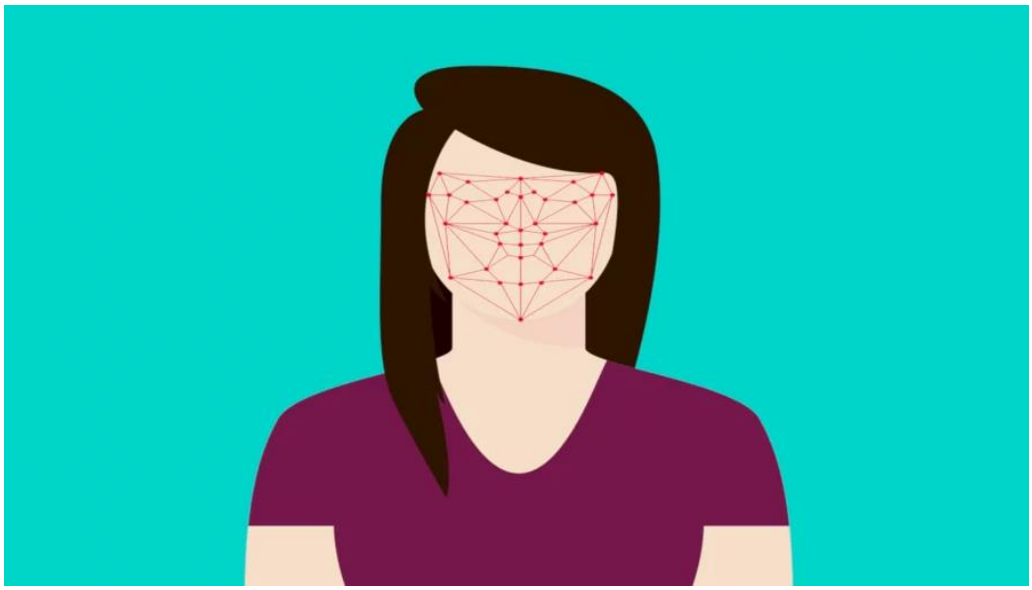
LES NUMERIQUES

LESNUMERIQUES.COM
Le 12 Novembre 2019
Audience : 5 700 000 Visites

https://www.lesnumeriques.com/vie-du-net/alicem-pourquoi-le-systeme-de-reconnaissance-faciale-de-l-etat-suscite-la-controverse-a142589.html

Alicem : pourquoi le système de reconnaissance faciale de l'État suscite la controverse

Par Jérôme Cartegini | Publié le 12/11/19 à 14h00

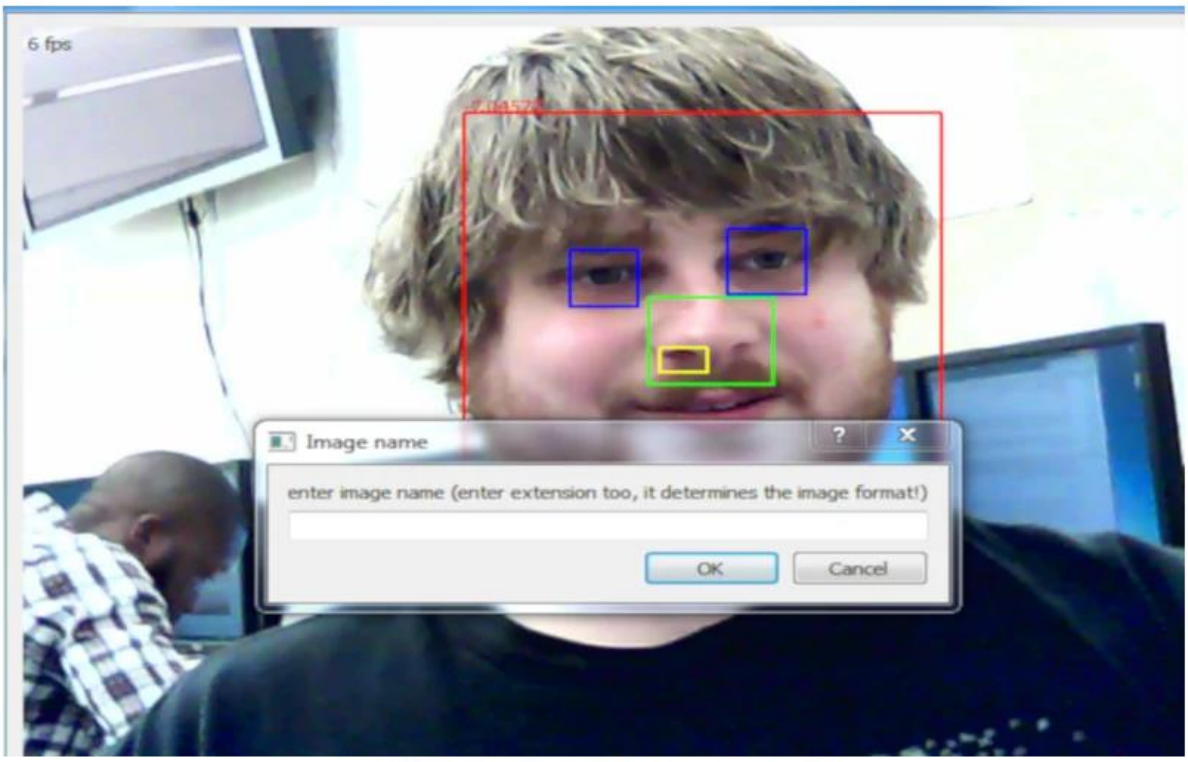


Actuellement en phase de test, la technologie de reconnaissance faciale Alicem que veut déployer l'État français suscite une vive polémique. Pourquoi fait-elle peur ? Quels sont les risques ? Des experts nous livrent leurs points de vue...

L'État français — qui a longtemps été critiqué pour son retard sur le déploiement d'Internet et des technologies numériques en général — se voit aujourd'hui reprocher par beaucoup de vouloir aller trop vite en tentant d'imposer sa première solution d'identité numérique régalienne sécurisée baptisée Alicem (Authentification en ligne certifiée sur mobile). Expérimentée depuis le mois de juin 2019, cette application mobile a été créée par Gemalto (propriété du géant Thalès) à la demande du Ministère de l'Intérieur pour l'ANTS (Agence nationale des titres sécurisés). Cette dernière a vocation à permettre aux Français de s'identifier facilement sur l'ensemble des services de FranceConnect, un dispositif de l'État donnant l'accès à plus de 500 services publics tels que les impôts, Ameli, etc.

Pour fonctionner, ce système d'identification numérique basée sur une technologie biométrique dite « forte » nécessite d'ouvrir un compte Alicem (non obligatoire), de posséder un smartphone Android ainsi qu'un passeport biométrique doté d'une puce sécurisée (délivré à partir de juin 2009). Pour l'heure, et sans doute faute aux restrictions imposées par Apple sur iOS, les iPhone ne peuvent pas fonctionner avec ce service. Une fois tous ces éléments réunis, l'utilisateur doit suivre la procédure d'identification qui consiste à filmer son visage sous différents angles puis scanner le passeport biométrique. Les données sont ensuite envoyées à l'ANTS qui les compare à l'aide d'un logiciel de reconnaissance faciale. Si elles correspondent, l'agence délivre un code personnel à l'utilisateur qui pourra ensuite s'en servir pour s'identifier via Alicem sur l'ensemble des services publics en ligne.

Sur le papier, ce système semble pratique, mais il préfigurerait un système d'identification bien plus large qui fait craindre le pire aux défenseurs du droit à la vie privée, mais pas seulement. Outre la crainte de voir à terme ce système utilisé à des fins de surveillance de masse et porter atteinte aux libertés individuelles, comme c'est déjà le cas en Chine, certains experts pointent également du doigt d'inquiétants problèmes de sécurité. Le projet est également critiqué parce qu'il ne propose aucune alternative d'inscription aux utilisateurs qui voudraient profiter de ce service.



Exemple d'un logiciel de reconnaissance faciale ©Mbroemme Wikimedia

> **Une fuite de données biométriques serait une grave atteinte à la protection des données**
>
> — Jérôme Soyer, Directeur Avant-Ventes de Varonis

Quid de la protection des données ?

Jérôme Soyer, Directeur Avant-Ventes de Varonis (société spécialisée de la gouvernance et la sécurité des données) identifie quelques points de vigilance quant au traitement et à la protection des données biométriques. "*Les données biométriques constituent une autre forme d'identification et, à ce titre, elles feront l'objet d'attaques : vol, suppression ou modification. Ce qui m'inquiète le plus est la manière avec laquelle les organisations protègent les données biométriques contre les abus. Du point de vue de la conformité au RGPD, cela pose un autre défi : comment les organisations vont-elles créer ou supprimer ces données biométriques ? Les systèmes de reconnaissance biométrique n'en sont qu'à leurs balbutiements, mais leur succès va grandissant à mesure que les développeurs les intègrent à leurs nouveaux produits. Industrie et consommateurs devraient prendre du recul et se demander si la commodité offerte vaut le risque encouru. Une fuite de données biométriques serait une grave atteinte à la protection des données.*"

"*Le problème est qu'il est impossible de modifier les données biométriques — elles sont à vous pour la vie. Les risques associés sont de fait incalculables. La meilleure façon de protéger des données biométriques est de les stocker sur des systèmes distincts et segmentés. De plus, ces données doivent être soumises à une fonction de hachage cryptographique (difficile à inverser) avant d'être stockées. Les principes traditionnels de sécurité informatique s'appliquent à la reconnaissance faciale. Des outils d'authentification automatiques doivent également être déployés pour contrôler qu'aucune application de services système compromise n'est dissimulée — aucun raccourci ne devrait être pris.*" conclut l'expert de Varonis.

Système d'identification faciale à la frontière chinoise ©MNXANL_Wikimedia

> **Même si l'utilisation de la reconnaissance faciale donne une illusion d'innovation et d'un État français au rendez-vous de l'ère numérique, d'un point de vue sécuritaire, le travail semble bâclé.**
>
> — Pascal le Digol, Directeur France de WatchGuard

Une technologie de pointe dotée d'une sécurité dépassée

Alors que tout le monde se concentre sur les enjeux de la protection des données privées, certains experts pointent du doigt la sécurité même d'Alicem. Celle-ci serait en effet loin d'être suffisante au regard des données personnelles qu'elle contient. Pascal le Digol, Directeur France de WatchGuard (spécialisée dans les solutions d'authentification multifacteur) met en avant un faux pas sécuritaire de la part de l'État dans une application censée donner accès aux informations les plus sensibles des citoyens. "*La particularité de cette nouvelle application, qui est à l'origine d'un débat, est l'utilisation de la reconnaissance faciale pour authentifier les utilisateurs (la reconnaissance faciale est croisée avec les données biométriques du passeport de la personne).*" Pour Pascal le Digol, même si l'utilisation de la reconnaissance faciale donne une illusion d'innovation et d'un État français au rendez-vous de l'ère numérique, d'un point de vue sécuritaire, le travail semble bâclé puisqu'une fois le compte utilisateur créé, l'application ne requiert finalement qu'un simple mot de passe — faible qui plus est — pour s'identifier !

"*Les attaquants qui se pencheront sur Alicem ne s'attaqueront certainement pas à la reconnaissance faciale utilisée en premier lieu puisqu'ils pourront simplement récupérer le code à 6 chiffres envoyé ensuite, à l'aide d'une simple campagne de phishing ! Il y a fort à parier que nous verrons une attaque de phishing de ce type — un email d'apparence très crédible, sans faute d'orthographe, avec des URL n'invitant pas au soupçon, usurpant un logo de l'État, etc. — apparaître assez rapidement après la mise en application d'Alicem… Ce dont nous pouvons être sûrs avec les cybercriminels, c'est qu'ils empruntent toujours les chemins les plus aisés pour parvenir à leur fin.*"

Le principal problème que soulève l'expert concerne l'absence d'une sécurité digne de ce nom pour protéger les données d'Alicem : "*Malgré l'intégration de la reconnaissance faciale, qui est en soi une avancée technologique, la deuxième étape revient à une méthode d'authentification qui est aujourd'hui totalement dépassée ! Après avoir créé son compte, l'utilisateur va ensuite se connecter avec un mot de passe à 6 chiffres, alors qu'aujourd'hui la grande majorité des applications et sites ont mis en place une politique minimale de mots de passe forts, intégrant des caractères spéciaux, majuscules, chiffres, etc. Au final, nous sommes ici sur une authentification monofacteur à l'heure où la norme devient petit à petit l'authentification multifacteur.*"alerte l'expert.

Le pire, c'est qu'à l'heure où il est nécessaire de sensibiliser massivement à la cybersécurité, cette initiative peut être pernicieuse, car d'aucuns pourraient penser qu'il suffit de ça pour être protégé, ce qui n'est pas le cas. Il est impératif de continuer à sensibiliser les utilisateurs à la cybersécurité et de prendre garde à ne pas envoyer des signaux contradictoires."

©Capture du site Alicem

> **Les attaquants qui se pencheront sur Alicem ne s'attaqueront certainement pas à la reconnaissance faciale utilisée en premier lieu puisqu'ils pourront simplement récupérer le code à 6 chiffres.**
>
> — Pascal le Digol, Directeur France de WatchGuard

Les risques de l'identité numérique

L'usurpation d'identité numérique est un vrai challenge pour à la fois les citoyens et les organisations gouvernementales. L'état doit s'assurer que la personne se connectant à ses services est bien le citoyen en question, et que son identité numérique (login/password) n'ait pas été usurpée. Matthieu Dierrick, Architecte Solutions EMEA chez F5 Networks pointe du doigt les faiblesses d'Alicem en termes de sécurité.

"*Le business le plus lucratif pour les hackers aujourd'hui est la revente de listes d'identifiants volés. Une liste fonctionnant pour un site web précis comme une banque, par exemple, est vendue plusieurs centaines d'euros (contre 10 euros pour des listes de numéros de cartes bancaires). Étant donné que les citoyens protègent mal leurs identifiants, il est indispensable pour les organisations gouvernementales de mettre en place une authentification à double facteur. Un deuxième ou troisième facteur consiste à fournir quelque chose que l'on connait (password), que l'on a (un token, une clé ...) et quelque chose que l'on est (empreintes digitales, reconnaissance faciale). Les empreintes digitales constituent le moyen d'identification le plus précis, mais il peut poser problème dans plusieurs situations où les conditions sont difficiles (poussières, mains sales ...). La reconnaissance faciale est la méthode fournissant le moins d'erreurs (faux positifs et négatifs).*"

Selon Matthieu Dierrick, les citoyens ne font pas encore confiance à l'État pour fournir leurs informations biométriques, alors que dans le même temps ils n'ont aucun problème à les donner aux GAFA (Google, Apple, Microsoft...) : "*Pour le citoyen, Alicem implique de fournir une information personnelle durable, car il n'est pas possible de changer une empreinte digitale. Le problème, c'est qu'il ne sait pas ce que l'organisation va en faire. Fournir son empreinte digitale et faciale à Apple ou Google ne pose pas de problème, alors que les fournir à un Etat pose des questions de confidentialité ! Pourquoi ? Est-ce que contrairement à l'État qui précise l'usage et le temps qu'il conservera les informations biométriques, Apple et Google donnent la moindre garantie sur leur traitement ?*"

> **Pour le citoyen, Alicem implique de fournir une information personnelle durable, car il n'est pas possible de changer une empreinte digitale.**
>
> — Matthieu Dierrick, Architecte Solutions EMEA chez F5 Networks

Comme la Chine, Israël est l'un des pays à utiliser le plus la reconnaissance faciale via ses innombrables caméras de surveillance. ©JCartegini

> **Si le citoyen ne peut plus exercer sa liberté de choix dans son identification, Alicem risque de nourrir de nouvelles inquiétudes sur la finalité réelle de la reconnaissance faciale.**
>
> — Emmanuel Richard, Directeur général de Extens Consulting

L’absence de choix du mode d'identification

Il est également reproché à l’État de ne pas proposer un autre système d’identification pour profiter du service Alicem. Emmanuel Richard, Directeur général du cabinet de conseil Extens Consulting fait le parallèle avec d’autres services basés sur la même technologie. "*Le consommateur connecté pratique déjà la reconnaissance faciale sur son mobile ou son ordinateur. C’est son choix et il le fait par commodité. Le consommateur voyageur passe la douane automatique qui utilise la reconnaissance faciale. Là aussi, c’est son choix : il le fait par commodité pour éviter la file d’attente. Dans ces deux cas, la reconnaissance faciale est une commodité qui simplifie l’expérience du consommateur, ce qui permet à ce dernier de l’accepter plus facilement.*"

"*Il s’agit donc pour la reconnaissance faciale, comme pour toute technologie innovante, de considérer sa valeur du point de vue du client final, consommateur et citoyen, en termes de facilité. Cependant, le système Alicem — en proposant la simplification d'accès aux citoyens — semble oublier une chose : le maintien du choix du mode d'identification. En imposant la reconnaissance faciale, il se différencie de l'identification sur mobile ou du passage en douane qui ouvrent toujours la possibilité d'être identifié autrement. Si le citoyen ne peut plus exercer sa liberté de choix dans son identification, Alicem risque de nourrir de nouvelles inquiétudes sur la finalité réelle de la reconnaissance faciale.*"

ALICEM : ce système est-il juridiquement légal ?

Le service de reconnaissance faciale que veut déployer l’État est-il juridiquement légal ? Pour essayer d’en savoir un peu plus sur ce sujet, nous avons intérrogé Sabine Marcellin, Avocate fondatrice du cabinet Aurore Legal, spécialisée dans le droit du numérique.

Pourquoi ALICEM pourrait porter atteinte à la vie privée ?

Ce système de reconnaissance faciale mis en œuvre par le ministère de l'intérieur permet d'authentifier l'identité des utilisateurs. Il s'applique aux personnes disposant d'un passeport biométrique ou d'un titre de séjour avec composant électronique. Les photos ou vidéos du visage sont envoyées à l'Agence nationale des titres sécurisés (ANTS), qui confirme que ce visage correspond à celui enregistré dans leur base de données. Avec cette authentification, les personnes pourront s'identifier auprès d'organismes publics et, à terme, privés.

Il s'agit naturellement d'un traitement de données, au sens du RGPD et de la loi Informatique et Libertés, et en particulier d'un traitement qui porte sur des données biométriques. Les traits du visage représentent des données intrinsèques à la personnalité. Dans ce cas la CNIL considère que le traitement présente un risque élevé pour les personnes. En effet, la reconnaissance faciale soulève des risques d'atteintes aux libertés individuelles, dont notamment la liberté d'aller et venir anonymement.

Quel est l'encadrement juridique pour ce traitement biométrique ?

Dans ce cas de traitement à caractère biométrique, le mécanisme réglementaire du RGPD prévoit que le Ministère de l'intérieur doit effectuer une demande d'avis auprès de la CNIL. Le projet a effectivement été soumis à la CNIL, qui après l'avoir analysé, a formalisé son avis, dans une délibération du 18 octobre 2018.
Dans cet avis, la CNIL émet des réserves notamment sur la réalité du consentement des personnes. Le consentement est une base légale qui, selon le RGPD, doit être libre, spécifique, éclairée et univoque. La CNIL considère que pour ALICEM le consentement n'est pas véritablement libre car "* le refus du traitement de données biométriques fait obstacle à l'activation du compte* ".

Des solutions alternatives, selon la CNIL, auraient du être présentées aux utilisateurs ne souhaitant pas l'utiliser, comme un appel vidéo avec un agent de l'ANTS. Mais ces alternatives n'ont pas été retenues. Le 13 mai 2019, un décret autorisait l'expérimentation d'ALICEM. Malgré les remarques de la CNIL, l'expérimentation d'ALICEM, sans modifications du projet initial, a commencé en juin 2019.

Est-ce qu'ALICEM pourrait être un système obligatoire ?

Aujourd'hui, l'usage d'ALICEM reste une possibilité pour l'utilisateur et non une obligation. Mais ce qui gêne les défenseurs des libertés, c'est que la possibilité d'utiliser ALICEM est fondée sur un dispositif de reconnaissance faciale obligatoire. L'association La Quadrature du Net a, le 15 juillet 2019, attaqué le décret en question. En considérant que le décret est contraire au RGPD, du fait de l'absence d'un réel consentement, l'association demande au Conseil d'Etat son annulation.

Le système est toujours en phase de test et reste en attente de certification de sécurité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).Mais l'ambition affichée par le Ministère de l'Intérieur pour ALICEM est large. L'un de ses enjeux est d' « d'assurer sa mission régalienne de certification dans un monde digital complémentaire du monde physique ».

ALICEM s'inscrit dans un projet plus global d'identité numérique. Cependant, la lutte contre l'usurpation de l'identité et la simplification des démarches administrative ne peuvent se construire que sur des bases juridiques solides. Les enjeux juridiques et politiques de la reconnaissance faciale mériteraient un encadrement légal ambitieux.