Commission nationale de l'informatique et des libertés

Délibération n° 2018-342 du 18 octobre 2018 portant avis sur projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité » (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile demande d'avis n° 18008244

NOR : *CNIX1911892X*

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre de l'intérieur d'une demande d'avis concernant un projet de décret autorisant la création d'un traitement automatisé permettant de délivrer une identité numérique dénommée « Application de lecture de l'identité d'un citoyen en mobilité » (ALICEM) ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE ;

Vu le règlement (UE) 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (« e-IDAS ») ;

Vu le règlement d'exécution (UE) 2015/102 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 susvisé ;

Vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales ;

Vu le code de l'entrée et du séjour des étrangers et du droit d'asile, notamment ses articles R. 311-13-1, R. 611-1 et suivants ;

Vu le code des postes et des communications électroniques, notamment son article L. 102 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (« TES ») ;

Vu l'arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect » ;

Vu l'arrêté du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DOCVERIF » ;

Vu la délibération n° 2015-254 du 6 juillet 2015 portant avis sur un projet d'arrêté portant création d'un traitement automatisé de donnée à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect » ;

Vu la délibération n° 2016-292 du 29 septembre 2016 pour avis sur un projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (« TES ») ;

Vu la délibération n° 2016-218 du 21 juillet 2016 portant avis sur un projet d'arrêté autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DOCVERIF » ;

Après avoir entendu M. François PELLEGRINI, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

La Commission a été saisie par le ministre de l'intérieur d'une demande d'avis concernant un projet de décret en Conseil d'Etat autorisant la création d'un traitement automatisé permettant de délivrer une identité numérique dénommé « Application de lecture d'un citoyen en mobilité » (« ALICEM »). Ce traitement, mis en œuvre par la direction de la modernisation et de l'action territoriale, doit permettre aux personnes majeures titulaires d'un passeport biométrique ou d'un titre de séjour étranger électronique de se créer une identité numérique à partir de leur titre d'identité sur son application mobile puis de s'identifier et de s'authentifier à des fournisseurs de services en ligne.

Elle relève que le traitement projeté repose sur un système de reconnaissance faciale permettant de vérifier l'exactitude de l'identité alléguée par la personne recourant à ce dispositif, l'identité numérique ainsi créée pouvant être utilisée pour s'identifier et s'authentifier auprès de services en ligne.

Compte tenu de ses finalités, la Commission estime que le traitement ALICEM relève du champ d'application du règlement (UE) 2016/679 du 27 avril 2016 susvisé (ci-après « RGPD ») et doit être examiné au regard de ces dispositions. Elle rappelle également que l'article 9.4 du RGPD prévoit que le droit national peut introduire des conditions supplémentaires en ce qui concerne les traitements de données biométriques.

Le traitement de données à caractère personnel, qui doit être regardé compte tenu de l'économie générale du dispositif décrite ci-après comme mis en œuvre pour le compte de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique, porte sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. Il doit dès lors faire l'objet d'un décret en Conseil d'Etat, pris après avis

motivé et publié de la Commission conformément aux dispositions de l'article 27 de la loi du 6 janvier 1978 modifiée.

Elle relève par ailleurs que le présent projet de décret, qui a été accompagné d'une analyse d'impact, modifie également le code de l'entrée et du séjour des étrangers et du droit d'asile (« CESEDA »). En particulier, il est prévu de modifier l'article R. 611-1 du CESEDA pour permettre la mise en relation du traitement « AGDREF 2 » (Application de gestion des dossiers des ressortissants étrangers en France) avec le traitement « DOCVERIF » et permettre ainsi la transmission à DOCVERIF des données relatives aux titres des ressortissants étrangers. Cette mise en relation n'appelle pas en soi d'observation particulière.

En ce qui concerne le traitement AGDREF 2, la Commission rappelle qu'il a pour finalité principale de « garantir le droit au séjour des ressortissants étrangers en situation régulière et de lutter contre l'entrée et le séjour irréguliers en France des ressortissants étrangers ». Ce traitement constitue ainsi le fichier principal de gestion administrative des étrangers en France et permet notamment la gestion, par les préfectures, des dossiers de ressortissants étrangers, la fabrication des titres de séjour et la gestion des mesures d'éloignement.

Au regard de ces éléments, la Commission estime que le traitement AGDREF 2 relève des dispositions des articles 70-1 et suivants de la loi « Informatique et Libertés » ayant transposé la directive du 27 avril 2016 susvisée et que la présente modification relève desdites dispositions en ce qu'elle s'inscrit pleinement dans la prévention et la détection des infractions pénales.

Conformément à l'article L. 611-5 du CESEDA et à l'article 30-II de la loi du 6 janvier 1978 modifiée, les modifications apportées à ce traitement doivent faire l'objet d'un décret en Conseil d'Etat pris après avis de la CNIL. De manière générale, elle rappelle également qu'en application de l'article 70-4 de cette même loi, les traitements qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, doivent faire l'objet d'une analyse d'impact sur la protection des données à caractère personnel (« AIPD »). La Commission rappelle également que les traitements présentant un risque élevé ayant fait l'objet d'une formalité préalable avant le 25 mai 2018 ne sont toutefois pas immédiatement soumis à la réalisation d'une AIPD, à moins que les conditions de mise en œuvre de ces traitements aient fait postérieurement l'objet d'une ou plusieurs modifications substantielles.

A cet égard, elle relève qu'au regard de ses finalités et des données biométriques qu'il contient, le traitement AGDREF 2 est, par nature, susceptible d'engendrer des risques élevés pour les personnes concernées. Elle considère en revanche que la modification examinée (ajout d'une mise en relation avec le traitement DOCVERIF) n'est pas substantielle. La Commission estime en conséquence que la modification du traitement qui lui est soumise ne nécessite pas, à ce stade et compte tenu des circonstances de l'espèce, la réalisation d'une analyse d'impact dans le cadre de la présente saisine.

Sur la finalité et les fonctionnalités du traitement

L'article 1er du projet de décret prévoit que le traitement a pour finalité de proposer aux ressortissants français titulaires d'un passeport biométrique et aux ressortissants

étrangers titulaires d'un titre de séjour comportant un composant électronique de s'identifier et de s'authentifier auprès d'organismes publics ou privés, au moyen d'un téléphone mobile disposant d'un système d'exploitation « Android » et doté de la technologie sans contact.

La Commission relève que l'article 1er du projet de décret précité ne mentionne pas la création et la délivrance de l'identité numérique (ou moyen d'identification électronique) à partir de l'application mobile, alors même que celle-ci constitue l'une des finalités du traitement projeté et que c'est à partir de la création de l'identité numérique qu'un individu pourra s'identifier et s'authentifier pour accéder à des services en ligne. L'article 1er devrait dès lors être modifié afin de de faire état, au titre des finalités poursuivies, de la création d'une identité numérique.

En premier lieu, en ce qui concerne la création d'une identité numérique, la Commission relève que celle-ci est subordonnée à la création d'un compte sur l'application ALICEM. Elle précise que la création de ce compte nécessite la saisie, par la personne concernée, de son adresse électronique et de son numéro de téléphone mobile, lesquels sont vérifiés par l'envoi d'un lien unique d'activation sur l'adresse électronique et d'un mot de passe à usage unique par un court message au numéro de téléphone mobile.

L'article 2 du projet de décret précise à cet égard que « *le traitement mentionné à l'article 1er s'applique* » aux ressortissants français titulaires d'un passeport biométrique et aux ressortissants étrangers titulaires d'un titre de séjour comportant un composant électronique conformément à l'article R. 311-13-1 du CESEDA.

Les personnes concernées munies de leur titre - un passeport biométrique pour les ressortissants français et un titre de séjour étranger électronique pour les ressortissants étrangers - procèdent ensuite à la lecture optique des données de la bande « MRZ » du titre en la photographiant au moyen de leur équipement mobile.

La technologie sans contact doit permettre la lecture des données du titre enregistrées dans le composant électronique, à savoir les données d'état civil, de l'adresse et de la photographie de l'utilisateur. La Commission prend acte que l'image numérisée des empreintes digitales n'est pas lue par le dispositif et ne sera par conséquent pas utilisée ni enregistrée dans le traitement projeté.

Une interrogation du traitement DOCVERIF, qui fait l'objet d'une saisine distincte, est effectuée afin de confirmer la validité du titre d'identité. A cet égard, la Commission prend acte qu'un utilisateur disposant d'un titre invalide ne pourra pas procéder à la création d'une identité numérique.

Enfin, elle relève que l'accès à l'application ALICEM est sécurisé par un code de sécurité (« code PIN ») défini par l'utilisateur de l'application et qui lui sera demandé pour accéder à l'application et pour s'authentifier auprès de services en ligne concernés. La Commission prend acte qu'une fois le compte créé, son activation est subordonnée à un processus de vérification de l'identité alléguée afin de s'assurer que la personne ayant créé le compte correspond à celle détenant le titre. Elle relève que cette vérification prend la forme d'un traitement biométrique de reconnaissance faciale à partir d'une vidéo prise en temps réel par l'utilisateur qui doit réaliser une série de défis imposés par l'application (clignement des yeux, mouvement de la tête,

mouvement du visage, etc.). Cette vidéo est ensuite envoyée sur les serveurs de l'Agence nationale des titres sécurisés (« ANTS »). La Commission prend acte que ces défis sont utilisés pour vérifier qu'il s'agit bien d'une personne en possession du téléphone mobile (phase de reconnaissance faciale dite « dynamique »). Enfin, une photographie est extraite de la vidéo pour réaliser une comparaison avec le portrait extrait du titre (phase de reconnaissance faciale dite « statique »).

A la suite du déroulement satisfaisant de la phase d'activation, l'identité numérique est générée. L'accès au compte ALICEM pourra dès lors s'effectuer *via* l'application mobile ou le site web dédié à l'application.

En second lieu, la Commission relève qu'une fois créé et activé, les utilisateurs du dispositif pourront s'identifier et s'authentifier auprès de fournisseurs de services en ligne.

Elle relève ainsi que les personnes peuvent opter pour l'identité numérique ALICEM directement auprès des fournisseurs de services en ligne ou par l'intermédiaire du dispositif « FranceConnect », préalablement examiné par la Commission. Dans un premier temps, l'utilisateur ne pourra sélectionner l'identité numérique ALICEM pour accéder à un fournisseur de services que par l'intermédiaire de FranceConnect.

La Commission relève que l'identification et l'authentification à des services en ligne ne comportent pas par elles-mêmes de traitement de données biométriques, tant pour l'accès à un service nécessitant un niveau de sécurité « élevé » au sens du règlement e- IDAS susvisé que pour l'accès à un service nécessitant un niveau de sécurité « substantiel » ou « faible » au sens de ce même règlement.

La Commission prend acte qu'un audit RGAA (Référentiel général d'accessibilité de l'administration) a été mené en 2017.

Sous réserve de ce qui précède, la Commission estime que les finalités poursuivies par le traitement ALICEM sont déterminées, explicites et légitimes, conformément aux dispositions de l'article 5-1-b) du RGPD.

Sur le traitement de données biométriques

La Commission relève que le ministère entend faire application du consentement au titre de la base légale permettant la mise en œuvre du dispositif ALICEM.

Elle considère toutefois qu'il résulte de l'examen des conditions de mise en œuvre du dispositif projeté, telles qu'elles lui ont été présentées, qu'il convient d'opérer une distinction entre la création d'une identité numérique ALICEM et l'étape de vérification de l'identité alléguée par la personne pour activer le compte ALICEM, cette activation étant subordonnée au traitement de données biométriques.

A cet égard, la Commission estime que s'il est effectivement expressément consenti à la création d'une identité ALICEM, la mobilisation du consentement pour fonder le recours à la biométrie aux fins de vérifier l'exactitude de l'identité alléguée par la personne créant son identité numérique, et procéder ainsi à l'activation du compte ALICEM, soulève des interrogations.

La Commission rappelle en effet que l'article 9.1 du RGPD pose un principe d'interdiction du traitement de certaines catégories de données dites « sensibles », parmi lesquelles figurent les données biométriques. L'article 9.2 précise quant à lui que l'interdiction précitée peut être écartée dans certains cas, notamment lorsque (a) « *la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques* » ou (g) lorsque le traitement est « *nécessaire pour des motifs d'intérêt public importants* ».

En premier lieu, elle rappelle que pour être valable, le consentement dont il est question doit être libre, spécifique, éclairé et univoque conformément à l'article 4-11) du RGPD.

A ce titre, la Commission prend acte que dans le cadre du traitement projeté, les personnes sont invitées préalablement au processus de création de l'identité numérique à consentir ou non au traitement de leurs données biométriques. Elle prend également acte que le refus de procéder à de la reconnaissance faciale au stade de la procédure d'activation du compte ALICEM empêche la création de l'identité numérique ALICEM.

Compte tenu de ce qui précède, la Commission rappelle que le consentement n'est susceptible de constituer la base juridique du traitement de données biométriques que dans l'hypothèse où la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou encore de la possibilité de les refuser sans subir de préjudice.

A cet égard, la Commission considère, conformément à la position retenue par le groupe de travail de l'article 29 (« G29 ») et reprise par le Comité européen de la protection des données (CEPD) dans le cadre de ses lignes directrices sur le consentement que, dans l'hypothèse où la fourniture d'un service est subordonnée au consentement au traitement de données personnelles, ce consentement n'est libre que si le traitement de ces données est strictement nécessaire à la fourniture du service demandé par la personne, ou si une alternative est effectivement offerte par le responsable de traitement à la personne concernée.

En l'espèce, le refus du traitement des données biométriques fait obstacle à l'activation du compte, et prive de portée le consentement initial à la création du compte. Or, la nécessité de recourir à un dispositif biométrique pour vérifier l'identité d'une personne dans le but d'atteindre le niveau de garantie « élevé » de l'identité numérique, au sens du règlement e-IDAS, n'a pas été établie, compte tenu notamment de la possibilité de recourir à des dispositifs alternatifs de vérification (cf. infra).

Par ailleurs, la Commission relève que le ministère ne propose pas, en l'occurrence et à l'heure actuelle, d'alternative à la reconnaissance faciale pour créer une identité numérique de niveau « élevé » au sens du règlement e-IDAS. Il en résulte que la création d'une identité numérique ALICEM est subordonnée à un processus de reconnaissance faciale sans qu'aucune autre alternative équivalente ne soit prévue pour permettre la délivrance d'une identité numérique par cette application.

Au regard des principes rappelés ci-dessus, le consentement au traitement des données biométriques ne peut être regardé comme libre et comme étant par suite susceptible de lever l'interdiction posée par l'article 9.1 du RGPD.

En deuxième lieu, la Commission relève qu'en l'espèce, il n'a pas été soutenu ni démontré que le traitement projeté serait « *nécessaire pour des motifs d'intérêt public important* ». Elle estime en particulier que s'il ne peut d'emblée être exclu que ce traitement puisse s'inscrire dans le cadre de « *motifs d'intérêt public important* » en favorisant à l'initiative de l'Etat la sécurisation de l'identification électronique, la caractérisation d'un tel motif, tout comme l'appréciation de la nécessité mentionnée au (g) de l'article 9.2. supposeraient en tout état de cause de la part du ministère des éléments de démonstration complémentaires.

Dans ces conditions, elle considère que la mise en œuvre du traitement projeté doit être subordonnée au développement de solutions alternatives au recours à la biométrie, telle qu'utilisée pour vérifier l'exactitude de l'identité alléguée par la personne créant son compte, et ainsi s'assurer de la liberté effective du consentement des personnes concernées au traitement de leurs données biométriques au moment de l'activation de leur compte ALICEM. Ces solutions alternatives pourraient notamment prendre la forme d'un face à face (tel qu'un déplacement en préfecture, en maire, ou auprès d'un autre service public accueillant directement le public.), d'une vérification manuelle de la vidéo et de la photographie sur le titre (telle qu'un envoi de la vidéo au serveur de l'ANTS et vérification de l'identité opérée par un agent) ou d'un appel vidéo en direct avec un agent de l'ANTS.

La Commission estime par ailleurs que le développement de ces solutions alternatives est également de nature à permettre à un plus grand nombre de personnes d'utiliser le dispositif ALICEM et, en particulier, s'agissant de celles qui ne seraient pas en mesure de réaliser les différents défis proposés.

Sur les données traitées

L'article 7 du projet de décret énumère les catégories de données enregistrées dans le traitement projeté, à savoir : les données permettant l'identification de l'usager, les données permettant l'identification du titre détenu par l'usager, les données relatives à l'historique des transactions associées au compte ALICEM et l'identifiant unique du service de notification aux fins d'identification du téléphone mobile.

La Commission relève à cet égard que certaines données à caractère personnel sont enregistrées sur l'équipement mobile de l'utilisateur et d'autres sur le serveur central de l'ANTS. Ce partage permet notamment que seules les données d'identification soient conservées sur l'équipement mobile de l'utilisateur et donc sous son contrôle exclusif.

Au titre des données permettant l'identification de l'usager, seront enregistrées les données d'état civil (nom, le cas échéant nom d'usage, prénom, date et lieu de naissance, nationalité, sexe, taille et couleur des yeux et adresse postale) ainsi que la photographie de la personne. La Commission relève que ces données sont directement issues de la lecture sans contact du composant électronique du titre pendant la phase d'enrôlement. Elle estime que ces données, permettant de certifier l'identité du

titulaire d'un titre, sont pertinentes, adéquates et non excessives au regard de la finalité relative à la création de l'identité numérique de la personne concernée.

En outre, la Commission prend acte que l'image numérisée des empreintes digitales contenue dans le composant électronique du titre ne sera enregistrée ni dans l'application mobile, ni dans le serveur central de l'ANTS conformément aux articles 5 et 6 du projet de décret.

Par ailleurs, sont également collectées l'adresse électronique et le numéro de téléphone mobile de la personne. Ces données, permettant d'amorcer le processus de création du compte ALICEM, n'appellent pas d'observations particulières de la Commission.

La Commission relève également que les données biométriques relatives à la vidéo et à la photographie de l'utilisateur prises avec son équipement sont nécessaires au traitement biométrique de reconnaissance faciale. Elles sont donc adéquates, pertinentes et non excessives. Elle prend acte que ces données seront effacées dès la fin de la comparaison réalisée.

S'agissant des données relatives à l'historique des transactions, réalisées par l'intermédiaire de « FranceConnect » et enregistrées dans le traitement, la Commission rappelle que ce dispositif garantit un principe de séparation stricte entre le fournisseur d'identités et le fournisseur de services, de manière à ce que le fournisseur d'identité ignore quel fournisseur de services a utilisé l'identité.

La Commission prend acte que les données mentionnées du a) au d) du 3° de l'article 7 du projet de décret, qui correspondent aux données relatives à l'historique des transactions permettant de connaître le fournisseur de services, ne seront pas transmises et donc conservées dans le traitement lorsque les transactions seront réalisées par l'intermédiaire de « FranceConnect ».

Enfin, les données permettant l'identification du titre détenu par l'usager et l'identifiant unique du service de notification aux fins d'identification du téléphone mobile, n'appellent pas d'observations particulières de la Commission.

Sous réserve de ce qui précède, la Commission considère que les données sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées, conformément aux dispositions de l'article 5-1-c du RGPD.

Sur les durées de conservation

L'article 11 du projet de décret prévoit des durées de conservation différentes en fonction des données concernées.

Les données conservées sur l'équipement mobile de la personne concernée, c'est-à-dire les données relatives à l'identification et les données relatives à l'historique des transactions, sont supprimées lors de la désinstallation de l'application, ce qui n'appelle pas d'observation particulière.

L'article 11.II du projet de décret précise que les données enregistrées sur le serveur central sont conservées jusqu'à la désinstallation de l'application par l'usager ou bien

sept ans à compter de la dernière utilisation du compte ALICEM. Le ministère a indiqué sur ce point que cette durée de sept ans est conforme aux exigences de l'ANSSI en application du règlement e-IDAS.

Enfin, ledit article prévoit deux durées de conservation spécifiques en cas de non achèvement du processus de création et d'activation de l'identité numérique ALICEM (vingt-quatre heures en cas de non achèvement de la création du compte et sept jours en cas de non activation du compte), lesquelles n'appellent pas d'observation de la part de la Commission.

Sur les personnes habilitées et les destinataires

L'article 8 du projet de décret précise que les agents des services du ministère de l'intérieur chargés de la maîtrise d'ouvrage du traitement, ainsi que les agents de l'ANTS chargés de la maîtrise d'œuvre du traitement, individuellement désignés et dûment habilités par leur directeur, peuvent accéder à tout ou partie des données et informations enregistrées dans le traitement, à raison de leurs attributions et dans la limite du besoin d'en connaître.

Si l'accès de ces personnes aux données semble justifié par la mise en œuvre opérationnelle du dispositif ALICEM, la Commission rappelle que les données d'identification mentionnées à l'article 7 1° du projet de décret sont exclusivement conservées sur l'équipement mobile, auxquelles ne peuvent pas, par principe, accéder les personnes précédemment citées. Elle estime dès lors que le projet de décret devrait être modifié afin d'exclure de manière explicite l'accès aux données contenues dans l'équipement mobile de l'usager. La Commission prend acte de la modification du projet de décret en ce sens.

S'agissant des destinataires, l'article 9 du projet de décret prévoit que « FranceConnect », « *les fournisseurs de téléservices liés par convention à FranceConnect* » et « *les fournisseurs de téléservices liés par convention à l'ANTS* » pourront être destinataires des données. La Commission relève que le dispositif « FranceConnect » n'est pas un destinataire à proprement parler mais un traitement permettant l'intermédiation entre ALICEM et le fournisseur de services concerné : en transmettant les éléments d'identification nécessaires au fournisseur de services, il garantit l'identification et l'authentification de l'usager. Elle considère que le projet de décret devrait être clarifié sur ce point. A cet égard, elle prend acte de la modification à venir, à savoir la mention de la « Direction interministérielle du numérique et du système d'information et de communication de l'Etat » (DINSIC) en lieu et place de « FranceConnect ».

L'article 9 II du projet de décret liste les données transmises par ALICEM aux destinataires. La Commission rappelle sur ce point que chacun des destinataires ne peut recevoir que les données strictement nécessaires pour permettre la vérification de l'identité ou des attributs d'identité exigés pour accéder au service concerné, et non pas l'intégralité des données énumérées audit article. Elle estime dès lors que le projet de décret devrait être complété en ce sens.

Sur l'information et les droits des personnes concernées

L'article 13 du projet de décret prévoit qu'une « *information de l'usager concernant l'utilisation d'un dispositif de reconnaissance faciale statique et de reconnaissance faciale dynamique* » sera délivrée à la personne concernée au moment de l'ouverture du compte.

La Commission relève que la personne concernée est informée par la mise à disposition de conditions générales d'utilisation de l'application et que celles-ci doivent être expressément validées pour procéder à la création du compte. La personne concernée est également informée du traitement de ses données à chaque demande d'identification et d'authentification auprès d'un fournisseur de services.

La Commission relève par ailleurs que le contenu de l'information n'a pas été porté à sa connaissance de manière précise et que le projet de décret se limite à une information sur l'usage de la reconnaissance faciale. Elle attire dès lors l'attention du ministère sur l'importance de délivrer une information « *de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* », conformément à l'article 12 du RGPD.

En outre, le ministère a indiqué la mise en place d'une information spécifique concernant le consentement au traitement de données biométriques, ce dont la Commission prend acte.

L'article 14 du projet de décret prévoit que les droits d'accès, de rectification, de limitation et d'effacement s'exercent auprès de l'ANTS, ce qui n'appelle pas d'observations particulières de la Commission.

La Commission relève enfin qu'il est prévu un mécanisme visant à la portabilité des données pour les personnes concernées. Elle s'interroge néanmoins sur l'effectivité de celui-ci en cas de renouvellement d'un titre. En effet, le renouvellement du titre implique la perte des traces relatives à l'ancien titre et ce, sans possibilité pour l'usager de les récupérer. Dans ce contexte, la Commission invite le ministère à envisager une solution afin de permettre à l'usager de récupérer ses données dans ce cas de figure. Elle prend acte de l'engagement du ministère de mener une réflexion sur ce point, laquelle pourrait être utilement portée à sa connaissance.

Sur les mesures de sécurité

En tant que moyen d'identification et d'authentification de niveau élevé, l'impact d'incidents de sécurité sur les personnes concernées peut être particulièrement grave. Dans ce contexte précis, la Commission constate que le responsable de traitement met en œuvre un ensemble de mesures permettant de réduire la vraisemblance de tels incidents.

La Commission relève que les données stockées par l'application, à l'exception des données de préférences (notamment issues d'un paramétrage par l'utilisateur), sont chiffrées avec des algorithmes et des procédures de gestion de clés conformes à l'annexe B1 du référentiel général de sécurité. De plus, les échanges de données entre l'application et les serveurs de l'ANTS sont réalisés via des canaux de communication

chiffrés et assurant à la fois l'intégrité des données et l'authentification de la source et du destinataire.

Par ailleurs, des profils d'habilitation sont prévus afin de gérer l'administration du système tout en respectant le principe d'accès aux données en tant que de besoin, ce qui n'appelle pas d'observation particulière.

La Commission relève que le responsable de traitement met en œuvre une politique de mot de passe, pour les utilisateurs ainsi que pour les administrateurs, conforme à la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe modifiée par la délibération n° 2017-190 du 22 juin 2017, et ce notamment en ce qui concerne le stockage des mots de passe. En outre, les accès administrateurs au système sont mis en œuvre de façon conforme au référentiel de sécurité du ministère sur les accès à distance.

L'article 12 du projet d'arrêté prévoit que les informations relatives aux opérations de création, consultation, mise à jour et suppression des données sont conservées pendant sept ans à compter de leur enregistrement. La Commission note que deux types d'informations sont conservés au titre des traces : d'une part, les données relatives aux transactions effectuées par l'utilisateur et, d'autre part, celles relatives à l'enrôlement.

Concernant les données conservées pour démontrer le bon enrôlement de l'utilisateur (SOD), la Commission considère que la durée prévue de sept ans est une exigence de sécurité formulée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui n'appelle pas d'observation de sa part. En revanche, la Commission estime que conserver les traces des accès à l'applicatif ALICEM, ainsi que l'historique des transactions effectuées pour cette même durée, est manifestement disproportionné. Elle recommande dès lors une conservation de ces données pour une durée maximale de six mois.

La Commission relève que pour limiter les risques liés aux logiciels malveillants, le ministère a choisi de limiter l'installation de l'application aux équipements mobiles ne mettant pas les privilèges d'administrateur à la disposition des usagers, excluant ainsi les équipements dits « rootés ».

La Commission s'interroge néanmoins sur la nécessité d'une telle restriction, le choix des usagers de disposer des droits d'administrateur sur leur équipement pouvant également être motivé par le besoin d'en accroître la sécurité. A cet égard, le ministère a indiqué que si pour une minorité d'utilisateurs disposer d'un équipement « rooté » peut accroître la sécurité, pour la majorité des utilisateurs disposer d'un tel équipement peut constituer un risque supplémentaire en matière de sécurité, ce dont la Commission prend acte.

La Commission constate que pour limiter la vraisemblance d'une usurpation d'identité par falsification de l'enrôlement, le dispositif met en œuvre différentes garanties, parmi lesquelles l'analyse du flux vidéo ou des défis aléatoires de reconnaissance faciale dynamique.

Enfin, la Commission relève que l'obtention d'une qualification du dispositif ALICEM au regard du règlement e-IDAS est en cours d'évaluation par l'ANSSI.

Sous réserve des précédentes observations, les mesures de sécurité décrites par le responsable de traitement sont conformes à l'exigence de sécurité prévue par les articles 5.1.f et 32 du RGPD.

La Commission rappelle toutefois que cette obligation nécessite la mise à jour de l'AIPD et de ses mesures de sécurité, pour prendre en compte la réévaluation régulière des risques.

La Présidente

I. FALQUE-PIERROTIN