Publié dans Questions Numériques éditions antérieures le 02/09/2013 (dernière mise à jour le 02/09/2013)
Tags : sécurité publiquesurveillance
http://reseau.fing.org/pages/view/132520/la-securite-publique-justifie-t-elle-une-surveillance-numerique-systematique
Page générée le 16/10/2019 à 13:01

La sécurité publique justifie-t-elle une surveillance numérique systématique ?

Description courte

Après beaucoup d'autres, l'affaire PRISM remet en débat le recours aux technologies pour surveiller de manière systématique et préventive la population : vidéosurveillance, écoute des échanges en ligne, etc. Est-il inévitable que nous n'ayons plus de secrets vis-à-vis des autorités ? Ces méthodes peuvent-elles se montrer efficaces ? Leurs bénéfices en matière de sécurité en justifient-ils l'usage ? Les citoyens continueront-ils de les accepter passivement ?

Description

(Les principales positions/les branches, les enjeux)

Acteurs

- Les autorités en charge de la sécurité public : police, sécurité extérieure, agences spécialisées dans la "cyber-sécurité"...
- Les gouvernements, à la fois en charge de la sécurité et comptables des libertés publiques
- Les pouvoirs législatifs, en charge de superviser les organes de sécurité et de voter les lois sécuritaires
- Le pouvoir judiciaire et les cours constitutionnelles, qui jouent un rôle significatif pour encadrer les pouvoirs de police en matière de surveillance
- Les collectivités territoriales, nombreuses à développer la vidéosurveillance
- Les fournisseurs de technologies de surveillance
- Les fournisseurs d'accès internet, les opérayeurs de réseaux et les grandes plates-formes du Web, sollicités et/ou piratés dans le cadre d'actions de cybersurveillance
- Les associations de défense des libertés individuelles, ACLU et EFF (Etats-Unis) en tête
- Les journalistes, blogueurs et "lanceurs d'alertes", parmi lesquels Edward Snowden
- Les autorités de protection de la vie privée et des données personnelles, Cnil en France, G29 à l'échelle européenne
- Les chercheurs dans le domaine technologique, à l'origine des technologies de surveillance (matérielles et logicielles), mais également nombreux parmi les défenseurs des libertés individuelles
- Les chercheurs en sciences humaines et sociales, qui se préoccupent des enjeux associés au développement de la surveillance "préventive"...

Dates clés

(Les tournants : Publication d'un papier, promulgation d'une loi, début d'une polémique)

- **1988, Royaume-Uni** : un journaliste révèle l'existence du réseau Echelon, système mondial d'interception des communications élaboré par les États-Unis, le Royaume-Uni, le Canada, l'Australie et la Nouvelle-Zélande dans le cadre du traité UKUSA.
- **1990, France** : Le tribunal administratif de Marseille annule la décision de la Ville d'Avignon d'installer des caméras de vidéosurveillance.
- **1993, Royaume-Uni** : L'identification des meurtriers d'un bébé dans une galerie marchande britannique et les attentats de Bishopgate donnent le signal d'un développement massif de la vidéosurveillance.
- **1999, France** : Par sondage, les Avignonnais, sondés, se déclarent favorables à 71 % à la vidéosurveillance. Le dispositif (64 caméras) sera installé en 2002.
- **2001, Etats-Unis** : le Patriot Act fait suite aux attentats du 11 septembre.
- **2006, ??** : Emergence des Anonymous.
- **2006, France** : Décret relatif à la vidéosurveillance : les systèmes doivent être normalisé et l'Etat se donne le droit d'utiliser les images faites par des tiers (privés).
- **2008, France** : naissance, contestation et disparition du fichier EDVIGE (Exploitation documentaire et valorisation de l'information générale).
- **2011, France** : loi Loppsi 2 étendant les pouvoirs des forces de sécurité en matière de cybersurveillance et de "vidéoprotection" (le mot remplaçant celui de "vidéosurveillance").
- **2013, USA** : affaire PRISM.

Références

(Les articles de presse, papiers de recherche, discours, analyses...)

- Daniel Solove : nombreux articles et ouvrages dont Nothing to Hide: The False Tradeoff Between Privacy and Security (Yale University Press 2011) - article : http://tehlug.org/files/solove.pdf
- Le blog collaboratif "Public Intelligence" réunit des dizaines de documents officiels ou officieux relatifs aux techniques, aux méthodes et aux règles de surveillance : http://publicintelligence.net/tag/government-surveillance/
- "PRISM est vital pour la sécurité des Etats-Unis", The Guardian, juin 2006 : http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records
- Rapport des Nations-Unies sur "Les effets de la surveillance des communications sur l'exercice des droits humains à la vie privée et à la liberté d'opinion", 2013 : http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf
- "Les atteintes aux libertés individuelles à travers un système de surveillance : Quelles sont les limites entre liberté et sécurité ?", 2008 : http://libertpe.over-blog.com/
- Hubert Guillaud, "Lutter contre la surveillance : armer les contre-pouvoirs", Internet Actu, 2013 : http://www.internetactu.net/2013/06/13/lutter-contre-la-surveillance-armer-les-contre-pouvoirs/