented for citizens' views to be freely expressed. The Tunisian net was abuzz with excitement.

Tunisian authorities, unprepared for public response to the new medium, were quick to develop the logistical and regulatory measures necessary to keep the Web entangled in their own censorship net. A veritable information police brigade was formed to watch over "the intellectual health of Tunisians."

Internet censorship is carried out through a wide range of laws and administrative regulations. Tunisia very early on developed the region's most extensive and strict regulation of the Web. Not all of these laws are bad in themselves; what they have in common, however, is the exorbitant and discretionary powers they give to public administrators, while at the same time limiting the recourse available to the private citizen, who feels, and often is, powerless before the abuses of an omnipotent administration.

Tunisia has invested a great deal in controlling Web traffic, erecting an infrastructure which allows for multi-level control, including backbone filtering.

From the outset, authorities have made the Internet in Tunisia little more than an intranet on a national scale. This type of censorship clearly poses a number of serious problems with respect to individual freedoms and the right to privacy, normally protected under Article 9 of the Constitution

[1] http://www.rfi.fr/actufr/articles/075/article_42639.asp

Control over the Internet is absolute, thanks to centralised locking officially administered by the ATI, the public operator; **in reality, it is not even the ATI that administers this control but another agency operating directly under the Ministry of the Interior and the president, and which does so with a complete lack of transparency.**

Tunisian authorities use two tools – Websence and Smartfilter – to conduct their content filtering; their database of web addresses (URLs) is updated daily. **Deep Packet Inspection** (DPI) is the technology currently used to monitor electronic messaging or Internet telephony (Voice over Internet Protocol - VoIP).

Who and what is censured? The authorities' obsession with Internet surveillance spares few people: from government critics and NGOs to ministers, traders, ruling party members, heads of national organisations, unions, academics, regional authorities, embassies, various police units and even everyday citizens.

Publinets are public Internet centres where private individuals can access the Internet. Users are heavily monitored and subjected to restrictive terms and conditions. In early 2009, authorities reinstated the requirement that all Internet users identify themselves before they begin surfing. A new programme called **Publisoft** was imposed by the ATI on all Publinets (see screen capture), allowing them to track which users attempt to visit which sites. The programme requires the client to register with his identity card; his personal information is then kept on file and he is given a username and password, which can then be used in any Publinet. At first, Publinet inspectors would simply install the software on the servers themselves during routine visits; later, operators in non-compliance were simply shut down, as was the case for many in the capital, and in La Marsa, where in March 2009, police used violence to close down one Publinet, while clients looked on (see cover photo).

The cyber police do not stop at monitoring Tunisians on national soil; they have also extended their stranglehold to the activities of Tunisians outside the country's borders. Cyber police have stepped up attacks on websites of dissidents hosted by other countries (which is all of them, since local ISPs refuse to host this type of content), and continue to monitor their e-mail accounts and connections, and spy on blogger activities.

Significant resources are invested in the monitoring of the Internet, spread over the budgets of communications and interior ministries, the ATCE and the president's office. Many observers argue that these resources would be better spent on more productive projects, and could reduce by at least one-third the jobless rate among Tunisian graduates.

Tunisia's European partners must also bear some responsibility for their unconditional support for these policies, undertaken in the name of security and regional stability.

II - Recommendations

OLPEC urges the Tunisian government to:

1 – Respect its obligations under international instruments, particularly those related to freedom of expression (Article 19 of the Universal Declaration of Human Rights as well as the International Covenant on Civil and Political Rights);

2 – Ensure that all legislation dealing with the dissemination of information on the Internet is founded on the principle of free expression, as defined by Article 19 of the Universal Declaration of Human Rights;

3 – Uphold Article 9 of the Tunisian Constitution, which stipulates that: "The inviolability of one's place of residence, the confidentiality of correspondence and the protection of personal information shall be guaranteed" and cease all interception of online and text messaging;

4 – Put an end to all forms of censorship and filtering of Web content relating to free expression and ensure that the issue of Internet governance does not become an excuse to introduce abusive regulations over web content;

5 – Repeal all laws threatening civil liberties, particularly those making Internet service providers responsible for websites visited by their customers, and lift all restrictions imposed on Publinets;

6 – Ensure that all decisions concerning the legality of websites are taken only by judicial authorities bound by the principles of fairness and independence;

7 – Allow information technology to serve the development of Tunisian citizens and put an end to the criminalisation of Internet surfing;

8 – Ensure that the right to publish text, audio or video content on the Internet is not restricted by regulatory or administrative measures;

9 – Make the Internet an open and global public forum, accessible to all without restriction or discrimination;

10 – Encourage this access by all available means, including satellite transmission.

III – Introduction: Media in a closed society

Tunisia was exposed to all the world as a country in which large scale Internet censorship is methodically practised at the World Summit on the Information Society (WSIS) in November 2005. During the summit, which was held under UN auspices, international and extraterritorial jurisdiction was blatantly flouted. Censorship was widely practised inside summit walls: an Amnesty International report was banned from distribution; foreign journalists were attacked[2]; Internet sites criticising authorities continued to be blocked. Above all, live broadcast of the inaugural speech of WSIS co-organiser Samuel Schmid, president of the Swiss Confederation, was interrupted on national television precisely as he spoke the words: "The UN still counts among its members states who imprison their citizens simply for criticising authorities on the Internet or in the print media… So I expect that freedom of expression and freedom of information will become central themes of this summit."

Catherine Trautmann, a member of the European Parliament and the head of its delegation at the summit, told a plenary session of Parliament devoted to an evaluation of the WSIS experience on 13 December 2005: "The serious attacks on freedom of the press, of expression and of assembly during the summit, not to mention on individuals, and the incidents targeting our delegation, in particular the sabotage of the human rights workshop, are completely unacceptable. They run counter to commitments undertaken by Tunisia in the Summit's conclusions, as well as in the association agreement, whose principal of reciprocity they clearly breach."

But a collective amnesia seemed to strike Tunisia's European institutional partners following Ms. Trautmann's remarks, and Tunisia once again claimed its place as "a model of Euro-Mediterranean cooperation[3]", praised for its performance in the area of human rights by French president Nicolas Sarkozy, who declared during his visit to Tunisia in April 2008: "The space for freedom is growing."

Yet all the reports published by Tunisian and international NGO's[4] continue to point to a shrinking of that space; in this closed society, the challenge of communication remains the number one problem.

---

[2] *Libération* reporter Christophe Boltanski suffered a knife attack; *RTBF* journalists were assaulted and had their tape confiscated; a *TV5* crew packed up and left in reaction to the oppressive police surveillance

[3] Romano Prodi, former president of the European Commission, during an official visit to Tunisia on 1 April 2003

[4] 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;

Not satisfied with their stranglehold on the press and the broadcast media, authorities have set their sights on the latest communication tool: the Internet. A veritable army of more than 400 agents has been mobilised within the Ministry of Communications to track Internet users and monitor their web use.

A superficial pluralism, masking a paucity of options

In a country where cult of personality has turned into a daily ritual of media praise, President Ben Ali's efforts to fashion a propaganda tool praising his every accomplishment while stifling all criticism, are clear.

To his partners in the West, he boasts of a "plural and free" media landscape, with 265 newspapers and magazines, two television stations and three private radio stations. The reality underneath this picture is quite different: only three of the 265 newspapers are owned by opposition parties (which face many restrictions) and none are independently owned, the last of these having been eliminated in 1990, shortly after Ben Ali came to power. Private radio and television stations are all owned by members of the president's inner circle, licensed under conditions lacking in any kind of transparency.

Freedom to publish or broadcast has been completely appropriated by government. No new license to publish has been issued to an independent media outlet since 1987, the year Ben Ali came to power. *Muwatinoun,* the country's sole opposition paper, was launched in 2007. The case of Radio Kalima in January 2009 speaks volumes about the regime's intolerance of any kind criticism. As the station was broadcasting on the Internet and via satellite from overseas, its offices were surrounded by police[5], its journalists arrested, its equipment seized, the apartment housing its studios shuttered and its editor-in-chief charged with "illegal use of frequencies[6]"; the case is still open.

Journalists are regularly harassed and subjected to such pressures that self-censorship reigns within both the state-run media and outlets run by those in the president's inner circle. Journalists working for foreign media outlets are routinely harassed, stripped of their press cards, and sometimes even physically assaulted or imprisoned.

[5] http://cpj.org/blog/2009/02/tunisias-radio-kalima-raided-shuttered-staffers-ha.php
[6] Cf legal arguments drafted by Radio Kalima lawyers

The recent takeover bid fought off by the national union of journalists (SNJT[7]) offers the best illustration of regime's efforts to exercise a complete stranglehold on the sector, and its inability to abide any form of criticism, however moderate.

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

IV – The Internet and the mechanics of censorship

A modern network covering the entire country

Tunisia prides itself on being the first Arab and African country to be connected to the Net. Since 1991 in fact, Tunisia has been connected to the Internet through the Regional Institute for Computer Science and Telecommunications (IRSIT). In 1993, a national network for research and technology (RNRT) was created to connect Tunisian research centres. In 1996, the Tunisian Internet Agency (ATI) was established to develop network technology in Tunisia and to serve as an Internet operator. Acting under the authority of the Ministry of Technology and Communication, the ATI became the country's wholesale Internet service provider (ISP).

But private citizens would have to wait until the end of 1997 before they would be able to sign on with one of Tunis's two independent service providers; today there are five, spread across the country, in addition to the six already in existence for the public sector.

Today, Tunisia boasts the largest connectivity figures in North Africa with a penetration rate of 4.12%, up from 3.36% in 2007, according to Ministry of Communications' figures.

A network of fibre-optic cables covers the entire country, in the form of SDH rings joined by multi-service switches. International connections are provided by way of fibre-optic submarine links to Europe, as well as via satellite.

It is worth noting however, that Tunisia is **the only African country that forbids satellite connection for private citizens**[8] and where such satellite use is punishable under the law.

Landlines remain the monopoly of **Tunisia Telecom**. There are currently 1.2 million fixed line subscribers in the country – a telephone density of approximately 25 lines for every 100 people – and the network has been fully digitalised since 1999. ADSL is offered jointly through Tunisia Telecom and privately service providers, at data transfer rates ranging from of 256 Kbps to 2048 Kbps.

Tunisia has also seen a growth in home computer ownership over the past several years, with figures reaching 472,000 units in 2004.

In January 2009, the ATI released figures on Internet use in Tunisia[9]: the total number of Internet users was listed at 2,810,000 over a population of 10 million, with a literacy rate of 74.3%. ATI's own subscribers numbered 282,914, including 227,221 high-speed users.

[8] http://www.rfi.fr/actufr/articles/075/article_42639.asp

Alongside home subscribers, public Internet cafés known as "Publinets" began to pop up around the end of 1998; by 1999, they numbered 200, with the government announcing plans to create another 400 centres by the end of 2001.

The Internet: the alternative medium

By 1999, dissidents and young people were flocking to the Internet in droves, drawn by the window it offered to the outside world and the alternative forum it presented for citizens' views to be freely expressed. The Tunisian net was abuzz with excitement.

A big part of that buzz was over one site in particular, *Takriz*, a webzine hosted in the US. Launched by two students in 1998, *Takriz* started out as a listserv but soon became so wildly popular that it was converted to an open forum in 2000, attracting young people eager to flout taboos under cover of anonymity. In August 2000, the ATI blocked the site; it disappeared shortly afterwards.

In August 1999, the Conseil national pour les libertés en Tunisie (CNLT) launched its own website and forum (hosted in Canada), after being refused NGO status in Tunisia. The CNLT site was a widely popular forum for debate, but it too was blocked by authorities shortly after its launch.

Outside the country, websites of opposition groups in exile flourished; *Tunisnews*, which launched its listserv in May 2000, quickly gained popularity and by 2003 had become a huge success.

In October 2000, the web magazine *Kalima* was launched after being denied a licence; it too would be blocked only weeks after its launch.

In July 2001, Zouhair Yahyaoui created *TUNeZINE*. The site's launch marked a turning point, crystallising youth anger outside of any political or community framework. Yahyaoui was arrested in June 2002 in the Publinet where he worked; he was sentenced to two years in prison for "spreading false news" but released in November 2003. Yahyaoui died in March 2005 after enduring near constant police harassment. Maintenance of his site stopped shortly thereafter but attempts to revive an experience that had marked an entire generation of Tunisians would soon follow, with sites such as Réveil tunisien, and later, Nawaat, in 2004.

These sites would become a sort of testing ground for a renascent civil society only beginning to emerge from the yoke under which it had struggled for over a decade.

[9] http://www.ati.tn/fr/index.php?id=90&rub=27

Tunisian authorities, unprepared for public response to the new medium, were quick to develop the logistical and regulatory measures necessary to keep the Web entangled in their own censorship net. A veritable information police brigade was formed to watch over "the intellectual health of Tunisians."

A repressive regulatory framework

Internet censorship is carried out through a wide range of laws and administrative regulations. Tunisia very early on developed the region's most extensive and strict regulation of the Web. Not all of these laws are bad in themselves; what they have in common, however, is the exorbitant and discretionary powers they give to public administrators, while at the same time limiting the recourse available to the private citizen, who feels, and often is, powerless before the abuses of an omnipotent administration. Below are some examples of these regulations.

Ministry of Communications Order of 22 March 1997

"setting out the terms and conditions for the implementation and the provision of value-added telecommunications services such as the Internet."

This text is the most draconian in the regime's legal arsenal regarding the Internet, as it holds service providers (ISPs) responsible for content visited by their customers and requires them to hand over their list of subscribers to the public operator (ATI).

Article 9 of the order states: "The director of the service provider, as defined by Article 14 of the aforementioned Order n° 97-501 of 14 March 1997, and whose name must be listed with the relevant public operator, **assumes responsibility for the content of web pages and servers he is asked to host** on his server, in accordance with the provisions of the aforementioned press code." Article 9 further states: "The director is responsible for ensuring constant monitoring of all content of servers accessed though the service provider, in order that **information contrary to public order and decency** not be allowed to flourish." (!) The service provider is also responsible for "providing the relevant public operator with a written list of all subscribers, duly updated and signed, at the beginning of each month." (Art. 8)

Ministry of Communications Order of 9 September 1997

This order sets out the terms and conditions for encryption use in the provision of value-added telecommunication services. Under the order, ISPs are required to obtain authorisation from the Ministry for use of encryption: "Any user or provider of value-added telecommunications services wishing to receive and/or to send encrypted information through the service must obtain prior authorisation enabling him to set up and use encryption" (Art. 2). "Authorisation is granted on an individual basis and cannot be transferred to a third party except by permission of the minister in charge of communications" (Art. 4).

Law n° 98-38 of 2 June 1998 governing postal services

The Postal Act authorises postal administrators to seize any mail - whether physical or electronic - suspected of "breaching public order". Article 20 of the law states: "It is forbidden to send mail which does not meet conditions set out by internationally ratified agreements or by the legal or regulatory texts in effect or which is liable to breach public order and security." Article 21 continues: "Should any such mail is found, it will neither be forwarded to the addressee nor returned to sender; the relevant authorities shall simply seize it in accordance with the laws in effect."

Law n° 2001-1 of 15 January 2001, promulgating the Telecommunications Act

The National Telecommunications Authority is equivalent to a court of law and settles disputes that arise over interconnection and network access, including the conditions of joint use of available network infrastructure (Art. 67). Its sessions are not public (Art. 69). The Act also sets out the terms and conditions under which the State, which previously held a monopoly on all communications services, may assign the provision of these services to private parties, and in so doing transfers authority over the broadcast, reception or use of any communications material to the Ministries of Defence and of the Interior (Arts. 52 and 56). A national frequencies agency is created, as well as a national council on communications. Private radio station operators, previously not subject to regulation, must now obtain prior authorisation from the agency or face up to five years in jail (Art. 82). Anyone connecting to a satellite network for any purpose, including telephone use, without having obtained prior authorisation from the agency faces similar punishment (Art. 82), as does anyone using encryption software or services (Art. 87).

Law n° 2000-83 of 9 August 2000 governing electronic commerce and exchanges

Creates the national agency for electronic certification

Law of 10 December 2003 on terrorism

Law n° 2003-75 of 10 December 2003, in support of international efforts to combat terrorism and crackdown on money laundering. "Anyone inciting hatred or racial or religious fanaticism, by use of any means, shall be subject to the same laws governing the offence of terrorism" (Art. 6). It is worth noting that since 2004, this is the law most invoked to sanction violations regarding Internet navigation and access to banned sites.

Law n° 2004-5 of 3 February 2004 governing information security

Creates the national agency for information security, which sets out the general rules designed to protect networks and information systems; the agency is also charged with the task of auditing information systems.

Blueprint law n° 2007-13 of 19 February 2007 governing the digital economy

This law establishes the right of the State, local authorities and publicly owned companies to enter into partnership agreements through direct negotiation.

Art. 3 – The State, local authorities and publicly owned companies may, with respect to the digital economy, entrust one or more commercial interests to execute all or part of their activities or to participate in the execution of projects of a larger scale.

Art. 4 – In digital economy partnerships between the public and private sector, contracts shall be awarded based on open and fair tendering procedures for all participants.

Order n°2008-2638 of 21 July 2008

Sets out the terms and conditions of telephone service provision via Internet Protocol

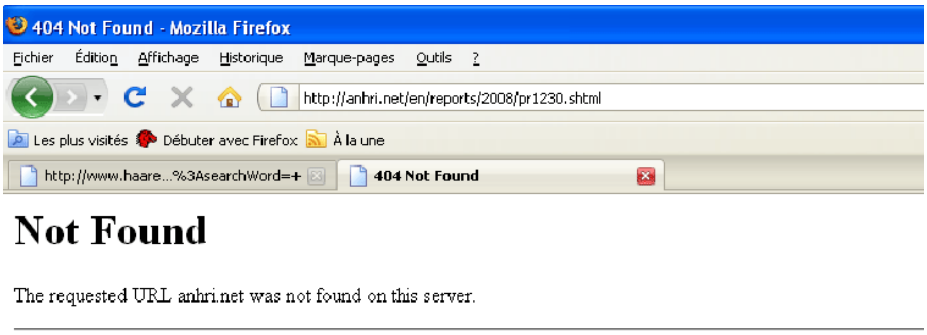
Order n° 2008-2639 of 21 July 2008

Sets out the terms and conditions for importing and marketing encryption software and services via telecommunications networks

A cyber police well-matched with a growing network

Tunisia has invested a great deal in controlling Web traffic, erecting an infrastructure which allows for multi-level control, including backbone filtering.

From the outset, authorities have made the Internet in Tunisia little more than an intranet on a national scale. Normally, when a request is made by an individual on his computer, the request passes through a number of relays before reaching its target. In Tunisia, the circuit is interrupted by a large firewall which closes the path, forcing the request to look for another one. It then passes through a filter which analyses the request and decides whether it may continue on its path or not; if the request is authorised, it is sent to an external relay, located outside national borders, which responds by loading the requested page. If the request is among the blacklisted sites, an error message is displayed indicating that the page could not be found. This is the famous **Error 404** (page not found) message that replaces the blocking message, and which Tunisian Internet users love to mock, renaming it, "Ammar 404"[10].



This type of censorship clearly poses a number of serious problems with respect to individual freedoms and the right to privacy, normally protected under Article 9 of the Constitution, which states: "The sanctity of the home, the privacy of correspondence, and the protection of personal information shall be guaranteed," as well as under Organic Law n° 2004-63 of 27 July 2004 governing the protection of personal information, which stipulates in Article 1: "Every person has the right to the protection of information regarding his or her private life as a

[10] http://www.letemps.com.tn/pop_article.php?ID_art=19839

fundamental right guaranteed under the Constitution and which shall be treated with transparency, fairness and human dignity in accordance with the provisions of the present law."

Such provisions are at odds, however, with the reality of a cyber police that controls Tunisian citizens by deciding for them which sites they may visit and which ones are forbidden. Control over the Internet is absolute, thanks to centralised locking officially administered by the ATI, the public operator; **in reality, it is not even the ATI that administers this control but another agency operating directly under the Ministry of the Interior and the president, and which does so with a complete lack of transparency.**

This situation did not please the owners of foreign companies with operations in Tunisia who wanted to use the Virtual Private Network (VPN) to share resources with their head office, using encoding and authentication to protect the virtual network against unauthorised users.

It was not until 2005 that foreign companies were able to use the VSAT (Very Small Aperture Terminal), a private satellite network for data transmission, between their head offices and the companies' various branches. The VSAT network, acquired by Tunisia Telecom in 2001 at a cost of several hundred thousand dollars, was never set up for use, then deliberately shelved; Divona Telecom eventually won the right to operate it after the telecommunications sector was privatised. Divona is owned by Planet, Tunisia's main Internet service provider; Planet is owned by Cyrine Mabrouk, the daughter of President Ben Ali.

Censorship techniques

Content filtering

Technically speaking, it is easy to filter Internet connections by analysing, on one hand, user searches, and on the other, server response. Web page searches are channelled through a control point, which will either authorise a request or deny it. When the filter is a positive one, i.e. the user's search is considered against a list of authorised searches, we speak of **whitelisting**; when it is compared to a list of banned sites, we speak of **blacklisting**. Finally, there is the analysis of server response according to a list of criteria (key words, etc.), which is called content filtering.

Tunisian authorities use two tools – Websence and Smartfilter – to conduct their content filtering; their database of web addresses (URLs) is updated daily.

Other tools used include:

- **Keyloggers**, which secretly record every keystroke typed on a computer keyboard and then transmit the data to their source. Keyloggers may be installed remotely via a network, either through a Trojan horse or a virus, and thus do not require physical access to the computer to recover collected data. Most keyloggers also record the name of the application in use, the date and time it was opened, as well as any keystrokes associated with the application.

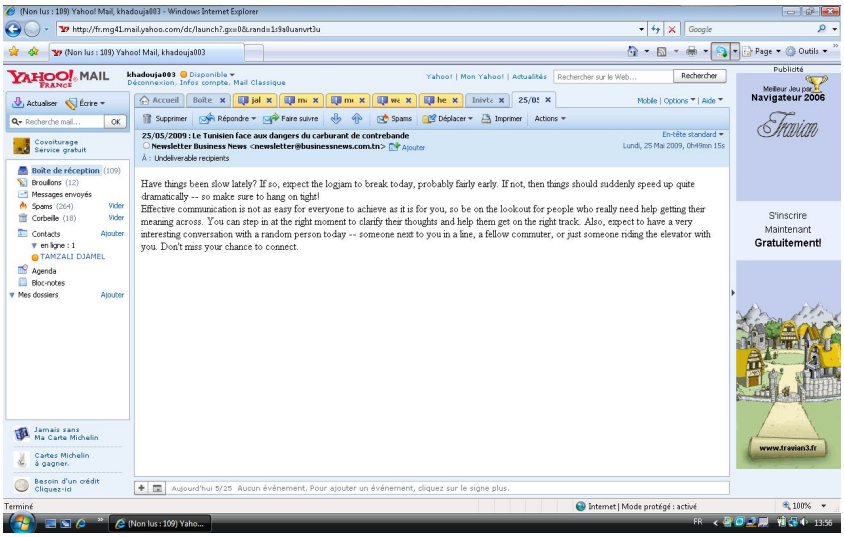
- **Trojan horses and viruses:** Trojan horses fitted with backdoor type programmes are also used. Much like a viruses, they are often hidden in executable files and can borrow names from the user's own files. Once executed, the Trojan horse opens a back door that allows the hacker access to the user's computer as long as it remains connected to the Internet.

Monitoring and interception of electronic messaging

Deep Packet Inspection (DPI) is the technology currently used to monitor electronic messaging or Internet telephony (Voice over Internet Protocol - VoIP). Traffic to the user's account is routed to another destination, where the system collects and records data at a rate of 10 GB per second. Specific messages may be "nabbed" based on e-mail address, IP address, or in the case of VOiP, telephone number.

To do this, the cyber police create a monitoring address; each time an e-mail is sent to or from the person being monitored, the software makes a copy of it and sends it to the monitoring address.

- **Disappearing mail and blocked attachments:** Since 2008, rights defenders and independent journalists have witnessed a new method of mail interception that abandons any pretence of discretion. When the inbox is opened, it displays the list of new messages; as soon as the user clicks on a message to open it, it disappears and is replaced by spam on the weather or an invitation to a swanky party or an insulting mail calling her unpatriotic. Moreover, when she attempts to send an e-mail with an attachment, the attachment is simply deleted. Other times, the e-mail is sent but never arrives at its destination.



The situation compelled three NGOs – the Tunisian League for Human Rights (LTDH), the Tunisian Association of Women Democrats and the Association of Tunisian Women for Development Research – to sound the alarm bell in September 2008: "We have been seriously handicapped in our work for months now. Our e-mails have become inaccessible and when they are not they are invisible, unreadable, or swallowed whole. Despite our numerous attempts to clarify the situation and our numerous complaints to the various Telecom operators and Internet service providers, blocking of our personal e-mail accounts and those of our associations continues. This is not due to any technical or connectivity problem but to a clear attempt to control Tunisian civil society. We condemn this insidious form of censorship which obstructs our daily activities. We ask too that our partners to be sensitive to our situation and understanding about our continuous delays in responding."

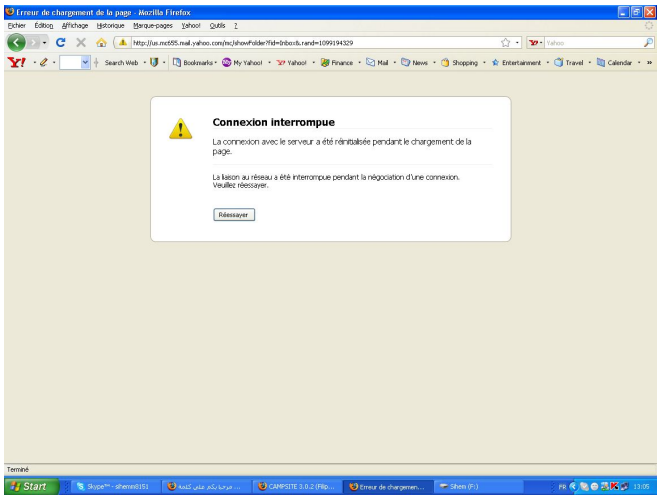
- **Cut connections:** Another method experienced by almost all NGOs, but especially by OLPEC and the CNLT, is the simple cutting of the user's Internet connection by Tunisia Telecom, the public operator, even though the account is in good standing. OLPEC and the CNLT, who share an office, were able to secretly obtain a record of complaints by their ISP to Tunisia Telecom over a nine-month period in 2008 (see appendix); in those nine months, 16 complaints were made over interruption of traffic. The ISP sends the telecom operator a report indicating the problem ("Modem synchronisation, no Internet access," or "No synchronisation") and the operator either ignores it or re-establishes the connection, only to cut it again a few days later.

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		

- **Blocked ports:** Some rights defenders and government opponents have also experienced blank pages, even with an Internet connection that is working normally. This occurs when few pages are accessible or a page does not display at all, though the status icon indicates normal loading. This is usually due to a blocking of some or all of the targeted person's port connections. Moreover, access to FTP ports (20, 21 or 22) may be closed and subject to authorisation, as well as access to ports allocated to secure traffic (443, for example).



- Another method consists of **attributing a fixed IP address** to certain groups (opposition figures or NGOs, for example) once their MAC address has been identified, thus allowing specialised departments to control their Internet activity. This was the case with Ahmed Bouazzi, an academic and member of the Parti démocratique progressiste (PDP), who, on 25 May 2009, launched an outcry over the diversion of his Internet connection. The following is an excerpt from his statement:

"Since mid-January 2009, my connection has slowed dramatically; I have not been able to download my mail, use chat features, access FTP or secure online payment services, or even access Facebook. Complaints to my Internet service provider revealed that my service had been disconnected and rerouted to another, unknown service provider who had set my IP address to 41.231.48.2, a number which does

not belong to any known service provider. Now, I pay an Internet service fee to Tunisia Telecom, under the conditions of which I am connected to my Internet service provider and guaranteed a bit rate of 2 megabits/s; yet not only has the company not provided me with the services I have paid for, worse still, they have illegally diverted my connection to a clandestine service provider so that a majority of even the most basic Internet services are not available to me. As a result of this attack, I wrote to the CEO of Tunisia Telecom, as well as to the minister of communications technologies, with no response. I thus found myself forced to seek justice through the courts. On 13 May 2009, my lawyer filed a complaint with the public prosecutor against Tunisia Telecom."

Who and what is censured?

The authorities' obsession with Internet surveillance spares few people: from government critics and NGOs to ministers, traders, ruling party members, heads of national organisations, unions, academics, regional authorities, embassies, various police units and even everyday citizens.

Until the end of 2007, foreign diplomatic offices even complained of monitoring, mail interception and blocking of certain sites they regularly visited; they have since been able to subscribe to the VSAT network, which allows them to bypass ATI channels and connect to the Internet via satellite.

In speeches and propaganda documents, the government claims: "*Free access to the Internet is a reality in Tunisia… Some of the websites most critical of government, including the sites of human rights organisations, are accessible to Tunisian citizens.*"[11]

Yet a number of studies and reports have revealed just the opposite. In 2006, an IFEX mission met with the communications minister, who acknowledged that blocking was used, but only on pornographic and "terrorist" sites. In a 2007 report[12], the Tunisia Monitoring Group (TMG) asserted: "These representatives in fact confirmed to us that systematic Internet blocking was taking place but explained that the blocking of news or political sites was justified by the terrorist or hateful content on the sites. Yet government officials were unable to name a single judicial or statutory procedure that would allow for those claims to be legally contested."

Blocking of sites may only be partial; for example, a site may be accessible but only the pages reporting on Tunisia blocked, allowing authorities to claim that the site is not being blocked, which, in effect, is not totally untrue.

[11] ATCE http://www.tunisiemedias.com/references/internet.html
[12] http://campaigns.ifex.org/tmg/IFEXTMGreport_April2007_The_Siege_Holds.pdf

A report published in 2005 by the OpenNet Initiative (ONI)[13] lists four categories of blocked content: human rights websites, political opposition websites, porn sites and sites offering anonymous surfing and circumvention tools. Today, the list would include automated translators, online encyclopaedias such as *Wikipedia* (not all pages), video hosting sites such as *YouTube* and *Dailymotion*, and, more recently, social networking sites such as *Facebook*.

It is worth pausing for a moment to look at the case of *Facebook*, which has exploded in Tunisia and become something of a social phenomenon. In August 2008, *Facebook* was blocked for 15 days and then reopened after a wave of protests[14] extending across all of society, including the ruling class, forced President Ben Ali to personally intervene. After the closure, the site saw its membership more than double in the space of a month, climbing from 28,000 to 60,000. *Facebook* continues to experience an exponential growth that has not gone unnoticed among those in the president's inner circle, including well-known businessman Imed Trabelsi – recently indicted by Ajaccio's public prosecutor[15] as an accessory in a yacht theft – who used the site as a platform to advertise the opening of his new box store, Bricorama.

To fully grasp the extent of public response, it is worth reading this tongue-in-cheek comment by a journalist which appeared on an unofficial site during the *Facebook* blocking of September 2008: *"Maybe we should consider drastically limiting e-mail use to professionals only. Better yet, we could set up specialised offices where writers under oath would send the most urgent missives for us. That way, we would create jobs and absorb the unemployed masses of French and Arabic language grads… Let the entire world Net be sacrificed, if necessary, if that is the price of our peace.[16]"*

But the *Facebook* episode, which focussed the public spotlight on the question of Internet censorship, was also exploited by regime toadies like Borhane Bsaies, an employee with the ATCE (the official propaganda agency), who saw it as an opportunity to call for more monitoring of the Web and the adoption of yet more restrictive regulatory measures: "…in order to avoid misunderstanding and one-upmanship, it is urgent that we strengthen our regulation of the sector, particularly in the monitoring and blocking of sites… it is our right and our responsibility to control this highway… and to regulate it through laws which clearly define the conditions of use and of net surfing… and put an end to the anarchy that now reigns and which must be sanctioned."[17]

[13] http://opennet.net/studies/tunisia
[14] Tous contre la censure de Facebook en Tunisie
[15] http://www.kalima-tunisie.info/fr/News-file-article-sid-13.html
[16] http://www.webmanagercenter.com.tn/management/article.php?id=46326
[17] http://www.assabah.com.tn/pop_article.php?ID_art=14204

V- Publinets under tight surveillance

Publinets are public Internet centres where private individuals can access the Internet. Users are heavily monitored and subjected to restrictive terms and conditions. Article 12, paragraph 5 of **Ministry of Communications Order n°2481 of 10 December 1998 governing Publinet operation** states that: "Copying or printing of downloaded documents must be done by a Publinet manager or by the technician in charge," and that computers "must not be equipped with disk drives." The article further states that Publinet managers "must ensure that content visited by users is in compliance with standards set out by the ATI," and that they "must control by remote access the content of clients' electronic mail."

Publinets have nevertheless transformed the behaviour of Tunisia's youths. From the moment they were launched, young people thirsting for a chance to connect to the outside world flocked to them in droves, heartened by the relief they offered in an arid media landscape.

Profile of Publinet users

According to a 2004 study on Publinet use conducted by Sami Ben Sassi[18], the average time spent online at a Publinet workstation is 1 hour and 40 minutes. Among those polled, 18% spent less than an hour online, 67% spent between 1 and 2 hours, while 15% were connected for more than two hours. The representative sample comprised 40% wage earners, 56% students and schoolchildren, and 4% unemployed persons. 64% of those questioned had completed between 1 and 5 years of university, 3% had completed more than 5 years of university, 29% had completed secondary school, while another 4% had completed primary school. The average rate of Publinet use was four times per week. 62% of those polled said they frequented the same Publinet. The average cost of one hour of Internet use was 1.35 dinars (approx. $US1). Among those polled, 24% were under 20, 64% were between the ages of 20 and 30, and 12% were over 30. The youngest person polled was 6, the oldest, 50. The average age of the sample was 24. 70% of respondents were male, 30% were female. 83% of respondents said they lived one kilometre or less from the Publinet where they were polled. 20% of respondents said they used the Publinet for their Internet searches, 44% said they used it for direct online communications (chatting), 28% used it only to check their e-mail, 4% used it to play games, while another 4% said they didn't know what their main Internet activity was.

[18] *Les publinets de Tunis, Une analyse microéconomique,* NETSUDS, n° 2, August 2004

Tighter surveillance and reduced public access

Young Tunisians are well versed in circumvention techniques and easily slip through the government's net; many of the "terrorist" cases that have made their way to the courts cite as their only evidence documents downloaded under the nose of censors.

The situation has authorities worried. The Ministry of Communications has clamped down on Publinet owners, already overwhelmed by the task of policing content visited by their clients. But regular Publinet inspections to record computer search histories were not enough; in 2004, authorities installed tracking devices directly connected to the ATI on server routers. The most common of these devices activates a log file on the router every time a connection is made; the requested page is then recorded in the file, along with the user's PIN, and the date and the time of the search.

But surveillance mechanisms such as these are not enough to deter Tunisian youth, who manage to access prohibited sites despite the measures. Now, authorities have adopted a deliberate policy of restricting the number of Publinets. Many of them have already been shut down for allowing access to government critics or dissidents, though the official reason given might be the lack of wheelchair access, as was the case recently in Médenine. Elsewhere, Publinet operators are encouraged to physically assault such users if they object when they are barred from entering. This was the case with Slim Boughdhir in Sfax and with Abdallah Zouari in Zarzis. And it is the victim who is then prosecuted for obstructing business activity or for defamation, as was the case for Zouari[19].

In 1999, there were 200 Publinets in Tunisia and the government had just announced plans to create another 400 by the end of 2001. By June 2002, there were only 306, with more than half that number located in the greater Tunis area. In 2009, the president of the national employers' federation for Publinets, Mr. Samir Sahnoun, sounded the alarm: ***"More and more Publinet owners are closing shop. Of the 400 operating four years ago in this sector, there are less than 200 left, if not fewer."***[20] Today, the ATI no longer even lists the number of Publinets on its statistics page.

Keeping files on users

In early 2009, authorities reinstated the requirement that all Internet users identify themselves before they begin surfing. A new programme called **Publisoft** was imposed by the ATI on all Publinets (see screen capture), allowing them to track which users attempt to visit which sites. The programme requires the client to register with his identity card; his personal information is then kept on file and he is given a username and password, which can then be used in any Publinet. Users will not be allowed to access the net until they enter this

[19] http://www.rsf.org/article.php3?id_article=7866
[20] Tunisia Today

information. The programme is linked directly to the ATI, allowing officials to know who the user is and exactly where he is located and to track, in real time, which sites he is surfing.

Many Publinet owners balked at installing the software, fearing the negative impact it would have on business if users began to think twice about surfing under the watchful eye of the cyber police. Citing the burden such a programme would impose on their equipment, many rejected the software. At first, Publinet inspectors would simply install the software on the servers themselves during routine visits; later, operators in non-compliance were simply shut down, as was the case for many in the capital, and in Marsa, where in March 2009, police used violence to close down one Publinet, while clients looked on (see cover photo).

When the cyber police fail, the courts to the rescue

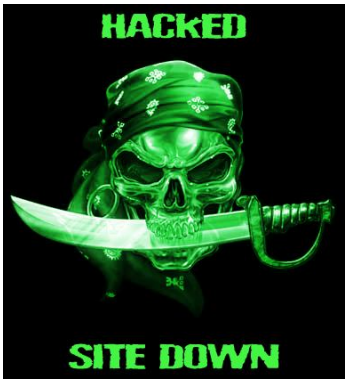
Hunting down novice terrorists in Tunisia is often done through the Internet. Frequently, in cases where young people have been accused of terrorism, the only proof offered in support of the claim is information downloaded onto a USB key or a CD Rom (see CNLT report "Justice préventive" or the report of the CRLDHT and ALT on torture in Tunisie).

VI - Surveillance beyond national borders

We have seen from examples that the quest for Internet control in Tunisia is absolute, but the cyber police do not stop at monitoring Tunisians on national soil; they have also extended their stranglehold to the activities of Tunisians outside the country's borders. Cyber police have stepped up attacks on websites of dissidents hosted by other countries (which is all of them, since local ISPs refuse to host this type of content), and continue to monitor their e-mail accounts and connections, and spy on blogger activities.

Attacks on websites hosted abroad

It is almost impossible to find a dissident blog or website hosted outside national borders that has not been the victim of a hacker attack that destroyed its archives or rendered it inaccessible for several days. In the past year alone, a number of sites were victims of such attacks: the popular news site Tunisnews, as well as Kalimatunisie and Tunisawatch, opposition sites PDPinfo.org and CPRtunisie, and blogs such as Reveiltunisien and Nawwaat.

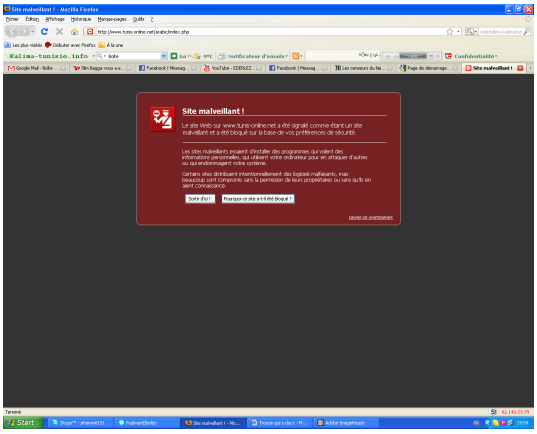


site du PDP

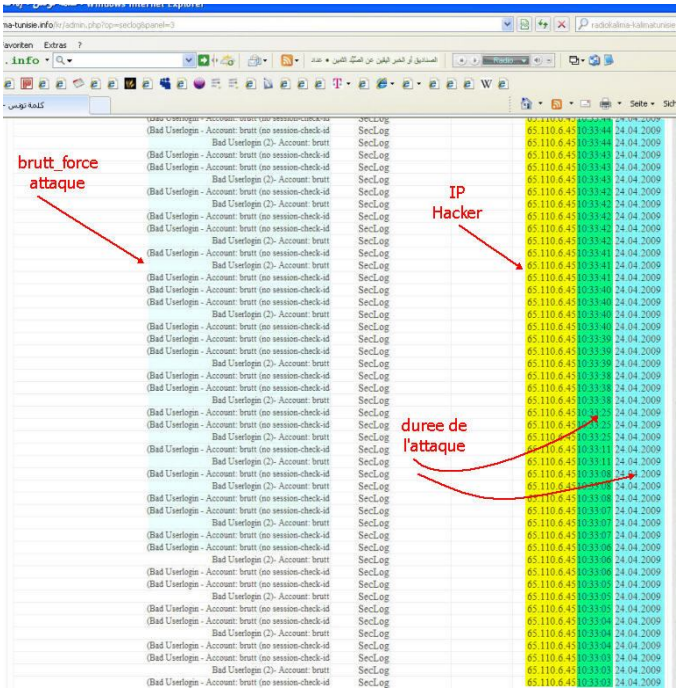
site d'Ennahdha

Though no one has claimed these attacks, the victims all agree that the Tunisian government is behind them. Naziha Rjiba, vice-president of OLPEC, openly said as much in an article posted on the Kalima website in October 2008, shortly after the attack on the site; on 23 October, she was summoned for questioning by the public prosecutor. The case is still open.

Another type of very virulent attack is to send a Trojan that seeps through a website user to visit it and multiplies, the goal is to attack all visitors who visit this page, and the computers of victims will then serve as a source of attack on other users. Google and other web search engines will then report the site as malicious and this information will be transmitted to the database of virus (Norton, Kaspersky etc ....) Which will be defined as a malicious site and their customers will block it indirectly. On May 29, 2009, the Tunis-online site has undergone this kind of attack.



Kalima's new site, rebuilt to better resist such attacks, was hit again on 24 April 2009; in just over four minutes, the site fought off more than 380 Brute force[21] attacks attempting to detect administrator passwords and gain access to the control table. Fortunately, all were unsuccessful. According to one IT technician: "Brute force attacks shouldn't last long; you don't want to be noticed by site administrators. Usually they're no more than two minutes max, which should be enough time to crack the site's password and attack it."



Monitoring connections of dissidents abroad

Tunisia's cyber police are equally interested in the activities of dissidents living abroad. For this work, however, they must rely on intermediaries such as intelligence agents (as part of an exchange of services, for example), Tunisian students living abroad (in exchange for special favours or threats of passport confiscation) or simply buy the services of foreign hackers who can take over their surveillance activities for them.

The methods used are classic, such as packet sniffing or ARP spoofing. These "sniffers" are a type of software that can pick up data sent over a local network, allowing the user to easily view any non-numerical information, as well as intercept passwords or any other unscrambled data sent over the network. The hacker can not only view the data but can also save it for later analysis. He can even block certain information from being sent, playing the role of censor with incoming and outgoing traffic.

[21] http://en.wikipedia.org/wiki/Brute_force_attack

In the case of ARP spoofing or ARP poisoning, the hacker poses as the victim, so to speak, associating his MAC address (a sort of IT fingerprint) with the victim's IP address in order to intercept traffic intended for that address or outgoing from it. "The technique is used to attack local networks that use an Address Resolution Protocol (ARP), the most common being an Ethernet wired or wireless network. The technique allows the attacker to divert the flow of communications on a switched local network, making it possible to listen to or corrupt them, but also to spoof an IP address or to block traffic. IP address spoofing occurs when the attacker sends a forged ARP packet to machine (A) so that its packets will then be diverted to the attacker (C), although they were intended for the victim (B). Similarly, the attacker (C) may send a forged ARP packet to the victim (B), so that his packet will be diverted to the attacker (C), instead of their reaching their intended destination (A). The attacker must also route A's packets to B and vice versa so that the connection between (A) and the victim (B) is maintained. By diverting this flow, the attacker can now view any uncorrupted data sent between the two machines." (Wiki)

Recently, OLPEC's secretary general, Sihem Bensedrine, was the victim of such an attack on her computer in Austria; for several months between September 2008 and February 2009 she could not access her e-mail or certain websites censored in Tunisia such as RSF and El Watan.

Infiltrating dissidents' blogs

Another technique authorities use to harass and discredit dissidents living abroad consists of infiltrating the forums on sites they've created or visit regularly and passing themselves off as highly critical, and often abusive, opponents of the regime. Once accepted into the club, they attack other dissidents in the forum, libelling and discrediting them. The method is a popular one among Tunisian secret service agents (*Mukhabarat)*, who recruit scribes to do the dirty work for them. These writers are regular contributors to dissident forums, but they can also have their own sites, as in these examples: Biladi; samibenabdallah; Kalima-horra.

VII- Conclusion :

The absence of any transparency in the management of public finances makes it impossible to calculate with any degree of accuracy the sums invested by authorities in Tunisia and abroad to control Internet use and block any information that might reflect negatively on the activities of those in power.

What is certain, however, is that significant resources are invested in the monitoring of the Internet, spread over the budgets of communications and interior ministries, the ATCE and the president's office. Many observers argue that these resources would be better spent on more productive projects, and could reduce by at least one-third the jobless rate among Tunisian graduates.

Tunisia's European partners must also bear some responsibility for their unconditional support for these policies, undertaken in the name of security and regional stability.

But most importantly it must be said that this battle, which has mobilised a veritable army of human and material resources to cut off Internet access to users and monitor their mail by violating their privacy, is a rearguard battle, lost before it began, because the technology used to circumvent censorship is developing as quickly as the one used by the censors to cast their nets, making those nets increasingly ineffective.