

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article10830>

# Un expert en cybercriminalité s'interroge sur la future loi Loppsi 2

- Renseignement - France -



Date de mise en ligne : jeudi 28 mai 2009

---

Spyworld Actu

---

**Guillaume Lovet, expert en cybercriminalité, responsable de l'équipe anti-menace EMEA chez Fortinet est assez sceptique quant à l'efficacité du futur dispositif technique informatique nécessaire à Loppsi 2 (La future loi d'orientation et de programme pour la performance de la sécurité intérieure).**

**Latribune.fr - Quel est votre sentiment, au vu des nouvelles mesures préconisées par la loi Loppsi 2, notamment sur la capture d'écran et l'intrusion informatique ou le piratage par la PJ des ordinateurs de certains particuliers à leur insu ?**

Guillaume Lovet - Deux choses sont importantes à signaler si l'on compare les mouchards informatiques aux micros d'écoutes téléphoniques « traditionnelles ». En ce qui concerne le piratage informatique, l'intrusion est nettement plus importante. De plus, l'écoute téléphonique au niveau technique ne permet pas une écoute à grande échelle tandis que la diffusion d'un software tel qu'un cheval de Troie (logiciel espion) peut se dupliquer à l'infini. En fait, il ne serait pas impossible d'envisager un système automatisé de mouchards informatiques à grande échelle tout ça à moindre coût. Il y a donc un risque de dérapage dans l'intrusion de la vie privée des gens. D'ailleurs, en Allemagne en février 2007, le même projet de dispositif de « cheval de Troie » au niveau national a été bloqué par la Cour Suprême de justice.

**- D'après vous, quelles sont les limites des techniques des "cyberpoliciers" tels que l'envisage cette loi ?**

- ▶ Les systèmes antivirus peuvent être un problème à terme car leur rôle est de bloquer ou de détecter les logiciels comme les logiciels malicieux ou "un cheval de Troie" que les cyberpoliciers pourraient utiliser pour infiltrer l'ordinateur d'un suspect. De plus, il paraît difficile pour la police de trouver des accords spécifiques avec les éditeurs de logiciels antivirus au niveau mondial. Aux Etats-Unis, cette idée avait été envisagée lors des attentats du 11 septembre via un système appelé "magic lantern" pour la captation de données mais elle a été abandonnée. Quant au filtrage et au blocage d'accès aux sites uniquement pédopornographiques par les fournisseurs d'accès Internet, il semble que ces derniers ne soient pas d'accords pour cette intervention systématique. Dans le cas où un accord serait toutefois trouvé, ils le feront moyennant finance et ils installeront un système de "contrôle" à l'image du contrôle parental sur le net à l'échelle nationale.

**- La police saura-t-elle faire face aux cybercriminels sachant que les nouvelles technologies sont en constantes mutations ?**

- ▶ Ce système ne sera pas incontournable, puisque sur la Toile, il suffit de faire une recherche sur la façon d'éviter le filtrage pour surfer sur le net sans être espionné et le tour est joué. Un autre problème d'ordre technique peut se poser, ce système de filtrage des fournisseurs peut également ralentir le flux et rendre la navigation des ordinateurs plus lente.

**- D'après vous cette nouvelle loi va-t-elle combler le vide juridique qui entoure les délits liés aux piratages informatiques ?**

- ▶ Sans aucun doute en ce qui concerne l'usurpation d'identité sur Internet, puisqu'elle prévoit de pénaliser sérieusement les voyous utilisateurs de cette technique.

### - Quel est votre sentiment général sur ce futur dispositif informatique ?

- ▶ Il ne faudrait pas que nous installions des systèmes de contrôle informatique comme en Chine, ou en Iran, où les gouvernements ont instauré une politique de contrôle d'Internet. Et puis il y a une question importante d'ordre moral qui se pose quant au contrôle de l'Etat sur le Web. Existe-t-il une menace d'ordre public en France via des sites Internet qui justifierait un tel dispositif ?

*Post-scriptum :*

<http://www.latribune.fr/actualites/...>