COMMENT LE FBI, LE PS ET ESTROSI ONT MIS LE NET SOUS SURVEILLANCE

LE 4 MARS 2011 ***JEAN MARC MANACH***

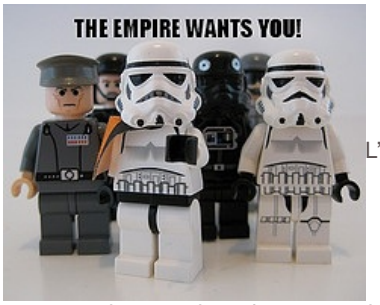
Le décret sur la "conservation des données de connexion" est la conclusion logique d'une dérive sécuritaire entamée il y a 10 ans maintenant, au lendemain des attentats du 11 septembre 2001. En voici l'histoire.

Vous imaginez une démocratie où la loi oblige les opérateurs de transport en commun et sociétés autoroutières à installer mouchards et caméras pour garder la trace, pendant un an, des endroits que les gens ont visités, de comment ils y sont allés, des personnes qu'ils ont rencontrées, et de ce qu'ils ont pu échanger ou partager ? Ce pays, c'est la France de 2011.

Un décret publié au JO le 1er mars contraint les fournisseurs d'accès à l'internet, les hébergeurs et prestataires de services web et de réseaux sociaux à conserver les données permettant d'identifier qui sont les gens qui vont sur l'internet, ce qu'ils y font, quand, et comment.

Ce **décret Big Brother** "*relatif à la conservation des données de nature à permettre l'identification de toute personne physique ou morale ayant contribué à la création d'un contenu mis en ligne*", est la conclusion somme toute logique d'une histoire commencée il y a près de 20 ans et qui s'est formidablement accélérée au lendemain des attentats du 11 septembre 2001.

Une demande pressante du FBI



L'histoire de la surveillance des internautes commence en 1993, alors que le web est en train d'exploser. En juin de cette année, on **dénombrait** 130 sites Web, et 623 en décembre. Les premiers navigateurs, Lynx, puis NCSA Mosaic, font exploser les usages, qui croissent à un rythme annuel de 341 634 %.

Cette même année, les autorités américaines commencent à mener une **intense activité diplomatique** afin de persuader les pays européens et l'OCDE de déployer des mesures de surveillance et d'interception des télécommunications, sous les auspices d'une organisation d'experts européens et américains, ILETS (pour *Interception Law Enforcement Telecommunication Seminar*).

Fondée par le FBI, son existence fut révélée par **Duncan Campbell**, dans le **rapport** que le parlement européen lui avait demandé de consacrer, en 1999, au réseau Echelon anglo-saxon d'interception des télécommunications.

Ses travaux débouchèrent, en 1995, sur l'**adoption** d'une résolution européenne relative à l'interception légale des télécommunications, largement inspirée du Communications Assistance to Law Enforcement Act (CALEA) américain, adopté en 1994, là aussi à l'initiative du FBI, afin d'imposer aux compagnies téléphoniques et aux fournisseurs d'accès internet de modifier leurs infrastructures pour faciliter la surveillance des réseaux.

Dans la foulée, **ENFOPOL** (pour "*ENFOrcement POlice*"), groupe de travail réunissant les ministères de l'intérieur des pays membres de l'Union considéré par certains comme la réponse européenne à l'organisation anglo-saxonne ECHELON, tente de définir les modalités techniques et standards de cette surveillance préventive des télécommunications.

Après avoir notamment proposé d'imposer la communication aux autorités des mots de passe des internautes, ou encore la présences de "backdoors" (portes dérobées) dans les logiciels et systèmes de cryptographie, le Parlement européen décida finalement de s'opposer à la conservation des traces de connexion, en juillet 2001, au motif que cela reviendrait à "*donner carte blanche dans l'intrusion dans la vie privée des citoyens, en dérogation des droits de l'homme et des libertés fondamentales*", comme le rapporta alors **ZDNet** :

> ***Le comité du Parlement européen a notamment précisé que des mesures de surveillance électronique doivent être «entièrement exceptionnelles, basées sur une loi spécifique et autorisées par une autorité judiciaire compétente dans le cas de personnes individuelles». Toute forme de surveillance électronique sur une large échelle devrait être interdite, tranche le comité.***

"Légalité républicaine" vs "ère du soupçon"

Deux mois plus tard, les attentats du 11 septembre 2001 allaient tout changer, dans le monde entier, entraînant nombre de pays à renforcer leurs boîtes à outils sécuritaires, au nom de l'anti-terrorisme.

En France, le gouvernement socialiste qui, **depuis 1997**, cherchait à border la droite sur le terrain de la lutte contre l'"*insécurité*", modifiait ainsi dans l'urgence son projet de loi relative à la sécurité quotidienne (**LSQ**), pour notamment contraindre les fournisseurs d'accès à l'internet à stocker, pendant un an, les traces (**"*logs*"**) de ce que font les internautes sur les réseaux, et ce quand bien même il n'a jamais été formellement prouvé que les terroristes avaient utilisés le Net pour communiquer (voir **Terrorisme : les dessous de la filière porno**).

De **nombreuses associations** avaient alors dénoncé des "*mesures d'exception*" instaurant une **ère du soupçon** faisant de tout citoyen un "*présumé suspect*" qu'il convenait de placer, par principe, sous surveillance.

Signe de la fébrilité des parlementaires, le sénateur socialiste Michel Dreyfus-Schmidt avait d'ailleurs vendu la mèche, avec un lapsus lourd de sous-entendus admettant que la France sortait du cadre de la "*légalité républicaine*" :

> ***« Il y a des mesures désagréables à prendre en urgence, mais j'espère que nous pourrons revenir à la légalité républicaine avant la fin 2003 ».***

Conscient du fait que les législations anti-terroristes se doivent d'être sévèrement encadrées, l'article 22 de la LSQ précisait en effet que les mesures anti-terroristes rajoutées en urgence dans la foulée des attentats, et donc ce placement sous surveillance des internautes, ne devaient courir que jusqu'au 31 décembre 2003, date à laquelle un "*rapport d'évaluation sur l'application de l'ensemble de ces mesures* devait permettre au Parlement de statuer sur leur prorogation, ou non.

Quand l'exception devient la norme

Le Parlement n'eut pas le temps de demander ni d'examiner quelque rapport d'évaluation que ce soit. Le 21 janvier 2003, un amendement déposé par Christian Estrosi, après avis favorable de Nicolas Sarkozy, à son projet de Loi sur la sécurité intérieure (**LSI**, ou "*Loi Sarkozy II*"), dont il était le rapporteur, grave dans le marbre, sans aucun débat et en moins d'une minute, le principe de surveillance préventive des internautes. **Verbatim** :

> ***M. Christian Estrosi, rapporteur. Prorogation ou pérennisation ? Dans l'article 17 du projet du Gouvernement, il n'est question que de proroger. Dans mon amendement, par contre, je propose de pérenniser certaines des dispositions visées, celles qui touchent à la conservation et au déchiffrement des données informatiques, c'est-à-dire à l'utilisation des nouvelles technologies de l'information et de la communication par la cybercriminalité.***
>
> ***Je vous ai soumis précédemment un amendement tendant à instituer de nouveaux délits pour donner à la police des moyens d'action dans la lutte contre la cybercriminalité et les réseaux qui s'y rattachent.***
>
> ***Il me paraît justifié de profiter de l'examen de cet article pour pérenniser des dispositions qui seront de plus en plus utiles à l'avenir, aux forces de l'ordre pour mener à bien leurs investigations en matière de lutte contre toutes les formes de trafics : drogue, armes, pédophilie, prostitution, blanchiment d'argent.***
>
> ***M. le président. Quel est l'avis du Gouvernement ?***
> ***M. le ministre de l'intérieur, de la sécurité intérieure et des libertés locales. Favorable.***
> ***M. le président. Je mets aux voix l'amendement n° 86.***
> ***(L'amendement est adopté.) "***

Avec l'adoption de l'amendement Estrosi, soulignait ainsi la Ligue Odebi dans ses **Logs pour les nuls**, "*la mesure d'exception consistant initialement à enregistrer tous les faits et gestes des internautes à des fins de lutte anti-terroriste, pour les mettre à disposition de l'autorité judiciaire, est devenue une mesure définitive, donc totalement séparée de l'existence ou non d'une menace terroriste*".

Extension du domaine des écoutes

En 2004, la loi pour la confiance dans l'économie numérique **LCEN**) étend l'obligation de conservation des données de connexion aux hébergeurs et responsables des sites et services web, qui doivent **détenir et conserver** "*les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires*".

En janvier 2006, la loi relative à la lutte contre le terrorisme (**LCT**), présentée par le ministre de l'intérieur, Nicolas Sarkozy, élargit l'obligation de conservation des "*données de trafic*" aux cybercafés, et prévoit de permettre aux services anti-terroristes de pouvoir y accéder en dehors de tout contrôle de l'autorité judiciaire, mais après avis d'une personnalité qualifiée placée auprès (et dépendant) du ministre de l'intérieur.

Le 15 mars 2006, une **directive européenne sur la conservation des données** définit la liste de ce que les fournisseurs de services de communications électroniques doivent logguer, suivie, en France, le 24 mars 2006 d'un **décret** "*relatif à la conservation des données des communications électroniques*". Les FAI et les opérateurs de téléphonie sont désormais tenus de pouvoir tracer et identifier :

la source et l'utilisateur de chaque communication
son ou ses destinataires
la machine utilisée pour communiquer
le type, la date, l'heure et la durée de la communication
les "*données relatives aux équipements terminaux de communication utilisés (et) aux services complémentaires demandés ou utilisés et leurs fournisseurs*"
la géolocalisation des équipements de communication mobile utilisés.
En 2007, le ministère de l'intérieur mettait en place, en toute discrétion (**dixit Le Figaro**) et entre les deux tours des présidentielles, une nouvelle plate-forme d'interception, en temps réel, des données de connexion des mails et des textos, à l'intention des services de renseignement :

> ***Qu'il s'agisse d'un appel sur mobile, d'un courriel envoyé par Internet ou d'un simple texto, les « grandes oreilles » de la République peuvent désormais savoir qui a contacté qui, où et quand.***

“L’internet est un moyen de se cacher”

Problème : de plus en plus de connexions sont chiffrées, empêchant les grandes oreilles de savoir qui fait quoi sur les réseaux, comme l’**expliquait** l’an passé Bernard Barbier, “*directeur technique*” de la Direction Générale de la Sécurité Extérieure (DGSE).

A son arrivée dans les services spéciaux en 1989, “*l’objectif, c’était le téléphone*” : des numéros, localisés et limités en terme de relais d’informations (fax, télex ou voix), à bas débit (”*un million de communications simultanées, c’est pas beaucoup pour nous* ”), et rarement chiffrés. Le recours à la cryptographie servait d’ailleurs d’alerte, car seuls les diplomates, les militaires ou les services secrets chiffraient leurs communications, *“et notre job était de les casser, et on devait traiter entre 100 et 1000 documents par jour*”.

Aujourd’hui, la couverture en téléphonie mobile est quasi-mondiale, le débit a considérablement changé (de l’ordre de 1 milliard de communications simultanées), et de plus en plus de services et de flux sont chiffrés (BlackBerry, Skype, Gmail -depuis l’**attaque des Chinois**), sans même que l’utilisateur ne s’en rende compte et, à terme, l’ensemble des télécommunications seront probablement chiffrées.

Dans le même temps, souligne Bernard Barbier, “*même les méchants se mettent à communiquer*” : souvent jeunes, instruits, “*tous les apprentis terroristes utilisent la crypto : pour eux, l’internet est un moyen de se cacher : ils savent qu’ils peuvent être écoutés, et donc se cachent dans la masse des utilisateurs de l’internet*”, ce qui fait que “***les cibles ont changé*** ” :

> ***“Nos cibles principales aujourd’hui n’utilisent plus le chiffrement gouvernemental ou militaire mais plutôt de la cryptographie grand public, car nous travaillons à 90% sur l’anti-terrorisme. Aujourd’hui, nos cibles sont les réseaux du grand public, parce qu’utilisés par les terroristes.”***

Parallèlement, et au vu de l’explosion du volume des télécommunications, les services de renseignement et de police judiciaire s’intéressent plus au contenant qu’au contenu, afin de savoir qui communique avec qui, quand, pendant combien de temps, voire où, si la communication est géolocalisée :

> ***“Et toutes ces méta-données, on les stocke, sur des années et des années, et quand on s’intéresse à une adresse IP ou à un n° de tel, on va chercher dans nos bases de données, et on retrouve la liste de ses correspondants, pendant des années, et on arrive à reconstituer tout son réseau.”***

“Nous stockons tous les mots de passe”

“*La mémoire humaine n’étant pas infinie, les utilisateurs utilisent souvent les mêmes mots de passe*“, expliquait également Bernard Barbier, ce qui peut s’avérer très pratique pour identifier les apprentis terroristes qui utilisent les mêmes types ou bases de mots de passe lorsqu’ils interviennent sous leurs pseudonymes de guerre, la nuit sur les forums de discussion, que lorsqu’ils s’expriment, le jour, sous leurs vrais noms, sur les réseaux sociaux :

> ***Ils mènent une double vie, mais ont les mêmes mots de passe. Et nous stockons bien évidemment tous les mots de passe, nous avons des dictionnaires de millions de mots de passe.***

On comprend mieux pourquoi le décret sur la conservation des données “*permettant d’identifier toute personne ayant contribué à la création d’un contenu mis en ligne*“, publié 6 ans après l’adoption de la LCEN auquel il se réfère explicitement, prévoit précisément la conservation, non seulement des noms, prénoms, pseudos, identifiants, n° de téléphone, adresses postales et électroniques de ceux qui s’expriment sur le Net, mais également de leurs “*mots de passe ainsi que des données permettant de les vérifier ou de les modifier* “.

Les services de police et de gendarmerie ont en effet de plus en plus recours à des logiciels d’analyse criminelle (**ANACRIM**) afin, “*par exemple, de rattacher les appels téléphoniques à des abonnés, les abonnés à leurs correspondants, les correspondants à leurs autres relations et ainsi de suite*“.

C’est ainsi que les statisticiens, spécialistes du datamining, sont **parvenus à exploiter** des centaines de milliers de CDR (Call Data Recording), les fiches contenant toutes les données relatives à un appel téléphonique, afin d’identifier le café où se réunissaient les terroristes de l’attentat de Madrid en 2004.

C’est également ce pour quoi les mots de passe pourront donc aussi servir à identifier des internautes, comme le **souligne Guillaume Champeau** sur Numerama :

> ***Avec ces méthodes, l’enquête peut devenir un véritable jeu de piste. Par exemple, si le suspect a pris soin de masquer son adresse IP et utilise une adresse e-mail jetable sur le lieu du crime, il sera peut-être***

possible pour les enquêteurs de trouver le même login (pseudonyme) sur un autre service en ligne, où la personne recherchée n'aura pas pris les mêmes précautions. La comparaison des mots de passe pourra peut-être alors confirmer qu'il s'agit bien de la même personne, auquel cas l'adresse IP utilisée pourra faciliter l'identification.

Les **services anti-terroristes**, qui ont le droit d'accéder aux données sans contrôle judiciaire, pourront ainsi plus facilement s'infiltrer sur les réseaux. Encore que : les terroristes n'utilisent guère les sites et réseaux sociaux hébergés en France, de même qu'ils passent rarement par des fournisseurs d'accès français, et l'obligation de conservation, et de transmission, des données de connexions prévus dans le décret ne s'applique pas aux forums et réseaux sociaux étrangers.

Il n'est, par contre, qu'à se souvenir de l'affaire Tarnac pour imaginer sans trop de difficulté les problèmes que cela pourrait engendrer dès lors que des policiers s'en serviraient pour infiltrer des "*organisations de nature subversive susceptibles de se livrer à des actes de terrorisme ou d'atteinte à l'autorité de l'Etat*", notion pour le moins floue mais dont la surveillance fait explicitement partie des **missions** de la Direction Centrale du Renseignement Intérieur (DCRI), le service de contre-espionnage français qui a fusionné les RG et la DST.

En attendant de tels éventuels dérives et dommages collatéraux, on aurait tort de verser dans la paranoïa, ne serait-ce que parce que conservation des données de connexion date donc de 10 ans maintenant et, comme le **souligne** Eric Freyssinet, chef de la division de lutte contre la cybercriminalité de la gendarmerie, "*d'ores et déjà, dans ces situations et dans la plupart des cas, les enquêteurs parviennent déjà très facilement à identifier le bon interlocuteur*".

A contrario, il n'est pas vain de rappeler pour autant que normalement, dans un État de droit, on ne place sous surveillance que les individus soupçonnés d'avoir commis un crime ou un délit. Dans nos démocraties sécuritaires, tout citoyen est a contrario un suspect en puissance, qu'il convient de surveiller, de manière préventive, "*au cas où*". Le problème est politique. Il en va de la "*légalité républicaine*".

Photographies CC ***leg0fenris***.

DAEMON
le 4 mars 2011 - 19:03 • SIGNALER UN ABUS - PERMALINK

bof … pas drôle tout ce dispositif ! m' enfin va falloir faire avec ! sauf si :
utilisation de proxy, cryptage disque dur "truecrypt", cryptage mails "pgp", cryptage trafic web "https everywhere" … hash, aes, ssl, etc …
bingbang2012

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

FANG BLACKBONE
le 4 mars 2011 - 22:38 • SIGNALER UN ABUS - PERMALINK

http://www.dailymotion.com/video/x9esvu_tu-es-un-terroriste-du-bist-terrori_news

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

REQUIS
le 5 mars 2011 - 0:37 • SIGNALER UN ABUS - PERMALINK

Très bon article.
Faîtes chauffer les proxies et changer de mot de passe toutes les semaines si ce n'est pas déjà fait..

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI REPONDRE

ZOU
le 5 mars 2011 - 1:11 • SIGNALER UN ABUS - PERMALINK

la prochaine etape de controle et de surveillance sera administré sous forme de vaccin. Qui sait peut etre les terroristes developpent des dons de télépathies la securité mondiale je suis pas contre,ni partisan de la paranoia mais si on a plus le droit de télécharger librement alors prk payer son abonnement dont les boites rachetent les sites de partages et de téléchargement c pour nous les revendre peut etre? Mystére peut etre pas

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

K.
le 5 mars 2011 - 8:28 • SIGNALER UN ABUS - PERMALINK

Bah ouai les gentils c'est forcément nous

n'est ce pas

Gentil toutou va

Forcément c'est nous

Et le peuple il faut le flicquer ca forcément lui le méchant

et le terrorisme, oula :c'est le mal et c'est ce qui a tué le plus de gens dans l'histoire

et puis …

Il y a de l'avenir dans le système les toutous

Disons il y a plus de travail , y compris pour les barbouze, il y a plus de retraite

qu'est ce que tu fais le toutou ?

tu va sucer tes maitres pour avoir une gamelle ?

Ou tu va crever comme les autres ?

dans un grand camps de concentration, camp de travail ou on ne partage ou on ne nourri pas

c'est faisable VOUS L'AVEZ DEJA FAIT

qu'est ce que vous attendez pour passer juste a la vitesse supérieur , qu'on en finisse

allez jusqu'au bout : les teigneux imbéciles

allez y

et vous comprendrez un jour votre bétise

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

K.
le 5 mars 2011 - 8:30 • SIGNALER UN ABUS - PERMALINK

PS : c'était un Message personnel a ceux qui nous fliquent

Le mal il est peut être pas ailleurs, regardez vous dans une glace

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GINSS
le 5 mars 2011 - 19:36 • SIGNALER UN ABUS - PERMALINK

Comme le disait un responsable politique français sur une chaine d'info en continu ou sur LCP au sujet de la LOPPSI ~ "c'est pas comme si c'était la Chine qui prennait ce genre de mesure" ~ Qui peut retrouver l'auteur de cette phrase ?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI REPONDRE

MERLIN
le 7 mars 2011 - 0:01 • SIGNALER UN ABUS - PERMALINK

“La trop grande sécurité des peuples est toujours l’avant-coureur de leur servitude.”
Les Chaînes de l’esclavage
Jean-Paul Marat

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GOURMET
le 7 mars 2011 - 13:37 • SIGNALER UN ABUS - PERMALINK

Il y a TOUJOURS une part de communications qui vise à faire peur et à colporter le message :
faites gaffe, on sait tout sur vous, on vous surveille et si vous faites un écart, on vous choppera.

C’est de la propagande de bas étage du type de celle que l’on voit dans les séries américaines : le hacker du coin trouve tout sur tout le monde en moins d’1 minute, cracke du “triple chiffrement” (sic), voit les comptes bancaires, et relie 30 personnes en moins de 3 clics de souris.

Evidemment que ces gens-là n’ont pas TOUS les mots de passe.
Déjà ils n’ont pas ceux de mes machines, ceux qui sont stockés dans mon téléphone, ceux du bureau, ceux de mon compte en banque à Shanghaï, ceux des différents forums auxquels je participe (ne serait-ce que parce qu’ils sont sous forme d’empreintes).

De toutes les manières, les terroristes, les vrais, ont un tel fric qu’ils peuvent se faire passer pour n’importe qui (si vous avez un coup de fil urgent, vous empruntez le téléphone de qqun au hasard dans la rue en lui filant 10 euros ou vous faites de la voix sur IP en utilisant un PABX de particulier situé en Ukraine : pas de trace, pas de remontée d’appel).
Toutes ces lois ne visent qu’une chose : faire peur.
En fait, l’état ne protège plus ses concitoyens depuis longtemps, il n’en a plus les moyens ni, surtout, la volonté (préférant faire plaisir aux actionnaires et aux patrons).
Incapable de prévoir les évolutions du monde (on l’a bien vu avec la Tunisie et l’Egypte) il préfère maintenir un état de peur dans la population afin de servir ses propres intérêts électoraux (pas de rébellion) en donnant l’impression qu’il s’occupe ainsi un peu de la sécurité.

Du reste, les vrais pirates, eux, courent toujours (et on le voit avec Bercy) !
Par ailleurs il faudrait étudier la communication autour de l’affaire de Bercy car révéler que l’on s’est fait avoir n’est jamais bon en termes d’images.
Qu’est ce que cela cache ?
Probablement de nouvelles lois et autres décrets en préparation afin de mieux verrouiller encore les citoyens !

db

VOUS AIMEZ 1 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MAX
le 10 mars 2011 - 12:15 • SIGNALER UN ABUS - PERMALINK

Et alors ? il demeure que nous sommes dans des pays de liberté, qu’il existe tout une batterie de lois qui permettent à tous de s’informer et d’intervenir. En dehors du fait que cet article nous éclaire fort bien sur une partie de cette histoire, il alimente la parano sur ce sujet oh combien difficile et complexe. Mais des articles sur les moyens de combattre, d’intervenir ou s’informer sont rare et c’est cela qui est regrettable. Nous sommes en démocratie, et même si nous le déplorons, ce tout sécuritaire semble bien satisfaire le plus grand nombre, si j’en juge par le laxisme de mes concitoyens et autres collègues de travail. Cette société est bien à notre image. Ce tout sécuritaire n’aura pas empêché certains dictateurs de tomber n’est-ce pas. Reste le pigeon voyageur, l’avion en papier, la discussion en bord de mer ou près d’une autoroute … Mais dans tous les cas, pour combattre, il faut des combattants. Et ça, c’est plutôt rare, si par ex. on en juge par la santé des Majors qui nous ont pourtant bien pourri nos libertés. Personne n’a jamais forcé personne à acheter des CD n’est-ce pas. Alors bon, faut pas pleurer. Cdt,

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GINKO
le 10 mars 2011 - 13:34 • SIGNALER UN ABUS - PERMALINK

@ Gourmet:

*[Evidemment que ces gens-là n'ont pas TOUS les mots de passe.
Déjà ils n'ont pas ceux de mes machines, ceux qui sont stockés dans mon téléphone, ceux du bureau, ceux de mon compte en banque à Shanghaï, ceux des différents forums auxquels je participe (ne serait-ce que parce qu'ils sont sous forme d'empreintes).]*

*Ahah, vous dites ça parce que vous n'avez pas compris de ce dont il s'agit.
Les "dictionnaires de millions de mots de passe" dont il est question sont sans doute ce que l'on appelle des rainbow tables destinées à accélérer le crack des hashs de mots de passe. Il ne s'agit sans doute pas de bases de données stockant des tuples url/login/mdp.*

@ max:

[Cette société est bien à notre image.]

En disant cela, vous sous-entendez que nous avons notre libre arbitre et donc que c'est en quelque sorte de notre faute. Mais c'est faux, vos collègues et concitoyens sont juste moulés par les engins propagande généralisée des états et des multinationales. Si toute cette dérive sécuritaire est permise, c'est bien par leur volonté, pas la notre.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

N°1
le 13 mars 2011 - 9:50 • SIGNALER UN ABUS - PERMALINK

« Ça y est Marcel, j'en tiens un ! »

Titre racoleur, article sécuritaire. Les conspirationistes sont fatigants. En plus, que vient faire le PS là-dedans ? Mystère… Mettez-vous d'accord, on est en Sarkozie depuis 2002 ou pas ?

La bascule sécuritaire date de 1997, du colloque de Villepinte, où le PS a commencé à vouloir bordé la droite du côté du sécuritaire, cf La "défaite idéologique" du PS.

Vous prétendez avertir le lecteur d'un danger le menaçant. En fait, c'est vous qui créez la peur. Dans le genre "ne dites pas ce que vous pensez parce qu'on vous surveille". Sauf que votre truc de la surveillance généralisée du net, c'est bidon. Ça fait penser à un type qui gueulerait ses opinons avec un porte-voix dans la rue et qui s'étonnerait qu'on sache ce qu'il pense, ce qui est légèrement contradictoire. Vous oubliez une petite chose : malgré ses larges imperfections, la France reste une démocratie. Et en démocratie, l'opinion n'est pas un délit. Tenez-vous bien, on peut même y afficher ses opinions en plein jour en se présentant aux élections. Incroyable non ? Donc, l'opinion des autres sur vos propres opinions, dans une démocratie, vous avez le droit de ne pas vous en préoccuper. C'est tout.

De fait, les socialistes avaient voté la conservation des données de connexion, et donc le placement sous surveillance du Net. Sinon, je fais moi aussi partie de ceux qui, justement, invite les gens à s'exprimer, et à ne surtout pas se taire, cf Les "petits cons" parlent aux "vieux cons" .

En plus, le contrôle généralisé est techniquement impossible et vous le savez très bien. Rien qu'en France, des dizaines de millions de messages sont envoyés chaque jour sur les forums, blogs, messageries instantanées. Vous croyez sérieusement qu'un contrôleur les lit tous, assis devant son écran ? Même avec les logiciels d'analyse les plus pointus, personne ne saura jamais ce que vous racontez aux gens sur les pannes de votre bagnole ou vos vacances à Ouarzazate, ni non plus d'ailleurs avec qui vous bouffez le midi. C'est comme les caméras de surveillance, dont 99% des images ne sont jamais vues par qui que ce soit. Du pipeau panoptique et surtout une histoire de gros sous. En plus, quand on connaît les erreurs des fichiers, l'incapacité à protéger les données sensibles et le manque de moyens récurrent des services publics français, mais comment voudriez-vous qu'on prenne au sérieux votre papelard ?

Tout ce que j'écris est factuel, et je n'ai nulle part écrit qu'il y avait un "contrôle généralisé", mais qu'il y avait une généralisation de la suspicion, ce qui n'est pas la même chose.

Bien sûr qu'il y a une poignée d'agents publics chargés de lutter contre les barbus ou les réseaux maffieux. Et alors ? Vous croyez qu'on vit dans un monde bisounours ?

D'ailleurs, l'espionnage laisse lui aussi beaucoup de traces, ce dont vous ne parlez jamais, bien sûr…

La peur fait vendre, c'est bien connu. Vous, votre fonds de commerce, c'est la peur.

La peur fait vendre, c'est bien connu. C'est même notamment ce pour quoi, ou comment, Nicolas Sarkozy a été élu. Je me contente de narrer, et contextualiser, cette montée en puissance de l'instrumentalisation de la peur.

En attendant le retour à la "légalité républicaine"…

manhack

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

ANASTASIE

le 13 mars 2011 - 9:53 • SIGNALER UN ABUS - PERMALINK

« Ça y est Marcel, j'en tiens un ! »

Titre racoleur, article sécuritaire. Les conspirationistes sont fatigants. En plus, que vient faire le PS là-dedans ? Mystère… Mettez-vous d'accord, on est en Sarkozie depuis 2002 ou pas ?

Vous prétendez avertir le lecteur d'un danger le menaçant. En fait, c'est vous qui créez la peur. Dans le genre "ne dites pas ce que vous pensez parce qu'on vous surveille". Sauf que votre truc de la surveillance généralisée du net, c'est bidon. Ça fait penser à un type qui gueulerait ses opinons avec un porte-voix dans la rue et qui s'étonnerait qu'on sache ce qu'il pense, ce qui est légèrement contradictoire. Vous oubliez une petite chose : malgré ses larges imperfections, la France reste une démocratie. Et en démocratie, l'opinion n'est pas un délit. Tenez-vous bien, on peut même y afficher ses opinions en plein jour en se présentant aux élections. Incroyable non ? Donc, l'opinion des autres sur vos propres opinions, dans une démocratie, vous avez le droit de ne pas vous en préoccuper. C'est tout.

En plus, le contrôle généralisé est techniquement impossible et vous le savez très bien. Rien qu'en France, des dizaines de millions de messages sont envoyés chaque jour sur les forums, blogs, messageries instantanées. Vous croyez sérieusement qu'un contrôleur les lit tous, assis devant son écran ? Même avec les logiciels d'analyse les plus pointus, personne ne saura jamais ce que vous racontez aux gens sur les pannes de votre bagnole ou vos vacances à Ouarzazate, ni non plus d'ailleurs avec qui vous bouffez le midi. C'est comme les caméras de surveillance, dont 99% des images ne sont jamais vues par qui que ce soit. Du pipeau panoptique et surtout une histoire de gros sous. En plus, quand on connaît les erreurs des fichiers, l'incapacité à protéger les données sensibles et le manque de moyens récurrent des services publics français, mais comment voudriez-vous qu'on prenne au sérieux votre papelard ?

Bien sûr qu'il y a une poignée d'agents publics chargés de lutter contre les barbus ou les réseaux maffieux. Et alors ? Vous croyez qu'on vit dans un monde bisounours ? D'ailleurs, l'espionnage laisse lui aussi beaucoup de traces, ce dont vous ne parlez jamais, bien sûr…

La peur fait vendre, c'est bien connu. Vous, votre fonds de commerce, c'est la peur.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

GINSS

le 14 mars 2011 - 10:08 • SIGNALER UN ABUS - PERMALINK

@anastasie c'est ce que je disais, certains pense que c'est parcequ'on est en France ce type de mesure n'ont pas le même impacte que si elle était prise dans d'autre pays. Sur internet y'a pas que des barbus ou des mafias, ton discours est des plus obscuricissant. Je pense qu'on a le droit d'être informé et les gens n'ont pas si peur que ça d'internet malgré les avertissement, la plus part y raconte leur vie. C'est bien ça la democratie le droit à l'information. Non?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

SARROUB MOURAD

le 16 mars 2011 - 0:35 • SIGNALER UN ABUS - PERMALINK

Comment les 'pirates informatiques' arrivent-ils à échapper à cette surveillance. Est-ce un manque de 'vigilance' ???…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JOHANNES
le 12 février 2012 - 14:23 • SIGNALER UN ABUS - PERMALINK

c'est par le biais de l'espionnage que les agents secret m'ont volé le secret de fabication et leconcept du ipad , ipod, ibook, et sont allés le revendre à steve jobs; ce n'est pas steve jobs qui aurait inventé le ipad;mais plutôt moi

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

YLIAN ESTEVEZ
le 3 avril 2012 - 0:50 • SIGNALER UN ABUS - PERMALINK

Tout y est ! La réalité rejoint la fiction ! qu'en sera t-il de l'épilogue ? http://www.youtube.com/watch?v=75hd2kwVQAM

Journal d'un hacker, de Maxime Frantini

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

7 pings

Ils le valent bien | Alter Oueb le 7 mars 2011 - 10:52

[...] (blog que m'a conseillé MHPA) l'évoque avec justesse, et m'a renvoyé sur un billet très instructif, qui montre l'évolution durant ces 20 dernières années du tout sécuritaire. En tant [...]

Ils le valent bien | Flux de blogs de gauche le 7 mars 2011 - 16:21

[...] (blog que m'a conseillé MHPA) l'évoque avec justesse, et m'a renvoyé sur un billet très instructif, qui montre l'évolution durant ces 20 dernières années du tout sécuritaire. En tant [...]

Le décret Big Brother qui cache la forêt « # numéro lambda # le 10 mars 2011 - 13:54

[...] Manach, dans son historique paru sur Owni.fr, rappelle comment un certain Christian Estrosi était parvenu à rendre totalement pérennes, [...]

Plus de fichiers = plus de fuites | BUG BROTHER le 10 novembre 2011 - 10:15

[...] d'Europe de la surveillance des télécommunications, depuis que le FBI, le PS et Christian Estrosi ont mis le Net sous surveillance, dans la foulée des attentats du 11 septembre [...]

Pour le président-candidat français, l'Internet met la république en danger « GenèveActive.com le 22 mars 2012 - 17:07

[...] Le président-candidat va-t-il s'attaquer au principal moyen de conditionnement que représentent les télévisions qu'il contrôle, devra-t-il annuler les multiples interventions au cours desquelles il diffuse le racisme, appelle à la haine, notamment des étrangers, et entretient la peur qu'il a suscitée? De longue date, l'Internet est son ennemi viscéral et il le combat sans faiblir. Les suites des « Printemps arabes » ont permis de prendre

connaissance des moyens mis, hier, par des gouvernements européens, au service des dirigeants de Libye, de Tunisie, d'Egypte ou de Syrie pour surveiller leurs peuples et attaquer leurs opposants. Mais les systèmes fonctionnaient déjà en France, par exemple en janvier 2006, la loi relative à la lutte contre le terrorisme (LCT), présentée par Nicolas Sarkozy, alors ministre de l'intérieur, a permis aux services anti-terroristes de pouvoir accéder aux "données de trafic" en dehors de tout contrôle de l'autorité judiciaire. (Lire sur OWNI) [...]

Mohammed Merah n'a pas été identifié grâce à une loi l BUG BROTHER le 27 mars 2012 - 10:58

[...] ainsi narré comment le PS et Christian Estrosi, suivant en cela les désidératas du FBI, avaient décidé de placer les internautes sous surveillance, dans la foulée des attentats du 11 septembre 2001, et alors même qu'il n'a jamais été [...]

Mohammed Merah n'a PAS été identifié grâce à une loi antiterroriste, mais grâce à un logiciel libre l Blog d'Harold Danfair ou comment l' IGS a détruit ma vie. le 6 avril 2012 - 18:28

[...] ainsi narré comment le PS et Christian Estrosi, suivant en cela les désidératas du FBI, avaient décidé de placer les internautes sous surveillance, dans la foulée des attentats du 11 septembre 2001, et alors même qu'il n'a jamais [...]