COMMENT CONTOURNER LA CYBERSURVEILLANCE ?

LE 24 MAI 2010 ***JEAN MARC MANACH***

Un article publié dans la revue Hermès revient sur les manières de protéger au mieux ses données personnelles sur Internet.

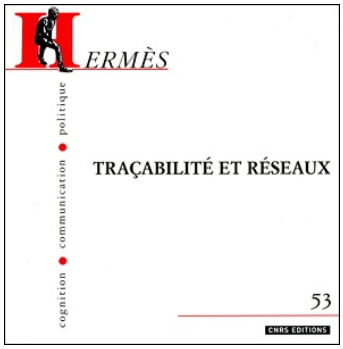
> ***Dans une démocratie, je considère qu'il est nécessaire que subsiste un espace de possibilité de fraude. Si l'on n'avait pas pu fabriquer de fausses cartes d'identité pendant la guerre, des dizaines de milliers d'hommes et de femmes auraient été arrêtés, déportés, sans doute morts. J'ai toujours été partisan de préserver de minimum d'espace sans lequel il n'y a pas de véritable démocratie.***

Ces **propos** n'émanent pas d'un crypto-révolutionnaire, mais de **Raymond Forni**, **considéré** comme le *"père inspiré de la loi Informatique et libertés* ", qui fut d'ailleurs, et **par trois fois**, vice-président de la CNIL entre 1981 et l'an 2000, un poste qu'il **quitta** pour devenir président de l'Assemblée Nationale.

En 1980, Raymond Forni **expliquait** déjà ce pour quoi l'opinion sécuritaire ne pouvait que nuire à nos démocraties et, a contrario, renforcer les logiques totalitaires :

> ***La thèse de l'infalsifiabilité comme moyen de lutte contre le terrorisme doit être ramenée à sa juste valeur. Faut-il rappeler que la carte nationale d'identité est – et demeure – facultative et que le terrorisme international se nourrit plus de faux passeports, voire de passeports de complaisance délivrés dans des conditions dont la diplomatie a le secret.***

Aujourd'hui, la question n'est plus seulement celle des papiers d'identité, mais aussi celle de la traçabilité, et de la surveillance, auxquelles les citoyens sont soumis dès lors qu'ils vont, notamment, sur l'internet.



La revue Hermès, "*l'une des grandes publications scientifiques en langue française consacrée à la communication*" (dixit le **CNRS**, qui la publie), m'a demandé d'écrire un texte pour expliquer, précisément, comment déjouer les nombreuses mesures mises en œuvre pour nous y surveiller, dans son dernier n°, intitulé "**Traçabilité et réseaux**" (voir l'**argumentaire** , et le **sommaire**), coordonné par l'équipe de **Prodoper**, un projet de recherche du CNRS consacré à la PROtection des DOnnées PERsonnelles.

Je ne prétends pas avoir intégralement couvert le sujet - d'autant que l'article a été écrit il y a maintenant un an), et je me devais aussi d'écrire à l'intention de gens qui sont probablement plus habitués à lire des textes écrits sur du papier qu'à cliquer sur les liens des hypertextes qu'on lit en ligne.

Il n'empêche : il n'est pas courant de pouvoir lire, dans une revue universitaire, et sous l'en-tête du CNRS, un tel modus operandi expliquant que tous ceux qui prétendent régir nos communications, et les surveiller, se trompent de cibles, parce qu'il est, tout simplement et de toute façon, possible d'y échapper.

Alors que, et comme le **rappelait** récemment Bruno Ory-Lavollée, ancien directeur de la Société pour l'administration des droits des artistes et musiciens interprètes (Adami) : *"si le droit d'auteur est un droit de l'homme, cela ne doit pas avoir pour prix une société policière*", il n'est pas inutile de rappeler que l'adoption de l'Hadopi, à l'instar de n'importe quel autre placement, sous surveillance, et par principe, de tout ou partie des internautes, ne pourra que nous entraîner à apprendre comment se protéger, et garantir nos libertés.

Pour bien comprendre en quoi l'Hadopi est une atteinte à nos libertés, et une régression indigne d'une démocratie, je vous conseille la lecture de l'excellente "**Lettre ouverte à un représentant de la nation**", sur Slate.fr, qui démontre point par point ce pour quoi cette *"loi d'exception".*

Ce texte a été écrit avant que soient rendues publiques les modalités de l'Hadopi, et se base sur une analyse datant de 2001, lorsque les premières velléités de placement sous surveillance de l'ensemble des internautes, sans discrimination, ont commencé à se faire jour.

Vous pouvez télécharger l'article en question, "**Comment contourner les systèmes de traçabilité ?**", dont voici l'introduction :

> ***En l'an 2000, Brian Gladman, ancien directeur des communications électroniques stratégiques du ministère de la Défense britannique et de l'OTAN, et Ian Brown, un cryptographe anglais membre de l'ONG Privacy International, rendaient public un texte expliquant comment contourner, en toute légalité, la RIP Bill britannique. Pour eux, cette loi visant à renforcer les moyens de surveillance et de contrôle des internautes s'avérait "techniquement inepte et inefficace à l'encontre des criminels" et risquait, a contrario, de " saper le droit à la vie privée et à la sécurité des citoyens et du marché ".***
>
> ***Partant du constat que les terroristes, et autres criminels, n'ont que faire de respecter la loi, Gladman et Brown avaient ainsi détaillé un certain nombre de moyens visant à aider les citoyens à apprendre à communiquer sur l'internet en toute confidentialité. Leur démarche est d'autant plus salutaire que les gouvernements se contentent généralement, au mieux, d'expliquer que toute action informatique laisse des traces et que l'on est de toute façon surveillé, au pire, de passer des lois sécuritaires renforçant cette cybersurveillance. Etrangement, ils n'expliquent jamais comment, concrètement, protéger sa vie privée sur l'internet, contribuant d'autant à créer un climat de peur, loin du climat de confiance nécessaire à toute démocratie.***
>
> ***Neuf ans plus tard, l'analyse de Gladman & Brown n'a rien perdu de sa pertinence. On ne compte plus les mesures sécuritaires substituant la suspicion de culpabilité à la présomption d'innocence. La France a elle aussi légiféré, dans la foulée des attentats de 2001, afin de placer sous surveillance, et "par principe", l'ensemble des internautes. Dans le même temps, de nouveaux outils et logiciels sont également apparus, qui renforcent, et facilitent, les moyens de lutter, en toute légalité, contre ce type d'atteintes à la vie privée.***

Téléchargez "Comment contourner les systèmes de traçabilité ?"

Article initialement publié sur Bugbrother

Illustration CC Flickr par **Niklas Plessing**

—

Retrouvez les deux autres articles de ce **second volet** de notre série sur le Contre-espionnage informatique : **Nokia, histoire d'un fail corporate** et **Petit manuel de contre-espionnage informatique**.

Retrouvez également le **premier** et **dernier** volet de cette série sur le contre-espionnage.

3 pings

Les tweets qui mentionnent Comment contourner la cybersurveillance ? » Article » owni.fr, digital journalism -- Topsy.com le 25 mai 2010 - 8:34

[...] Ce billet était mentionné sur Twitter par Sir.chamallow, Mehdi Lamloum, Business Commando, HaDeSss, Owni et des autres. Owni a dit: [#owni] Comment contourner la cybersurveillance ? http://goo.gl/fb/mwIx7 [...]

Cactus Acide » » L'observatoire du neuromancien 05/25/2010 le 26 mai 2010 - 0:34

[...] Comment contourner la cybersurveillance ? » Article » owni.fr, digital journalism [...]

Gola profonda: come assicurare la copertura delle fonti nell'era della sorveglianza totale | LSDI le 4 juin 2010 - 22:25

[...] La Rete è supersorvegliata quanto si vuole, ma c'è sempre la possibilità di aggirare la cybersorveglianza. [...]