La reconnaissance faciale dans les fichiers de police

La reconnaissance faciale des manifestant·e·s est déjà autorisée

18 novembre 2019 – Quadrature du net

Suivi de Quand la France se lance dans la reconnaissance faciale

Depuis six ans, le gouvernement a adopté plusieurs décrets pour autoriser l'identification automatique et massive des manifestants. Cette autorisation s'est passée de tout débat démocratique. Elle résulte de la combinaison insidieuse de trois dispositifs : le fichier TAJ (traitement des antécédents judiciaires), le fichier TES (titres électroniques sécurisés) et la loi renseignement.

L'hypocrisie du gouvernement est totale lorsqu'il prétend aujourd'hui ouvrir un débat démocratique sur la reconnaissance faciale : il en a visiblement tiré les conclusions depuis longtemps, qu'il nous impose déjà sans même nous en avoir clairement informés.

Nous venons de lui demander formellement d'abroger ce système et l'attaquerons devant le Conseil d'État s'il le refuse.

Pour bien comprendre le montage juridique qui autorise le fichage massif des manifestants, il faut retracer l'évolution historique de ses trois composantes – le fichier TAJ (I), le fichier TES (II) et la loi renseignement (III) – puis en interroger les conséquences concrètes (IV).

I. Le fichier TAJ

La première brique de l'édifice est le fichier de police appelé TAJ, pour « traitement des antécédents judiciaires ». Rappeler son **origine** (A) nous permet de mieux comprendre son **fonctionnement actuel** (B) et la façon dont il a ouvert la voie à la **reconnaissance faciale** policière (C).

A. Les origines du TAJ

Dans son rapport sur la loi de sécurité du 21 janvier 1995, le gouvernement explique son projet de modernisation de la police. Le futur fichier nommé « système de traitement de l'information criminelle (**S.T.I.C.**) » est alors présenté comme une grande nouveauté, « le projet prioritaire pour l'informatisation des services de police » : il « permettra de **fédérer au niveau national l'ensemble des fichiers de police** et de documentation criminelle ».

Ce fichier ne sera officialisé que six ans plus tard, par un décret du 5 juillet 2001. Le gouvernement de Lionel Jospin crée ainsi un fichier nommé « système de traitement des infractions constatées (STIC) ». Concrètement, dans son avis préalable, la CNIL explique que le STIC centralisera un ensemble « d'informations actuellement conservées dans des fichiers manuels ou informatiques épars, le plus souvent cantonnés au niveau local », et donc peu exploitables. Désormais, pour l'ensemble du territoire français, **le STIC réunira toute la mémoire de la police sur les personnes mises en cause** dans des infractions, auteurs comme complices, ainsi que leurs victimes : noms, domicile, photographie, faits reprochés…

Il faudra attendre une loi du 18 mars 2003 pour que ce fichier soit clairement endossé par le législateur. À la suite du STIC, créé pour la police nationale, un décret du 20 novembre 2006 crée un fichier équivalent pour la gendarmerie, dénommé « système judiciaire de documentation et d'exploitation» (**JUDEX**).

Cinq ans plus tard, l'article 11 de la loi du 14 mars 2011 (dite LOPPSI 2) prévoit de fusionner le STIC et le JUDEX au sein d'un fichier unique, que le gouvernement envisage alors d'appeler **ARIANE**. Cette loi de 2011 est une loi de « programmation » et se voit donc accompagnée d'un « rapport sur les objectifs et les moyens de la sécurité intérieure à horizon 2013 ». D'importantes évolutions sont attendues : « la police déploiera son programme de minidrones d'observation », « une recherche en sécurité au

service de la performance technologique […] visera notamment à trouver les solutions innovantes dans des domaines tels que […] la miniaturisation des capteurs, **la vidéoprotection intelligente**, la transmission de données sécurisée, la fouille des données sur internet, **la reconnaissance faciale**, les nouvelles technologies de biométrie… ».

La fusion du STIC et du JUDEX est formellement réalisée par un décret du 4 mai 2012. Le fichier unique n'est finalement pas nommé ARIANE mais **TAJ**, pour « traitement des antécédents judiciaires ». L'une des principales différences entre, d'une part, le STIC et le JUDEX et, d'autre part, le TAJ, concerne la reconnaissance faciale. Alors que les fiches du STIC et du JUDEX ne comprenaient qu'une simple « photographie » des personnes surveillées, le TAJ va bien plus loin. Il est explicitement destiné à contenir toute « **photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale** (photographie du visage de face) », ainsi que toutes « autres photographies ».

Dans son avis de 2011 sur le décret TAJ, la CNIL « relève que c'est la première fois qu'elle est saisie par un service de l'État d'une demande d'avis sur un traitement reposant sur […] ces technologies de reconnaissance faciale ». Elle explique que ce système « permettra de comparer à la base des photographies signalétiques du traitement, les images du visage de personnes impliquées dans la commission **d'infractions captées via des dispositifs de vidéoprotection** », ce qui « présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection ».

B. Le fonctionnement du TAJ aujourd'hui

Un rapport parlementaire de 2018 explique qu'il « existe 18,9 millions de fiches de personnes mises en cause et plus de 87 millions d'affaires répertoriées dans le TAJ », et que « le TAJ comprend entre **7 et 8 millions de photos de face** ». En théorie, l'article R40-25 du code de procédure pénale prévoit que le TAJ ne devrait ficher que des personnes contre lesquelles existent des indices graves et concordants d'avoir participé à la commission d'une infraction, comme auteur ou complice. En pratique, il s'agit davantage d'un **outil de communication interne aux forces de l'ordre**, qu'elles utilisent pour échanger un maximum d'informations pratiques, indépendamment de la véracité ou de la pertinence de celles-ci. Comme l'explique la CNIL en 2012, les policiers et gendarmes remplissent eux-mêmes les fiches, choisissant les qualifications juridiques et les faits à retenir.

Lorsque la photographie du visage d'une personne y figure, elle peut avoir été prise au commissariat ou à la gendarmerie, mais les policiers et gendarmes peuvent tout aussi bien avoir simplement **photographié un document d'identité** de la personne concernée

dans un autre cadre, par exemple dans la rue lors d'un contrôle, ou bien encore, après tout, collecté **une photo sur Internet**.

En théorie encore, la tenue du TAJ devrait être contrôlée par les magistrats du parquet. Pourtant, Vincent Charmoillaux, vice-procureur de Lille et secrétaire général du Syndicat de la magistrature, expliquait le 28 septembre dernier lors d'un colloque sur le fichage des étrangers organisé par le Syndicat des avocats de France à Lille, que pendant plus de 15 ans, contrairement à la loi, **les procureurs n'ont eu aucun accès direct au TAJ** qu'ils sont pourtant chargés de contrôler, et que le déploiement des outils informatiques nécessaires à un accès effectif n'était qu'une annonce très récente.

Il ajoutait que, par manque de temps, les services des parquets omettent aussi trop souvent de faire mettre à jour le TAJ lorsqu'une affaire conduit à un classement sans suite, un non-lieu ou une relaxe. Ainsi, une personne peut être **fichée pendant 20 ans pour une infraction pour laquelle elle a été mise hors de cause par la justice**. Selon lui, si l'utilisation du TAJ par la police, la gendarmerie et l'administration s'est autant développée, c'est en raison des règles bien plus strictes qui encadrent l'utilisation du casier judiciaire et qui ne leur permettent pas de satisfaire ce qu'elles jugent être leurs besoins opérationnels.

C. La reconnaissance faciale dans le TAJ

La police entretient l'absence de transparence au sujet de la reconnaissance faciale, de sorte que celle-ci reste peu documentée, et que ces pratiques ne peuvent être perçues qu'à travers une multitudes de faits divers (et désormais aussi par la campagne Technopolice)

Dès 2013, des gendarmes niçois se réjouissent auprès de Nicematin : « un homme ayant perdu la tête a été trouvé dans le jardin d'une propriété et il s'est révélé incapable de donner son nom. Les gendarmes l'ont pris en photo et nous l'ont envoyé. **Et « bingo », sa fiche est sortie.** Il a pu être identifié, puisqu'il était connu des fichiers ». Les gendarmes évoquent aussi le cas « d'un escroc ayant acquis une voiture d'occasion avec un passeport volé et falsifié mais comportant sa photo », retrouvée dans le TAJ par reconnaissance faciale.

En 2014, le Figaro rapporte à Lille un cas d'identification automatisée d'un adolescent, déjà fiché au TAJ, qui s'est vanté sur Snapchat et à visage découvert d'avoir volé un téléphone : « une fois la photo en notre possession, **il n'a fallu que quelques minutes pour que 30 ou 40 visages apparaissent à l'écran**, explique un commandant ».

En 2018, le Parisien explique que la police a exploité les photographies du TAJ par reconnaissance faciale afin d'identifier un terroriste mort. Plus récemment, une affaire judiciaire en cours à Lyon concerne l'utilisation d'un logiciel pour rapprocher l'image

prise par une caméra sur le lieu d'un cambriolage à la photographie d'une personne connue des services de la police et fichée dans le TAJ.

Ces seules anecdotes laissent comprendre que la reconnaissance faciale réalisée à partir du TAJ serait déjà **largement déployée en France et depuis longtemps**.

Pour résumer, en France, **une personne sur dix pourrait avoir sa photo dans le TAJ**. La police et la gendarmerie peuvent l'analyser automatiquement afin de la rapprocher d'images prises sur des lieux d'infraction, notamment par des caméras de surveillance. On appelle cette approche la « comparaison faciale ». C'est déjà bien trop de pouvoir pour la police, qui agit ici sans aucun contre-pouvoir effectif. Mais le fichier TES a conduit à l'extension de cette technique à l'ensemble de la population française et donc, à terme, bien au-delà des 8 millions de photographies contenus dans le TAJ.

II. Le fichier TES

La deuxième brique de l'édifice est le fichier TES, pour « titres électroniques sécurisés ». Alors que le TES n'avait à l'**origine** qu'un champ réduit (A), il s'est finalement **étendu** à l'ensemble de la population (B) pour en ficher **tous les visages** (C).

A. Le premier fichier TES (2004 – 2012)

Un règlement européen du 13 décembre 2004 impose aux États membres de délivrer des **passeports biométriques** qui, notamment, « comportent un support de stockage qui contient une photo faciale ». En pratique, le passeport intègre **une puce** qui contient une photo du visage. Elle n'est stockée nulle part ailleurs et il faut accéder physiquement au document pour la consulter. À première vue, rien qui puisse directement déboucher sur de la surveillance de masse.

Un an plus tard, le gouvernement français adopte le décret du 30 décembre 2005 qui crée les passeports électroniques afin d'appliquer ce règlement. Au passage, et sans qu'il s'agisse ici d'une exigence européenne, ce décret crée le fichier des « titres électroniques sécurisés » (**TES)** qui centralise, pour chaque personne détentrice d'un passeport électronique, ses noms, domicile, taille et couleur d'yeux. Guère plus.

Deux décrets ultérieurs changent la donne. Un premier du 23 janvier 2007 permet à la police et à la gendarmerie de consulter le fichier TES pour lutter contre le terrorisme. Un deuxième décret du 30 avril 2008 ajoute au fichier TES « **l'image numérisée du visage** ». Depuis 2005, l'image du visage n'était enregistrée que sur la puce du passeport. Par cette évolution, **le visage tombe dans les mains de l'État**.

Cette évolution ne concerne alors pas les cartes d'identité. Depuis un décret de 1987, le ministère de l'Intérieur est autorisé à réaliser un traitement de données personnelles pour

fournir des cartes d'identité. Ce système centralise nom, prénoms, date de naissance, etc., mais pas la photo, qui n'apparaît que sur la carte. Un décret du 21 mars 2007 permet à la police et à la gendarmerie de consulter ce fichier des cartes d'identités pour lutter contre le terrorisme – tel que cela a été autorisé pour les passeports deux mois plus tôt – mais sans leur donner accès à ces images.

B. Le nouveau fichier TES (2012-2016)

Une proposition de loi, soumise par deux sénateurs et adoptée par le Parlement le 6 mars 2012, prévoit de **fusionner le « TES passeport » et le fichier des cartes d'identité** en un méga-fichier unique. De plus, ce fichier unique contiendra désormais aussi les photographies présentes sur les cartes d'identité (jusqu'ici, seul le « TES passeport » contenait des photos). Le texte suscite d'importants débats : il prévoit aussi de centraliser dans ce fichier les **empreintes digitales** de l'ensemble de la population, tout en permettant à la police d'y accéder pour **identifier une personne** à partir d'une empreinte retrouvée sur les lieux d'une infraction. De nombreux parlementaires saisissent le Conseil constitutionnel qui, dans une décision du 22 mars 2012, déclare la plupart des dispositions de cette loi contraire à la Constitution. La loi, presque entièrement dépouillée, n'est jamais appliquée.

Toutefois, le gouvernement semble avoir été séduit par cette initiative parlementaire. Quatre ans plus tard, il **reprend l'essentiel de cette loi avortée** dans un décret du 28 octobre 2016, qui intègre au sein du fichier « TES passeport » toutes les données relatives aux cartes d'identité. Le nouveau « méga-fichier TES » comprend désormais les photographies de **l'ensemble de la population ou presque** : celles de toute personne demandant un passeport ou une carte d'identité.

C. Les visages du TES (2016-aujourd'hui)

Même si ce décret échappe au contrôle du Conseil constitutionnel (qui n'examine que les lois et non les décrets), le gouvernement a manifestement retenu les leçons de l'échec de 2012 : le décret prévoit explicitement que la police **ne peut pas accéder aux empreintes digitales** conservées dans le fichier TES.

Toutefois, dans le même temps, ce décret a **largement étendu le nombre de photographies accessibles** aux policiers et gendarmes (pour rappel, les photographies des cartes d'identité n'étaient jusqu'alors ni centralisées ni donc facilement exploitables par la police).

Contrairement au TAJ, le fichier TES ne prévoit pas en lui-même de fonctionnalité de reconnaissance faciale. Mais cette limite est purement technique : il ne s'agit pas d'une interdiction juridique. **Rien n'interdit que les photos du TES soient utilisées par un logiciel de reconnaissance faciale extérieur.** Ainsi, dans certaines conditions, la police

peut consulter le TES pour obtenir l'image d'une personne, la copier dans le TAJ et, à partir de là, traiter cette photo de façon automatisée pour la comparer à d'autres images, telles que celles prises par des caméras de surveillance.

Cette évolution est d'autant plus inquiétante que, contrairement au cadre initial du « TES passeport » et du fichier des cartes d'identité, la police peut accéder aux photos contenues dans ce nouveau fichier pour des raisons qui vont bien au-delà de la seule lutte contre le terrorisme.

III. La loi renseignement

La troisième brique de l'édifice est constituée des lois de sécurité qui permettent à la police de faire le lien entre le TAJ et le TES. Initialement limitées à la lutte antiterroriste, ces lois ont insidieusement **étendu leur champ** à d'autres domaines (A), jusqu'à ce que la **loi renseignement** consacre les « intérêts fondamentaux de la Nation » (B).

A. L'extension des règles d'exceptions

C'est une loi du 23 janvier 2006 sur le terrorisme qui avait autorisé la police et la gendarmerie à accéder au « TES passeport » et au fichier des cartes d'identité « pour les besoins **de la prévention et de la répression des actes de terrorisme** ». Cette loi autorisait aussi les services de renseignement à y accéder pour prévenir ces actes. Cette disposition a été appliquée par deux décrets de janvier et mars 2007, déjà cités plus tôt.

La loi du 14 mars 2011 (la même qui avait créé le TAJ) a modifié cette loi de 2006, permettant à la police et à la gendarmerie de consulter ces fichiers pour bien d'autres finalités que celles motivées par le terrorisme : atteintes à l'indépendance de la Nation, à la forme républicaine de ses institutions, aux **éléments essentiels de son potentiel scientifique et économique…**

La loi de programmation militaire de 2013 poursuit cette extension. La liste de finalités est entièrement remplacée par le vaste ensemble des « intérêts fondamentaux de la Nation ». Il faut attendre la loi renseignement de 2015 pour bien cerner ce que recouvrent ces « intérêts fondamentaux de la Nation », dont elle donne **une liste explicite**.

B. Les intérêts fondamentaux de la Nation

Cette liste se retrouve à l'article L811-3 du code de la sécurité intérieure

On y trouve des « intérêts » assez classiques, liés à la sécurité : indépendance nationale, prévention du terrorisme ou de la prolifération d'armes de destruction massive. On y trouve aussi des « intérêts » d'ordre purement politico-économiques : politique étrangère et exécution des engagements européens de la France, intérêts économiques, industriels et scientifiques. Enfin, un troisième groupe est bien plus ambigu : « atteintes à la forme

républicaine des institutions » et « **violences collectives de nature à porter gravement atteinte à la paix publique** ».

Juste après son vote au Parlement, la loi renseignement a été examinée par le Conseil constitutionnel. Dans sa décision du 23 juillet 2015, celui-ci a défini concrètement ce à quoi renvoient certaines de ces notions. Les « violences collectives » recouvrent ainsi les « incriminations pénales définies aux articles 431-1 à 431-10 du code pénal ». Parmi ceux-ci, l'article 431-4 sanctionne le fait de « **continuer volontairement à participer à un attroupement après les sommations » de se disperser**. L'article 431-9 sanctionne le fait d'organiser une **manifestation non-déclarée ou interdite**. Pour toutes ces situations, policiers et gendarmes sont donc à présent autorisés à accéder aux photographies contenues dans le fichier TES.

IV. Le fichage des manifestants

Maintenant que toutes les briques de l'édifice sont posées, il s'agit de voir comment la police peut l'utiliser pour identifier les manifestants par reconnaissance faciale. Deux cas sont facilement envisageables – la lutte contre les **attroupements** (A) et contre les **manifestations illégales** (B) – qui nous permettent d'interroger la **situation concrète** du dispositif (C).

A. Fichage après sommations

Prenons un exemple concret. Une manifestation se tient dans une grande ville. La police intervient pour disperser le cortège. **Elle fait deux sommations puis photographie la foule.** Les personnes dont le visage est visible sur le cliché n'étaient manifestement pas en train de se disperser. Les policiers considèrent qu'il s'agit d'indices graves et concordants selon lesquels ces personnes commettent le délit défini à l'article 431-4 du code pénal, à savoir « continuer volontairement à participer à un attroupement après les sommations ». Une fiche est ouverte dans le TAJ pour chacune d'elle : leur nom est encore inconnu et la fiche ne contient donc que leur photo, accompagnée de la date et du lieu de l'événement.

La police est autorisée à utiliser des logiciels de reconnaissance faciale pour **établir un lien entre la photo contenue dans le TAJ à une autre photo collectée ailleurs**. Lutter contre cette infraction constitue un « intérêt fondamental de la Nation » (la prévention des violences collectives) qui permet à la police de collecter ces autres photos dans le fichier TES, où presque toute la population sera à terme fichée (au gré des renouvellements de cartes d'identité et de passeports).

Pour obtenir une photo dans le TES, il faut avoir le nom de la personne concernée. Ainsi, pour identifier les manifestants, la police techniquement peut interroger le fichier TES à

partir du nom de chaque personne dont elle estime qu'elle a pu participer à la manifestation. Cette liste de noms peut être constituée de nombreuses façons : renseignements policiers en amont, groupes Facebook, personnes ayant retweeté un appel à manifester, etc. Après tout, si elle veut arriver à ses fins, la police peut directement utiliser la liste de noms des habitant·e·s d'une ville ou d'un quartier.

Une fois la liste de noms constituée, celle-ci permet à la police de réunir au sein du TES un ensemble de photographies. **Chaque photo est comparée de façon automatisée aux photos ajoutées dans TAJ** à l'issue de la manifestation, afin d'établir des correspondances. Chaque fois que le logiciel de comparaison faciale trouve une correspondance, les données (noms, prénoms, date de naissance, adresse, etc.) issues de la fiche TES d'une personne peuvent être transférées dans le fichier TAJ pour venir garnir la fiche du manifestant qui, jusqu'ici, était resté anonyme.

Ce processus **se renforce au fur et à mesure des manifestations** : dès que des participantes ont été fichés au TAJ avec leur photographie, il devient toujours plus aisé de les retrouver lors des manifestations suivantes en allant les chercher directement dans le TAJ sans plus avoir à passer par le TES.

B. Fichage des complices

Le refus de se dissiper après sommation n'est pas la seule infraction qui permet de ficher massivement les manifestants. Comme vu ci-dessus, la lutte contre **l'organisation de manifestations interdites ou non-déclarées** est, d'après le Conseil constitutionnel, un autre « intérêt fondamental de la Nation » qui permet de fouiller le TES. Or, tel que vu plus haut, toute personne peut être fichée au TAJ en simple qualité de **complice d'un délit**, et notamment de celui-ci.

Dès lors, que penser de ce qu'a déclaré Emmanuel Macron lors des mouvements sociaux de l'an dernier : « Il faut maintenant dire que lorsqu'on va dans des manifestations violentes, **on est complice du pire** » ? De même, que penser de ces propos de Gérard Collomb, ministre de l'Intérieur au même moment : « Il faut que les [manifestants] puissent s'opposer aux casseurs et ne pas, par leur passivité, être d'un certain point de vue, **complices de ce qui se passe** » ?

Ne s'agit-il pas d'autorisations données aux forces de l'ordre de considérer presque tous les manifestants comme complices de chaque manifestation partiellement interdite ou non-déclarée à laquelle ils participent ? Leur fichage massif dans le TAJ à partir du fichier TES en serait permis. Dans ce cas de figure, la police serait autorisée à chercher à identifier toutes les personnes figurant sur des photos prises au cours de manifestations.

C. Que se passe-t-il en pratique ?

Ces différents exemples illustrent le fait que le droit actuel permet déjà la généralisation de la reconnaissance faciale des manifestants. Sans contre-pouvoir effectif, difficile d'y voir clair sur les pratiques réelles des policiers et gendarmes.

Peu importe que ce fichage soit ou non déjà généralisé en pratique, il est **déjà autorisé, ne serait-ce qu'en théorie**, et cela de différentes façons. Dans ces conditions, **difficile d'imaginer que ces techniques ne soient pas déjà au moins expérimentées sur le terrain**. Difficile d'imaginer que, parmi la dizaine de drones déployés dernièrement au-dessus des manifestations, aucun n'ait jamais participé à une telle expérimentation, si tentante pour les forces de l'ordre et soumise à si peu de contrôle effectif. C'est d'autant plus probable quand on voit à quel point « l'analyse vidéo » a été présentée comme cruciale dans la répression des manifestations de l'hiver dernier (2018-2019).

De plus, la présente démonstration concerne le fichage massif des manifestants. Elle s'intéresse à l'hypothèse selon laquelle n'importe quelle personne peut faire l'objet d'un fichage policier particulièrement intrusif grâce à la reconnaissance faciale. C'est pour cette raison que nous nous sommes attardé·e·s à démontrer comment la police pouvait accéder au TES, où la quasi-totalité de la population est fichée.

Toutefois, une démonstration plus simple pourrait se limiter à **la seule utilisation du TAJ, qui autorise à lui seul et depuis 2012 la reconnaissance faciale des manifestants**. Certes, cette reconnaissance faciale ne concernerait alors que les personnes dont le visage est déjà contenu dans le TAJ, suite à une interaction antérieure avec la police. Mais, comme nous l'avons vu, le fichier TAJ concerne déjà une part significative de la population.

Conclusion

Les conséquences découlant du fait d'être fiché dans le TAJ en tant que « **participant à une manifestation violente** » sont suffisamment graves pour dissuader une large partie de la population d'exercer son droit de manifester.

L'article R40-29 du code de procédure pénal prévoit que le TAJ est consultable dans le cadre d'« **enquêtes administratives** » : l'administration peut vérifier qu'une personne n'y est pas fichée avant de l'embaucher dans de nombreuses fonctions publiques, pour encadrer certaines professions privées liées à la sécurité ainsi que pour délivrer ou renouveler des titres de séjour aux personnes étrangères.

Une personne raisonnable pourrait tout à fait vous **déconseiller de participer à des manifestations à l'avenir**. Elle vous inviterait à renoncer à ce droit fondamental : les risques sont trop importants, surtout si vous imaginez rejoindre un jour la fonction

publique ou que vous n'êtes pas de nationalité française. Une personne encore plus raisonnable vous dirait l'inverse : **ce système est intolérable et il nous faut le déconstruire**.

Nous venons d'envoyer au gouvernement une demande d'abrogation des dispositions du décret TAJ qui autorisent la reconnaissance faciale. Ce décret permet de recourir massivement à cette technique **sans que la loi ne l'ait jamais autorisée**, ce que la CNIL a récemment et clairement rappelé être illégal dans des affaires similaires. Si le gouvernement rejette notre demande, nous attaquerons le décret TAJ devant le Conseil d'État.

* * * * *

Quand la France se lance dans la reconnaissance faciale

Par Pierre Januel le mercredi 02 octobre 2019 sur le site de Nextimpact.com

Si des expériences locales de reconnaissance faciale ont été fortement médiatisées, d'autres pratiques restent plus discrètes. En coulisses, les industriels poussent pour que la France ne soit pas à la traîne et l'Intérieur est sensible aux arguments. L'idée d'une loi pour encadrer les expérimentations progresse rapidement et selon nos informations, un texte pourrait être déposé dès cet automne. Enquête.

La reconnaissance faciale n'est pas quelque chose d'inédit en France. Récemment, le décret qui impose cette technologie pour l'outil d'authentification en ligne ALICEM a été attaqué par La Quadrature du Net.

L'une des utilisations les plus importantes reste celle autour du fichier TAJ (Traitement des antécédents judiciaires). Géré par la police et la gendarmerie, ce fameux fichier rassemble les informations sur les procédures policières. Il contient 18,9 millions de fiches de personnes mises en cause, près de 8 millions de photos et représente 6 téraoctets de données.

L'un des soucis récurrents de ce fichier est celui des doubles identités. Fréquemment, des personnes mises en cause déclarent à la police une fausse identité. Depuis 2017, une application permet donc de faire la chasse aux doublons, via des dispositifs de reconnaissance faciale. Selon un rapport du député Didier Paris, « *cette fonctionnalité permet également de proposer des tapissages de photos faciales de suspects afin de les soumettre aux victimes* ».

La reconnaissance faciale via le TAJ permet aussi de résoudre des enquêtes. L'attentat au couteau qui a eu lieu à Paris en mai 2018 ou du « terroriste à vélo » qui a posé une bombe

à Lyon en mai 2019 en sont deux exemples. Mais la reconnaissance faciale est aussi utilisée pour des infractions moins graves, comme pour ce vol de camion en septembre. L'enquête a abouti grâce à une image tirée du système de vidéo-surveillance de l'entreprise. Rien n'empêche les enquêteurs d'utiliser la comparaison faciale dans une procédure pénale.

Autre fichier, le Fichier des personnes recherchées (FPR) contient lui aussi des photos. Il rassemble près de 600 000 personnes recherchées pour différents motifs, des fameux « fichés S » aux mineurs en fugue. Dans un avenir proche, une consultation du FPR pourra se faire à partir d'une photo.

Ces systèmes de reconnaissance pourraient gagner en mobilité : actuellement, les tablettes NEO des forces de l'ordre ne permettent pas la consultation des fichiers à partir de la biométrie. Toutefois, comme le notait le rapport de Didier Paris, « *l'appareil photo intégré offre des perspectives intéressantes peu explorées et qui pourraient être prometteuses* ».

Selon le service du ministère de l'Intérieur qui suit les modernisations technologiques (ST(SI)²), « *des projets en laboratoire chez certains industriels en ont déjà démontré la faisabilité. D'ici deux ans, sans ajout d'appareil de capture biométrique, NEO pourrait être un vecteur de contrôle et d'identification des personnes recherchées, ou des étrangers en situation irrégulière, et de contrôle aux frontières* ».

Fin mai dernier, selon nos informations, le gouvernement a publié un appel à compétences à destination des industriels. L'accord-cadre sur le TAJ devant être renouvelé fin 2020, le ministère de l'Intérieur a sollicité les entreprises afin qu'elles l'aident à la préparation de ce marché public.

Le but est d'établir la faisabilité technique du besoin mis à jour par les forces de l'ordre. « *La création de tapissage photo et l'utilisation en mobilité sont quelques-unes des fonctionnalités recherchées en plus de celles proposées nativement par les solutions.* » On parle également de reconnaître les tatouages ou les cicatrices.

Les expérimentations de reconnaissance faciale en temps réel

Si, pour le traitement des infractions, la loi permet l'utilisation de la reconnaissance faciale, le cadre est plus flou concernant la reconnaissance en temps réel via des caméras. L'État a cependant été partie prenante de plusieurs expérimentations.

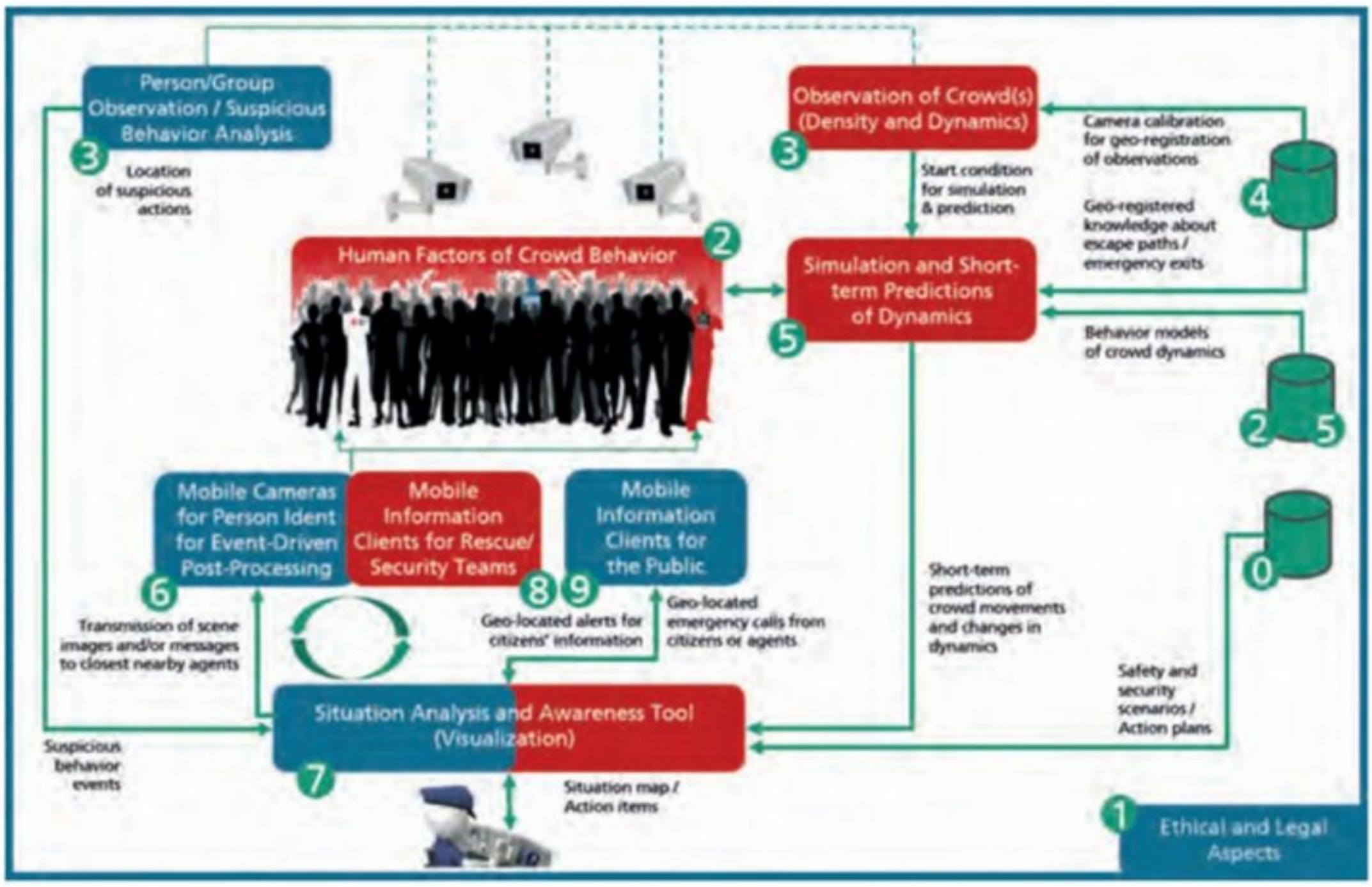
Citons ainsi le projet VOIE (« *Vidéoprotection Ouverte et IntégréE* »), qui associait des industriels (Thales, Morpho devenu Idemia, Deveryware), des transporteurs (SNCF, RATP), la préfecture de police de Paris et avait bénéficié d'un financement de la Banque publique d'investissement. L'objectif était le suivi d'individus et l'analyse de vidéo dans le cadre de réquisitions judiciaires. Le projet avait même reçu le prix « *Coup de Cœur* »

aux Trophées de la Sécurité 2015. Mais la CNIL s'était opposée aux traitements en temps réel dans l'espace public.

Autre projet de recherche, démarré en 2017 : S²UCRE (« *Safety and Security of UrbanCrowded Environments* »). Mené avec l'Allemagne et bénéficiant d'un financement d'un million d'euros de l'Agence nationale pour la recherche, S²UCRE est destiné à la gestion des foules.

Il vise à combiner cinq domaines technologiques, basés sur de l'analyse vidéo avec des méthodes de simulation : outre la surveillance d'une foule, l'objectif est de prédire son comportement à court terme, de repérer des comportements suspects, détecter et géolocaliser des auteurs d'infraction et repérer les équipes de sécurité.

Comme souvent, ce projet est mené par un consortium qui regroupe industriels, institutions et universitaires. S²UCRE est conduit par Idemia (ex « *Safran Identifiy & Security* ») avec pour partenaires Deveryware et la préfecture de police de Paris. Selon nos informations, pour expérimenter et passer outre les barrières réglementaires françaises, les autorités françaises ont passé un partenariat avec Singapour, modèle mondial de Safe city, qui teste cette solution.



Aéroports et collectivités locales

À Paris, si la reconnaissance des véhicules se développe, la préfecture de police ne prévoit pas pour l'instant de reconnaissance faciale en temps réel des personnes. Et ce,

même si les caméras se multiplient et si la construction de centres de commandement, comme à Marseille, permettra, à terme, de centraliser les flux vidéos de plusieurs acteurs (collectivités, transports...). La reconnaissance faciale en temps réel se développe plutôt dans d'autres lieux.

Chaque mois, le bulletin officiel du ministère de l'Intérieur indique que les sas Parafe (« *Passage automatisé rapide aux frontières extérieures* ») sont mis en place dans de nouveaux aéroports, ou dans d'autres lieux de passage frontaliers comme le Tunnel sous la Manche.

Pour accélérer ses contrôles, le passager a le choix d'utiliser la reconnaissance faciale. Cet été, quatre-vingts de ces sas étaient en activité à Roissy. Mais les contrôles aux frontières ne sont qu'une première étape. Selon L'Express, deux compagnies, dont Air France, devraient tester pour un an la reconnaissance faciale sur les systèmes de dépose bagages et à l'embarquement des avions. Le visage devient billet.

Une autre expérimentation, très médiatisée, fut celle du carnaval de Nice. La ville avait utilisé le logiciel Anyvision de la société Confidentia. Parmi les fonctionnalités testées : la reconnaissance de personnes dans la file d'attente, mais également dans la foule, de jour comme de nuit. Le journal Le Monde a dévoilé le bilan de l'expérimentation. Sans surprise, la ville est enthousiaste. Le logiciel a même été capable de reconnaître une personne avec des lunettes, distinguer deux « vrais jumeaux » ou identifier une personne à partir d'une photo vieille de 40 ans.

Pour passer les barrages légaux, la ville avait demandé leur consentement préalable aux 5 000 personnes testées. La ville a également fait une « *étude d'acceptabilité* » en marge du carnaval. Parmi les neuf questions posées aux carnavaleux, la dernière donne le ton : « *Face à l'avancée des nouvelles technologies, considérez-vous qu'il soit nécessaire de modifier davantage la loi Informatique et Libertés de 1978 ?* » Les deux tiers des personnes répondent oui, 10 % non, 23 % ne se prononçant pas.

Christian Estrosi, maire d'une ville où il a fait installer 3 000 caméras, est un militant de longue date de la reconnaissance faciale. Il avait déjà poussé cette technologie pour l'Euro 2016. La première proposition de loi pour légaliser l'expérimentation de reconnaissance faciale vient de la députée Marine Brenier... son ex-suppléante.

Vers une loi pour expérimenter la reconnaissance faciale ?

La députée Brenier n'est pas la seule. D'autres parlementaires s'y sont intéressés. Surtout, à l'Intérieur et chez les industriels, beaucoup poussent au développement de cet outil avec une angoisse : se faire dépasser par les Américains et les Russes.

La France veut mettre en avant ses champions comme Idemia, Thales ou Gemalto. Avec un mot d'ordre qui revient souvent : « *l'acceptabilité d'une technologie* » et la volonté de construire un cadre plus éthique que le modèle chinois, qui sert de repoussoir.

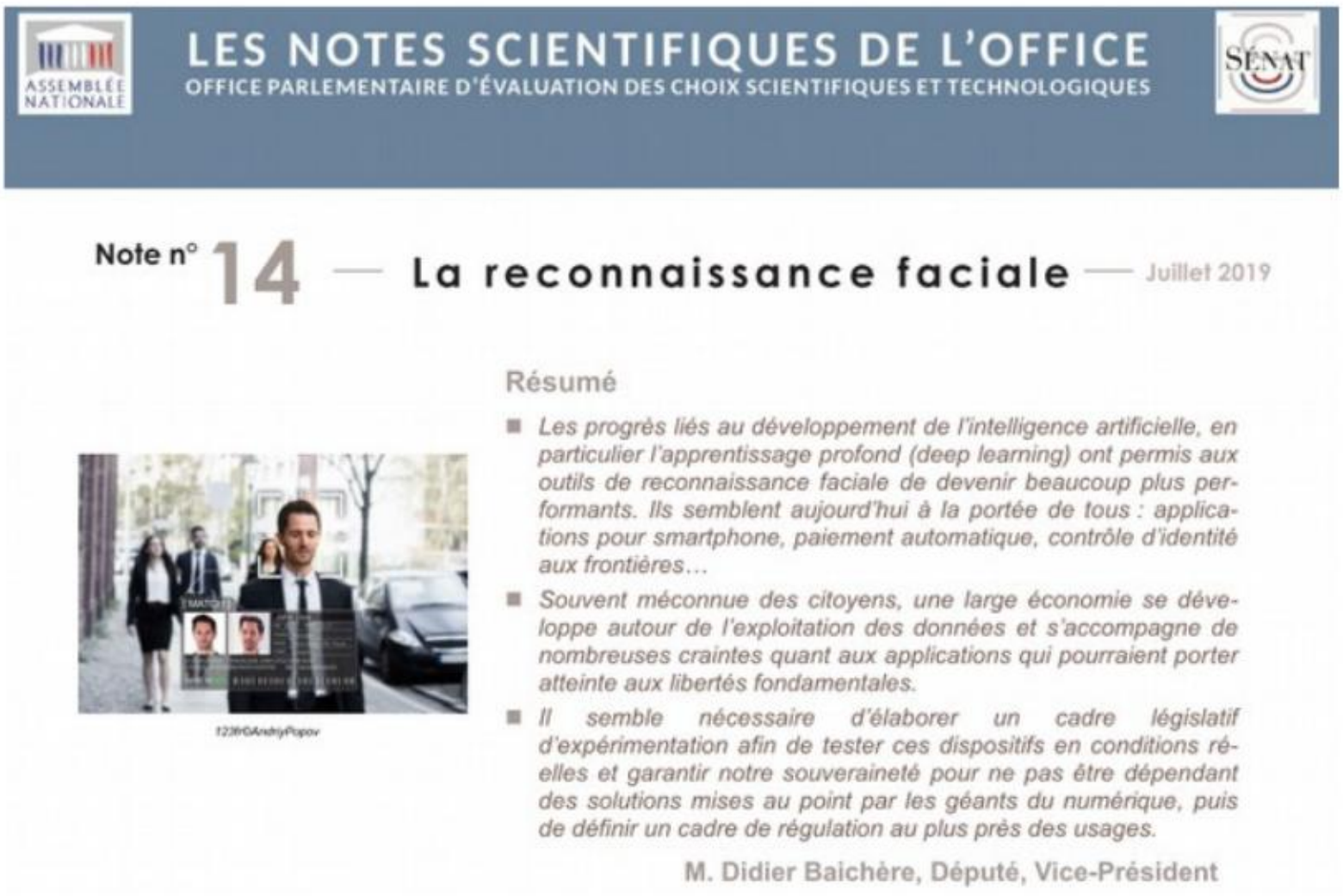
Pour dépasser les résistances, les acteurs soulignent que des outils de reconnaissance faciale se développent rapidement dans un cadre privé. Et que les enjeux sécuritaires importants vont arriver. Comme le souligne un chercheur du Creogn, « *la Coupe du monde de rugby en 2023 et les JO de Paris en 2024 représentent des opportunités remarquables de convaincre la population de l'intérêt de déployer la reconnaissance faciale.* »

De nombreuses voix demandent l'adoption d'un nouveau cadre légal. En septembre 2018, la CNIL a appelé « *d'urgence à un débat démocratique* » sur les nouveaux usages des caméras vidéo, et « *à ce que le législateur puis le pouvoir réglementaire se saisissent de ces questions.* »

L'appel a été entendu. Ainsi, le 24 septembre dernier, les 24ème Technopolice, qui tous les six mois traitent des enjeux techniques pour les forces de l'ordre, avaient pour thème : « *Reconnaissance faciale – Applications, Acceptabilité, Prospective* ». Nous n'avons pas été autorisés à nous y rendre. Mais, mis à part une intervention offensive de la Quadrature du Net, la plupart des intervenants ont appelé à l'adoption d'un cadre légal.

Selon L'Essor, le préfet Renaud Vedel a martelé la nécessité d' « *accepter de trouver un équilibre entre des usages régaliens et des mesures protectrices pour nos libertés. Car sinon, la technologie sera mûrie à l'étranger et nos industriels, pourtant leaders mondiaux, perdront cette course.* »

Autre initiative : le Forum économique mondial et le Conseil national du numérique ont lancé un projet de coconstruction d'une régulation de la reconnaissance faciale. Des ateliers vont se tenir durant toute cette année (le dernier avait lieu le 1er octobre).


LES NOTES SCIENTIFIQUES DE L'OFFICE
OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES
Note n° 14 — La reconnaissance faciale — Juillet 2019
Résumé
Les progrès liés au développement de l'intelligence artificielle, en particulier l'apprentissage profond (deep learning) ont permis aux outils de reconnaissance faciale de devenir beaucoup plus performants. Ils semblent aujourd'hui à la portée de tous : applications pour smartphone, paiement automatique, contrôle d'identité aux frontières…
Souvent méconnue des citoyens, une large économie se développe autour de l'exploitation des données et s'accompagne de nombreuses craintes quant aux applications qui pourraient porter atteinte aux libertés fondamentales.
Il semble nécessaire d'élaborer un cadre législatif d'expérimentation afin de tester ces dispositifs en conditions réelles et garantir notre souveraineté pour ne pas être dépendant des solutions mises au point par les géants du numérique, puis de définir un cadre de régulation au plus près des usages.
M. Didier Baichère, Député, Vice-Président
123RFGAndriyPopov

Parlementaire le plus actif sur le sujet, le député Didier Baichère a publié cet été [une note sur la reconnaissance faciale](). Le document insiste sur les imperfections de cette technologie et ses effets discriminatoires (couleur de peau, âge,...).

Joint par Next INpact, le parlementaire plaide la nécessité d'un cadre légal pour mener des expérimentations. Pour lui, il est nécessaire de tester plus solidement les algorithmes européens, afin qu'ils évitent les différents biais discriminatoires. Il faut également impliquer plus fortement les citoyens dans le débat sur la reconnaissance faciale. Cela doit passer par une loi.

Didier Baichère a également noté l'intérêt de la nouvelle présidente de la Commission européenne Ursula von der Leyen pour donner [un cadre européen à la reconnaissance faciale](). Pour le député, anticiper une nouvelle législation européenne et mener des expérimentations permettrait à la France d'avoir un pouvoir d'initiative. Parmi les pistes qu'il étudie : donner à la CNIL un rôle d'accompagnement de l'innovation, sur le modèle de ce que fait l'Arcep.

En lien avec différents acteurs, il travaillera donc à un texte législatif cet automne. Toutefois, le calendrier parlementaire rend peu probable une proposition de loi sur ce seul sujet. Le véhicule législatif qui intégrerait cette disposition pourrait venir l'an prochain, avec le projet de loi « *décentralisation et différenciation* » des collectivités locales. Le débat commence tout juste.

* * * * *

Pour avoir accès aux sources des 2 articles :

1) https://www.laquadrature.net/2019/11/18/la-reconnaissance-faciale-des-manifestants-est-deja-autorisee/

2) https://www.nextinpact.com/news/108256-quand-france-se-lance-dans-reconnaissance-faciale.htm

Un site qui donne des méthodes de maquillage pour casser la reconnaissance faciale : https://cvdazzle.com/