Les CNIL mondiales blâment la transparence des apps mobiles

Les autorités de protection des données personnelles du monde entier se sont penchées sur les applications mobiles et sur leur traitement des informations privées. L'audit s'est déroulé en mai 2014 sur plus de **1200 applications** gratuites et payantes dans des domaines variés, jeux, gestion des comptes bancaire, etc. Sur le plan méthodologique, le groupe de régulateurs réunit au sein de l'OCDE sous le nom GPEN (Global Privacy Enforcement Network) a voulu savoir plusieurs choses. Quel type de données est collecté par les applications ? Le niveau d'information des utilisateurs et la qualité des explications fournies par l'apps sur les motifs de cette collecte ?

Les utilisateurs mal informés

Les résultats de l'audit ne sont pas surprenants. Une grande majorité (**3/4) des applications collectent différentes données**, la localisation, l'identifiant du terminal mobile, mais aussi des informations d'accès à des comptes utilisateurs. Les CNIL reconnaissent que certaines de ces données sont liées « *à la finalité de l'application, mais d'autres c'est moins évident* ». La transparence s'opacifie un peu plus sur l'information de l'utilisation des données personnelles. Pour plus de la moitié des applications, ces renseignements sont « *difficiles à trouver ou inadaptés à un écran de petite taille* ». Au final, seul 25% des applications fournissent une information satisfaisante. A noter que la situation en France qui a audité 121 applications dresse le même constat que ses homologues internationaux.

Des maux déjà connus

Ce type d'audit n'est pas nouveau. En avril 2013, la CNIL s'est rapprochée de l'INRIA pour le projet **Mobilitics**. Ce projet avait pour objectif d'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. Le fruit de cette collaboration a été 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.). Les résultats de l'étude ont été aussi éloquents que ceux de l'audit mondial cité précédemment. **La géolocalisation** était la donnée la plus sollicitée, tout comme **l'identifiant du terminal**.

A lire aussi :

Larry Page craint les excés de protection des données personnelles

Une faille du WiFi d'Android dévoile les données personnelles