CONSEIL D'ETAT, 10EME ET 9EME CHAMBRES REUNIES, ARRET DU 4 NOVEMBRE 2020, LA QUADRATURE DU NET/ ETAT

MOTS CLEFS : RGPD – biométrie – données personnelles– identité numérique

Depuis juin 2019, l'application « Authentification en ligne certifiée sur mobile » dite ALICEM est en phase de test sur la plateforme « France Connect » et ce à l'initiative du gouvernement français. Cette technologie utilise la reconnaissance faciale pour s'assurer de l'identité des utilisateurs, et porte des enjeux à la fois juridiques et techniques. C'est en partie ce pourquoi elle fait polémique. Mais malgré qu'elle soit décriée, l'application a été validée par le Conseil d'État le 4 novembre dernier et verra bien le jour.

FAITS : Le décret n°2019-452 du 13 mai 2019 a autorisé la mise en œuvre d'une application ayant pour finalité de proposer aux titulaires d'un passeport ou d'un titre de séjour biométrique la délivrance d'un moyen d'identification électronique, leur permettant, grâce à leur téléphone mobile doté d'un dispositif de lecture sans contact, de se connecter aux services publics et privés français.

PROCEDURE : Pour une association, ce système soulève des enjeux tant en matière de protection des données personnelles qu'au regard des risques d'atteintes aux droits et libertés individuelles. C'est pourquoi elle a demandé au Conseil d'état d'annuler ledit décret pour excès de pouvoir et, à titre subsidiaire, de poser à la CJUE des questions préjudicielles. Concernant l'appréciation de la validité du consentement ainsi que celle du caractère adéquat, pertinent et non excessif, de la collecte et du traitement des données biométriques, au regard des finalités pour lesquelles elles sont collectées et traitées par une application mobile recourant à une technologie de reconnaissance faciale à des fins d'authentification auprès de certains services publics et de leurs partenaires. L'association fait également valoir la position de la CNIL, qui avait souligné l'importance de subordonner le traitement prévu à des solutions alternatives au recours à la biométrie, afin que la personne qui refuserait de se soustraire à la reconnaissance faciale ne soit pas lésée.

PROBLEME DE DROIT : Est-ce illégal de conditionner la création d'une identité numérique à un traitement de reconnaissance faciale obligatoire ?

SOLUTION : Dans un arrêt rendu le 4 novembre 2020, le Conseil d'Etat rejette la demande de l'association et par conséquent valide l'ALICEM. L'utilisation de la reconnaissance faciale à des fins d'identification et d'authentification, et le traitement des données biométriques qui en découle, utilisé en priorité pour l'accès à des services dont les fournisseurs sont liés par convention à FranceConnect, est entièrement légale et légitime.

SOURCES :

V. Cimino, « Malgré le recours déposé par la Quadrature du Net le système de reconnaissance faciale Alicem verra bien le jour », siecledigital.fr, 6 novembre 2020.
L. Costes, « Création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile », Revue Lamy Droit de l'Immatériel, Nº 160, 1er juin 2019

NOTE :

Dans une société du « tout numérique » la certification de l'identité dans un monde digital complémentaire au « monde physique » semble impérative et doit se faire à un niveau de fiabilité de sécurité comparable à celui que les titres d'identité fournissent au quotidien. ALICEM est la première expérimentation d'un service plus large d'identité numérique en cours de conception dans le cadre d'un programme interministériel mis en place en janvier 2018.

ALICEM, une technologie respectueuse de la législation en vigueur en matière de données

En l'espèce, le Conseil d'état s'est prononcé sans équivoque : ALICEM répond aux strictes exigences de traitement des données biométriques définies par le RGPD et la loi Informatique et Libertés. Concernant le consentement, les juges rappellent l'interdiction de principe posée par l'article 8 de la loi du 6 janvier 1978, relative au traitement des données biométriques aux fins d'identifier une personne physique de manière unique, et contrebalance avec le fait que cette interdiction n'est pas absolue puisque le RGPD (art.9) permet de déroger au principe si la personne en question donne son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques. De plus, selon la Commission nationale de l'information et des libertés « le consentement n'est susceptible d'être valide que dans l'hypothèse où la personne concernée dispose d'un contrôle et d'un choix réel concernant l'application avec la possibilité de les refuser sans subir de préjudice ». En examinant cette question, le Conseil d'état estime que celui qui refuse d'utiliser cette technologie « ne subit aucune conséquence négative quant à la nature des services accessibles ». Dans la mesure « les télé services accessibles via l'application Alicem l'étaient également, à la date du décret attaqué, à travers le dispositif FranceConnect, dont l'utilisation ne présuppose pas le consentement à un traitement de reconnaissance faciale », aucun citoyen n'est contraint de recourir à l'ALICEM. Par conséquent, il n'y a pas lieu de dire que sa mise en place prive d'emblée d'accès aux télétraitements offerts par l'ensemble des services publics celui ou celle qui ne souhaite pas recourir à l'application.
S'agissant du caractère pertinent, adéquat et non excessif de la collecte de ces données, le décret autorise le traitement ALICEM à lire les données enregistrées dans le composant électronique des passeports et des titres de séjour étrangers, à l'exception des empreintes digitales. Les données collectées par ce système de reconnaissance faciale ont pour seule fin l'identification de l'usager et sont effacées sitôt ces reconnaissances terminées. Le Conseil d'Etat observe que la collecte par l'ALCEM répond aux exigences légales, à savoir que les finalités, la nature et la durée de conservation des données traitées et enregistrées ainsi que les catégories de personnes ayant accès à ces données ne sont pas laissés au hasard mais définis par le décret de mai 2019.

Reconnaissance faciale et données biométriques, une garantie pour l'identité numérique

Parmi les nombreuses révolutions numériques, celle de l'identité est l'une des plus discrète mais son importance demande une grande vigilance. Le monde réel et le monde virtuel s'entremêlent, le gouvernement tente en utilisant la technologie de la reconnaissance faciale par le biais de l'ALICEM de lutter contre l'usurpation d'identité et de façon plus générale de lutter contre la cybercriminalité. Toutefois, l'espace numérique, conçu comme un champ ouvert et de liberté, est aussi le terrain de nombreuses malversations. En l'espèce, le Conseil d'Etat a admis qu'il ne ressortait pas « des pièces du dossier que, pour la création d'identifiants électroniques, il existait [lors du recours] d'autres moyens d'authentifier l'identité de l'usager de manière entièrement dématérialisée en

présentant le même niveau de garantie que le système de reconnaissance faciale. ». Les juges se sont donc assurés que le système mise en œuvre soit doté d'un niveau de garantie « élevé » au sens du règlement européen « eIDAS » du 23 juillet 2014 avant qu'il soit mis à disposition du public. Outre garantir la sécurité des citoyens, l'ambition est également de renforcer leur croyance dans le numérique. En validant ALICEM, le Conseil d'état rompt la lignée jurisprudentielle à propos de la reconnaissance faciale. Rappelons que le Tribunal Administratif de Marseille avait annulé la délibération du conseil régional de Provence-Alpes-Côte d'Azur visant à expérimenter cette technologie à l'entrée de deux lycées de la région. En effet, pour être en accord avec la position de la CNIL en la matière, les juges avaient considéré cette expérimentation comme contraire aux principes de proportionnalité et de minimisation des données issus du RGPD. Aussi, l'approbation de la reconnaissance faciale aux fins d'identification diffère selon le contexte. De plus, la carte d'identité numérique devrait apparaître dès août 2021, ce qui suscitera très certainement de nouveaux bouleversements. L'utilisation de la biométrie fait l'objet de controverse, mais cette décision enrichit toutefois la jurisprudence relative à l'application du RGPD.

Emma Cedrone
Master 2 Droit des médias électroniques
AIX-MARSEILLE UNIVERSITE, LID2MS-IREDIC 2011

ARRET :

CE, Conseil d'Etat, 4 novembre 2020, La Quadrature du Net/ Etat

7. Par ailleurs, l'article 7 de la loi du 6 janvier 1978 dispose, dans sa rédaction applicable au litige, que : " Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée, dans les conditions mentionnées au 11) de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ". L'article 4 (11) du règlement général sur la protection des données définit le consentement comme " toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ". En outre, l'article 7 du même règlement précise que : " 4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ". Il est indiqué au considérant 42 du même règlement que " Le consentement ne devrait pas être considéré comme ayant été donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix ou n'est pas en mesure de refuser ou de retirer son consentement sans subir de préjudice " tandis que son considérant 43 précise que : " Le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution ".

9. D'autre part, il ressort des pièces du dossier que les téléservices accessibles via l'application " Alicem " l'étaient également, à la date du décret attaqué, à travers le dispositif FranceConnect, dont l'utilisation ne présuppose pas le consentement à un traitement de reconnaissance faciale. Dès lors que les usagers qui ne consentiraient pas au traitement prévu dans le cadre de la création d'un compte Alicem peuvent accéder en ligne, grâce à un identifiant unique, à l'ensemble des téléservices proposés, ils ne sauraient être regardés comme subissant un préjudice au sens du règlement général sur la protection des données précité. Il s'ensuit que l'association requérante n'est pas fondée à soutenir que le consentement des utilisateurs de l'application Alicem ne serait pas librement recueilli ni, par suite, que le décret attaqué méconnaîtrait pour ce motif les dispositions du règlement général sur la protection des données et de la loi du 6 janvier 1978.

10. Par ailleurs, l'article 6 de la loi du 6 janvier 1978 dispose, dans sa rédaction applicable à la date du litige, que les données à caractère personnel doivent être " 3° (...) adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ". Pour l'application de ces dispositions, les données pertinentes au regard de la finalité d'un traitement sont celles qui sont en adéquation avec la finalité du traitement et qui sont proportionnées à cette finalité. En vertu de l'article 7 du décret attaqué est prévue la collecte de données relatives, en premier lieu, à l'identification de l'usager, en deuxième lieu à l'identification de son titre biométrique, en troisième lieu à l'équipement terminal de communications électroniques qu'il utilise et, enfin, à l'historique des transactions associées à son compte, ces dernières données ne pouvant être communiquées aux fournisseurs de téléservices en vertu de l'article 9. Eu égard à leur objet et aux finalités du traitement rappelées au point 1, le recueil de ces données doit être regardé comme adéquat et proportionné à cette finalité.