

# CNIL et Inria : les apps Android et iOS toujours aussi indiscrètes

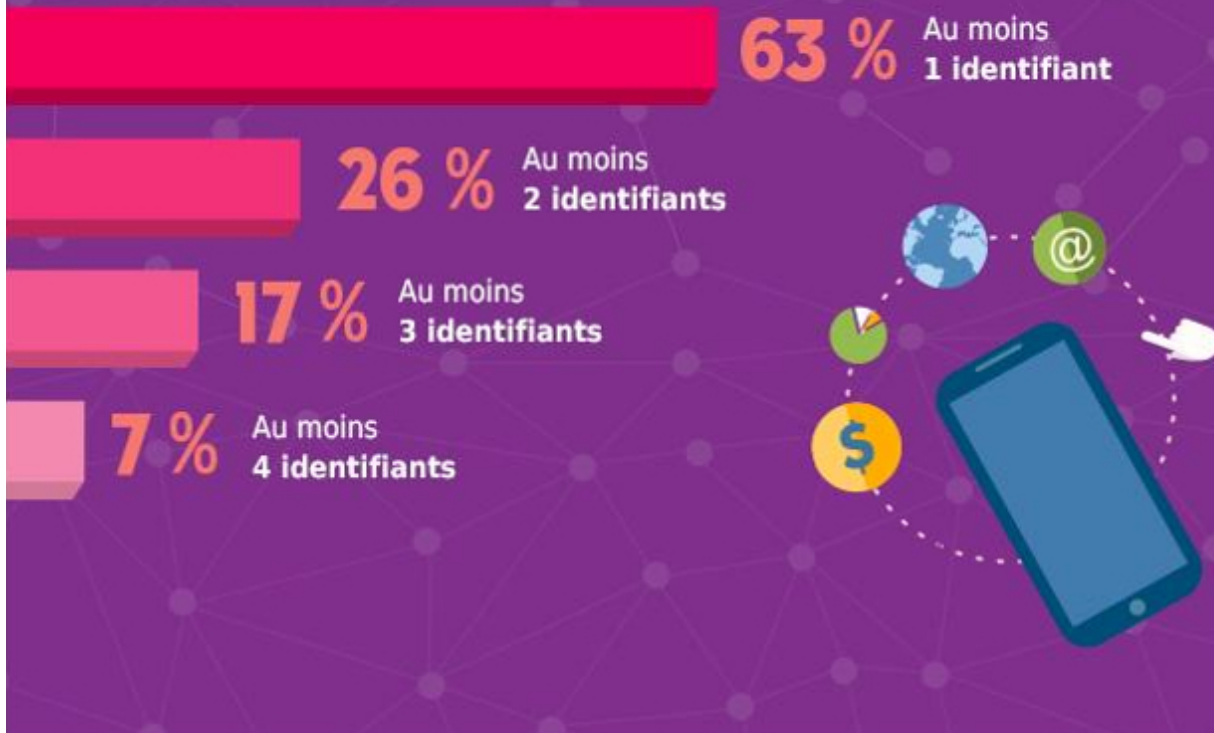
La **CNIL et l'Inria** ont donc publié les résultats de la deuxième saison de son expérience baptisée **Mobilitics**. Les équipes du laboratoire **Privatics** ont conçu un outil capable de détecter les accès des données personnelles (localisation, photo, carnet d'adresses). En 2013, les deux acteurs avaient mené [une première vague de tests](#) uniquement sur les terminaux iOS 5 avec un panel de **189 applications**. De juin à septembre 2014, des agents de la CNIL ont testé **121 applications** sur des terminaux Android Jelly Bean. Après ces tests, le régulateur estime avoir un panorama sur 87% du marché français et en à tirer quelques enseignements.

## Une course aux identifiants

Le premier est la course aux identifiants. De plus en plus d'applications souhaitent accéder à des informations personnelles issues du smartphone. Lors de la première vague de test sur iOS, une application sur deux avait accédé à l'identifiant unique alphanumérique de l'appareil appelé **UDID**. Mais la CNIL constate que les évolutions d'iOS ont limité l'accès à cette donnée, tout en créant des ID spécifiques pour les publicitaires et les éditeurs d'applications. Pour Android, l'identifiant s'appelle **Android ID** et il est unique pour l'ensemble de la chaîne de valeur (éditeurs et publicitaires). La CNIL constate que sur 121 applications, 41 ont accédé à cet identifiant. Il est par ailleurs compliqué d'effectuer les réglages du terminal pour limiter cet accès. Les apps ont pu atteindre d'autres identifiants, le code IMEI, la carte SIM ou la liste des points d'accès WiFi.

## Une course aux identifiants des appareils

Sur 121 apps Android, pourcentage d'apps ayant eu accès à :



## Une forte intensité pour accéder à la géolocalisation

Autre confirmation, la localisation reste la reine des données sur un smartphone, qu'il soit Android ou iOS. Dans leurs tests, la CNIL et l'Inria ont constaté que **31% des appareils iOS** accèdent à la géolocalisation et **24% pour l'OS mobile de Google**. Le régulateur ne conteste pas la nécessité pour certaines applications d'obtenir des informations de géolocalisation pour fonctionner. Elle critique par contre l'intensité des requêtes. L'application Facebook a ainsi demandé plus de **1 million de fois des informations de localisation en trois mois**, soit 1 accès par minute. Cette fréquence pose des problèmes de vie privée en traçant de manière quasi continue l'utilisateur. La CNIL s'interroge sur cette intensité en émettant deux hypothèses, une mauvaise optimisation des commandes de l'application ou l'acquisition d'informations riches à des fins de ciblage marketing.



**A lire aussi :**

[Les CNIL mondiales blâment la transparence des apps mobiles](#)

[Quiz Silicon.fr – Connaissez-vous la CNIL ?](#)

**Crédit Photo : Nucleartist-Shutterstock**