La Cnil et l'Inria se penchent sur nos données mobiles

Que deviennent les données stockées sur nos smartphones ? Et quelles données, d'abord ? C'est pour répondre à ces questions que **la Cnil** (Commission nationale informatique et liberté) et **l'Inria** (Institut national de recherche en informatique et en automatique) ont rapproché leurs équipes autour du projet Mobilitics.

Couché sur le papier fin 2011, Mobilitics consiste à analyser en profondeur les données personnelles enregistrées, stockées et diffusées par le smartphone afin de favoriser par la suite des innovations et nouveaux services durables, protecteurs des droits des utilisateurs.

Un an de développement, trois mois d'analyse

Après un an de développement, l'Inria a mis au point un outil capable de détecter et d'enregistrer les accès à des données personnelles par des applications ou programmes internes du téléphone (accès à localisation, aux photos, au carnet d'adresses, à des identifiants du téléphone, etc.). La Cnil se consacrant ensuite au décorticage de ces données.

Faute de compatibilité avec les systèmes Android et Windows Phone (promise dans les semaines qui viennent), la première salve d'analyses se limite à des données recueillies sur la plate-forme iOS d'Apple. L'expérimentation a porté sur 6 iPhones utilisés pendant 3 mois autour de 189 applications au total. Ce qui s'est traduit par 9 Go de données récoltées et l'analyse de 7 millions d'évènements.

Les utilisateurs « pistés »

Les résultats sont éloquents. Comme on peut s'en douter, ils révèlent combien les utilisateurs de smartphones sont « pistés ». À commencer par la géolocalisation effectuée en moyenne 76 fois par jour (si l'utilisateur l'a bien activée, évidemment). C'est *« la donnée la plus intensément consommée »*, indique le communiqué des deux institutions.

Si environ 15% des applications s'intéressent au nom du terminal (qui peut être changé par l'utilisateur), elles sont près de 50% à accéder à l'identification unique de l'appareil (UDID, inaccessible pour l'utilisateur) pour transmettre cette information à l'éditeur ou des acteurs tiers.

Quel contrôle des données ?

Voilà qui pose la question du contrôle par l'utilisateur des informations émises depuis son téléphone. *« Cela est d'autant plus vrai que la problématique des cookies prend de l'ampleur au sein de l'écosystème des applications mobiles*, estiment les auteurs de l'expérimentation. *S'il est déjà très difficile d'effacer les traqueurs sur son ordinateur, rien n'est aujourd'hui possible concernant ceux présents à l'intérieur des applications mobiles. »* Le contrôle des données personnelles serait-il inversement proportionnel à la mobilité de l'appareil ?

À défaut de répondre à la question, la Cnil entend mettre en œuvre des mécanismes de protection. À savoir l'intégration dans les applications d'une démarche de *privacy by design* ; des modes innovants pour proposer une meilleure information de l'usage des données aux utilisateurs (*« La situation actuelle, binaire, du "à prendre ou à laisser » n'est pas satisfaisante »*) ; des paramétrages plus fins du système d'exploitation mobile ; et, enfin, une collecte transparente des données par les acteurs qui fournissent services et outils aux développeurs. Vaste programme.

Crédit photo © igor.stevanovic – Shutterstock

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes