Alicem, le sésame numérique qui préoccupe les défenseurs de la vie privée

Le ministère de l'Intérieur expérimente Alicem, une application qui donnera aux utilisateurs de smartphones un sésame pour accéder à des services en ligne nécessitant une forte sécurité d'identification. Mais il faudra passer par une étape de reconnaissance faciale, qui suscite l'inquiétude des défenseurs de la vie privée.

Temps de lecture : minute

---

18 octobre 2019

Alicem doit permettre à un utilisateur de smartphone Android, doté d'un passeport ou un titre de séjour biométrique, de s'identifier pour avoir accès à des services en ligne, un peu comme les identifiants Google ou Facebook. Il est conçu pour permettre une authentification forte, pour pouvoir donner accès à des services en ligne "sensibles", qui ont besoin d'une protection maximum.

Pour utiliser Alicem, il faudra détenir un passeport ou un titre de séjour biométrique, car celui-ci sera utilisé pour "construire" leur sésame numérique.

Comment utilisera-t-on Alicem ?

Pour s'identifier sur un service en ligne, l'utilisateur d'Alicem disposera d'un code personnel à six chiffres, qui lui aura été remis au moment de son inscription sur le service. Si le service auquel il tente d'accéder exige une authentification forte, il devra en plus scanner son passeport ou son

titre de séjour biométrique avec son smartphone.

La reconnaissance faciale n'intervient qu'une seule fois, au moment de l'inscription sur Alicem et de l'obtention du code. Lorsqu'il s'inscrit, l'utilisateur est invité à scanner son passeport ou son titre de séjour biométrique. Il est aussi invité à filmer une courte vidéo de lui-même, où il doit faire certains mouvements. Le smartphone envoie à l'ANTS (l'Agence nationale des titres sécurisés qui gère le système) la photo du titre biométrique, et la vidéo. Un logiciel de reconnaissance faciale vérifie que la vidéo et la photo correspondent bien. Si c'est le cas, le code à six chiffres est généré et communiqué à l'utilisateur. Il sera valable pour toutes les identifications futures. La vidéo est ensuite détruite, selon l'ANTS.

Pourquoi la Cnil a-t-elle critiqué ce système ?

La Cnil, l'agence publique chargée de protéger la vie privée des Français, critique le fait qu'il n'y ait pas d'autres solutions que la reconnaissance faciale pour s'inscrire sur Alicem et obtenir le code. Pour la Cnil, il devrait exister d'autres solutions, par exemple se présenter physiquement dans une préfecture.

La Cnil critique également le fait que les serveurs de l'ANTS conservent certaines données d'historique de connexion pendant sept ans, même si celles-ci ne permettent pas de savoir sur quels services l'usager s'est connecté.

Le gouvernement a-t-il tenu compte des observations de la Cnil ?

En l'état actuel du projet, non. Sur la durée de sept ans, il affirme que c'est obligatoire pour qu'Alicem soit considéré comme une authentification forte par la législation européenne.

Sur la nécessité de fournir un moyen d'éviter la reconnaissance faciale pour bénéficier d'Alicem et de son identification forte, le gouvernement n'offre pour l'instant aucune réponse. Mais Alicem n'a pas encore été lancée et se trouve encore en phase de test, fait-il valoir.

Pourquoi Alicem inquiète-t-il ?

Pour beaucoup d'observateurs, l'arrivée de cette technologie biométrique sur les serveurs de l'Etat ne peut se faire en catimini, et mérite à tout le moins un débat informé. "Même s'il ne s'agit ici pas de reconnaissance faciale en temps réel par des caméras de surveillance, il s'agit néanmoins bien de normaliser la reconnaissance faciale comme outil d'identification", souligne l'association La Quadrature du Net, qui défend les libertés individuelles dans le monde du numérique.

À lire aussi
La Quadrature du Net passe à l'offensive contre les Smart Cities

Au-delà même du problème de la reconnaissance faciale, la Quadrature et

d'autres experts voient se profiler le spectre d'un monde ultra-contrôlé, ou l'utilisation d'un identifiant numérique est à la fois indispensable pour le citoyen et parfaitement traçable par les autorités.

Baptiste Robert, un expert informatique spécialiste notamment des failles sur Android, met en garde contre les dérives du système indien d'identité numérique indien Aadhaar, qui repose également sur la biométrie.

Présentée à l'origine comme fonctionnant sur la base du volontariat, l'inscription dans Aadhaar est devenue centrale dans la vie des 1,25 milliard d'Indiens, et est en train de devenir nécessaire pour passer un examen ou prendre l'avion.

À lire aussi
En Inde, la reconnaissance faciale remplace les papiers d'identité dans les aéroports

Article écrit par Maddyness avec AFP