## Des tableaux à clés installés dans nos rues?

Imaginez-vous que des tableaux à clés soient installés dans toutes les rues. Sur ces tableaux on y accrocherait en libre-service toutes les clés de chaque maison avec une affichette précisant que ces clés ne pourront être utilisées uniquement par la Police et dans le cadre d'une perquisition. Il ne viendrait à l'idée de personne de proposer une telle loi. Et pourtant c'est exactement ce que nous allons faire en acceptant l'utilisation des Chevaux de Troie („GovWare").

Afin de fonctionner, les Chevaux de Troie doivent d'abord être installés sur l'appareil visé par la surveillance. L'Etat s'efforce ainsi à ce que les ordinateurs, les tablettes ou encore les téléphones soient vulnérables aux attaques informatiques tout en le cachant au public. En réalité, c'est exactement le contraire qui devrait se passer: la population devrait être protégée des dangers numériques notamment des cyber-criminels.

Et ce n'est pas tout: l'installation d'un Cheval de Troie dans le système d'exploitation ouvre une faille qui peut être utilisée par une personne tierce. Elle peut avoir accès à des secrets commerciaux, au disque dur ou encore à la webcam. Il y de nombreuses questions: qui va écrire un tel logiciel? Ou devons-nous l'acheter à l'étranger? Comment pourrons-nous nous assurer que la bonne personne se trouve bien assise devant l'ordinateur? De tels résultats seront-ils valables dans le cadre d'une procédure? Pour toutes ces raisons, l'utilisation des Chevaux de Troie doit être refusée.

## Un bracelet électronique pour tous?

Chaque individu peut commettre un crime au cours de sa vie. Pourquoi ne pas équiper préventivement la population de bracelets électroniques? Cet appareil enregistre régulièrement la position de chaque personne et conserve l'historique de toutes les données. Cela vous paraît excessif? Mais cela est déjà aujourd'hui la réalité, lorsque nous nous déplaçons avec notre téléphone. Et les opérateurs de télécommunications doivent selon la LSCPT conserver ces données pendant 6 mois.

Il y a quatre ans, la Cour Constitutionnelle Fédérale allemande a considéré la conservation des données comme inconstitutionnelle. Les opérateurs ont dû cesser tout enregistrement des meta-données. Depuis ce jugement, selon une étude de l'institut Max-Planck, commandée par le ministère fédéral de la justice en Allemagne, aucune aggravation significative du taux de criminalité n'a été constatée.

D'un autre côté, il n'existe aucune preuve démontrant que ces meta-données ont amélioré le taux de criminalité. La Suisse ne publie aucune information concernant l'impact de cette surveillance. Personne ne sait si la conservation de ces données est utile et donc si une telle mesure de surveillance est proportionnée au but recherché.

Il existe une alternative à l'enregistrement préventif des meta-données, compatible avec nos droits fondamentaux: le Quick Freeze. Les opérateurs de télécommunications peuvent être sollicités de conserver toutes les données concernant un suspect à partir du moment de cette demande. Ainsi, la surveillance d'un suspect peut s'effectuer sans considérer comme coupable l'ensemble de la population. Cela est aussi une alternative bien moins chère pour les opérateurs de télécommunications.

partipirate
www.partipirate.ch

Des questions?
Contacter simplement:

Denis Simonet
076 509 84 82
info@partipirate.ch