N° 432656 – La Quadrature du Net

10ème et 9ème chambres réunies

Séance du 9 octobre 2020
Lecture du 4 novembre 2020

CONCLUSIONS

M. Alexandre Lallet, rapporteur public

L'identification électronique repose sur un double processus :

- d'une part, **l'établissement et la remise des moyens d'identification électronique à la personne, après vérification de son identité physique** – c'est l'équivalent de la fabrication et de la délivrance de sa pièce d'identité physique[1] ;

- d'autre part, **l'authentification de la personne** lors des opérations et transactions nécessitant son identification[2] : c'est l'équivalent de la présentation et de la vérification de sa pièce d'identité lors d'une démarche physique. Cette opération repose sur l'utilisation des « facteurs d'authentification » définis lors de la première étape, lesquels facteurs peuvent relever de trois catégories différentes : la possession (« j'ai »), c'est le fait de détenir un objet auquel est rattachée l'identification électronique et qui est nécessaire pour accéder au service, comme une carte ou un smartphone -, la connaissance (« je sais »), c'est le fait de connaître un mot de passe ou une information confidentielle, et, enfin, le facteur « inhérent » (« je suis »), qui est basé sur un attribut physique de la personne, comme une empreinte digitale ou les caractéristiques de son visage.

Selon le degré de sécurisation de ces opérations et les garanties qu'elles offrent en termes de réduction ou de suppression du risque d'utilisation abusive ou d'altération de l'identité, un schéma d'identification électronique est éligible à l'un des trois niveaux de garantie prévus

[1] Cette phase est parfois dénommée « enrôlement ».
[2] Selon le point 5 de l'article 3 du règlement eIdas, l'authentification est le « *processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* ».

par le règlement dit e-Idas du 23 juillet 2014[3] : niveau faible, niveau substantiel ou niveau élevé.

Jusqu'à récemment, l'accès aux **téléprocédures administratives** reposait exclusivement sur une identification présentant tout au plus un niveau de garantie faible, consistant, premièrement, à créer ou à se voir attribuer un identifiant – par exemple, son adresse mail, son numéro fiscal ou son numéro de sécurité sociale ; deuxièmement, à créer un mot de passe associé ; et, troisièmement à utiliser ces deux informations pour s'authentifier sur un site de service public. C'est sur ce principe, ainsi que sur une logique de reconnaissance mutuelle, que repose le dispositif *France Connect*, qui vous permet de réaliser de nombreuses démarches en ligne à l'aide de l'identité numérique dont vous disposez auprès du service des impôts, de la sécurité sociale ou encore de La Poste.

Le ministère de l'intérieur et l'agence nationale des titres sécurisés (ANTS) ont souhaité franchir un cap dans la sécurisation en proposant une application pour smartphone, baptisée ALICEM – pour « Authentification en ligne certifiée sur mobile », permettant d'accéder aux mêmes démarches que par le portail *France Connect*, mais en offrant un niveau de garantie supérieur. La procédure de certification d'ALICEM au niveau de garantie élevé au sens du règlement eIDAS est d'ailleurs en cours auprès de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Au stade de la création du compte ALICEM, c'est-à-dire de l'établissement et de la **délivrance des moyens d'identification électronique**, plusieurs garde-fous sont prévus : l'utilisateur doit saisir un code envoyé par SMS sur son mobile, valider un lien figurant dans un mail, scanner la bande MRZ de son passeport ou de son titre de séjour biométrique, lire sans contact la puce du titre et, enfin – on en arrive à ce qui fait la spécificité de l'application et l'origine du litige – valider un **test de reconnaissance faciale**. Ce dernier consiste à enregistrer une vidéo dans laquelle la personne accomplit des mouvements prédéfinis, appelés « défis » – sourire, tourner la tête, cligner des yeux… - et à envoyer cette vidéo sur les serveurs de l'ANTS pour que celle-ci vérifie, via un algorithme de **reconnaissance faciale**, que l'utilisateur du service est bien le détenteur légitime du titre biométrique, auquel s'ajoute un algorithme de **reconnaissance du vivant**, destiné à vérifier que l'utilisateur n'est pas un robot. Les données biométriques utilisées sont immédiatement détruites après utilisation.

[3] Règlement n° 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, précisé par le règlement d'exécution n° 2015/1502 de la Commission du 8 septembre 2015.

Une fois le compte créé, l'utilisateur peut accéder aux téléprocédures administratives via son smartphone en utilisant le code de sécurité qu'il a choisi au cours de la procédure et, dans certains cas, en recourant à une lecture sans contact de la puce du titre biométrique. La phase d'authentification de l'utilisateur, c'est-à-dire l'utilisation courante d'ALICEM, ne fait donc appel à aucun dispositif de reconnaissance faciale.

Le traitement de données à caractère personnel correspondant a été autorisé par le décret n° 2019-452 du 13 mai 2019 dont l'association La Quadrature du Net, que vous connaissez bien, vous demande l'annulation.

La version du décret ne diffère du projet initial du Gouvernement et de celui du Conseil d'Etat qu'en ce qu'elle corrige une erreur de plume relative à l'intitulé du texte dans deux articles. Une telle modification, qui ne modifie ni la portée, ni l'économie générale du texte, n'entache pas la **procédure de consultation du Conseil d'Etat** d'irrégularité (CE, 30 décembre 2009, *Association SOS Racisme*, n° 312051).

En outre, le garde des sceaux, le ministre de la cohésion des territoires et le ministre des outre-mer n'étant appelés à prendre aucune mesure d'exécution du décret, leur **contreseing** n'était pas requis.

Les deux premiers moyens de légalité interne mettent en cause la licéité du traitement en raison de l'utilisation de la reconnaissance faciale dans les conditions que nous avons décrites et qui a suscité un certain émoi médiatique.

L'article 9 du RGPD interdit les traitements utilisant des données biométriques aux fins d'identifier une personne physique de manière unique, mais assortit cette interdiction d'une série d'exceptions, dont, au a) de son 2., le **consentement explicite** de la personne concernée et, au g. du même point 2, la nécessité de ce traitement au regard de **motifs d'intérêt public important**.

Il ressort tant des visas et de l'article 13 du décret attaqué que du fonctionnement concret de l'application, qui subordonne la création du compte à l'acceptation non seulement des conditions générales d'utilisation mais aussi, de manière distincte, à celle du traitement de reconnaissance faciale, que l'administration a entendu fonder ce traitement sur le **consentement explicite**. Ses écritures en défense le confirment. Par suite, il ne peut être utilement soutenu que le traitement litigieux ne serait pas nécessaire pour des motifs d'intérêt public important.

Il reste – c'est le deuxième moyen - à déterminer si le consentement peut valablement constituer la base légale de ce traitement. L'association requérante le conteste vigoureusement au motif que **ce consentement ne serait pas libre**, et ne répondrait donc pas aux exigences posées par le 11) de l'article 4 du RGPD. Elle convoque un allié de poids dans sa démarche : la CNIL, qui, tant dans l'avis qu'elle a rendu sur le projet de décret que dans ses observations devant vous, considère que les modalités de recueil du consentement ne garantissent pas son caractère libre. Son argumentation est la suivante : l'utilisateur ne peut pas s'inscrire sur ALICEM ni, par conséquent, utiliser ce service sans se prêter à l'opération de reconnaissance faciale que nous avons décrite, alors même que le recours à cette technologie n'est pas indispensable pour que le schéma d'identification électronique correspondant soit éligible au niveau de garantie élevé.

Nous retrouvons ici un débat récurrent et toujours délicat sur la réalité du libre consentement.

Rappelons les règles pertinentes, qui sont les mêmes que celles auxquelles nous avions récemment confronté le dispositif des « *cookie walls* » :

- d'une part, le considérant 42 du RGPD, qui explicite la notion de consentement libre, prévoit 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* » ;

- d'autre part, il résulte du paragraphe 4 de l'article 7 du RGPD que, « *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.* ». Le considérant 43 présume en pareil cas l'absence de consentement libre[4].

Il est nécessaire de bien cerner les conséquences qui s'attachent au refus de donner son consentement au traitement de reconnaissance faciale mis en œuvre dans le cadre de l'application ALICEM.

[4] Ce considérant 43 exclut en outre le fondement du consentement « *lorsqu'il existe un déséquilibre manifeste entre la personne concernée et le responsable du traitement, en particulier lorsque le responsable du traitement est une autorité publique et qu'il est improbable que le consentement ait été donné librement au vu de toutes les circonstances de cette situation particulière* »

La conséquence immédiate est de **se priver de l'application**, puisqu'il est impossible de créer un compte sans passer par l'étape de « reconnaissance faciale ». On en est donc ramené à l'analyse des implications, pour un citoyen, de l'impossibilité d'utiliser le service ALICEM.

A la date du décret attaqué, qui est la date pertinente s'agissant d'un recours direct contre ce dernier, cette application ne permettait pas d'accéder à une téléprocédure administrative qui n'était pas accessible par d'autres moyens en ligne, en particulier par *France Connect*. C'est toujours le cas d'ailleurs. L'offre de services accessible via ALICEM n'est pas plus riche non plus que celle qui est disponible dans le monde physique, puisque, comme vous l'avez jugé dans votre décision *La Cimade et autres* du 27 novembre 2019 (n° 422516, aux T.), aucune disposition, notamment les articles L. 112-8 à L. 112-10 du code des relations entre le public et l'administration, ne fait obligation aux citoyens de saisir l'administration par voie électronique et, notamment, d'utiliser un téléservice mis en place par l'administration, sauf disposition législative contraire[5]. **Le refus de consentir au traitement de reconnaissance faciale litigieux n'emporte donc aucune conséquence négative quant à la <u>nature des services accessibles</u>**.

Il est vrai, en revanche, qu'il n'est pas sans inconvénient en termes de **sécurité des usages**. *France Connect* comme les autres processus d'authentification mis en place par l'administration repose sur un **unique facteur d'authentification** basé sur la connaissance de l'identifiant et du mot de passe – ce qui correspond tout au plus à un schéma d'identification électronique présentant un niveau de garantie **faible** au sens du règlement e-IDAS. A l'inverse, l'application ALICEM repose sur l'utilisation de **deux facteurs d'authentification** relevant de deux catégories différentes : d'une part, le code de sécurité, facteur basé sur la connaissance ; d'autre part, la détention du smartphone auquel est rattaché le numéro de téléphone – facteur basé sur la possession, voire, dans certains cas, la détention du titre biométrique lui-même, dont la puce est lue sans contact. C'est l'une des conditions de la reconnaissance par l'ANSSI du niveau de garantie élevé[6].

Il s'ensuit que l'unique conséquence du refus de donner son consentement au traitement litigieux est **l'impossibilité d'utiliser les téléprocédures administratives éligibles avec un niveau de protection renforcé contre l'usurpation d'identité**, ce qui implique **soit de renoncer à ce niveau de protection, soit de renoncer à une démarche en ligne au profit d'une démarche physique**.

---

[5] C'est le cas, par exemple, de la déclaration des revenus soumis à l'impôt sur le revenu, sauf exceptions (art. 1649 quater B quinquies).

[6] V. le point 2.2.1. du règlement d'exécution du 8 septembre 2015.

Nous ne pensons pas qu'on puisse qualifier cette seule conséquence de « **préjudice** » au sens du RGPD, comme le soutient l'association requérante. Les lignes directrices du CEPD sur le consentement qualifient de préjudice le fait de ne pas pouvoir accéder au service ou seulement à une version dégradée, mais exclut cette qualification en cas de perte d'un « incitant » ou d'un « avantage ». On peut considérer que la double authentification offerte par ALICEM constitue tout au plus un avantage – celui de réduire considérablement le risque d'usurpation d'identité dans l'accès à un téléservice – qui est d'ailleurs contrebalancé par un inconvénient en termes d'**expérience utilisateur**, puisqu'ALICEM ne peut être utilisé que sur smartphone, et même sur l'équipement déclaré dans le compte. L'immense majorité des citoyens qui utilisent aujourd'hui des téléservices se satisfont d'un niveau de garantie faible, sans qu'on puisse les qualifier de victimes d'un préjudice. Il faut aussi observer que des garde-fous existent contre l'usurpation d'identité, de l'exigence de comparution personnelle pour certaines démarches administratives énumérées dans les décrets du 5 novembre 2015, comme l'obtention d'une carte nationale d'identité, au délit d'usurpation d'identité numérique[7].

La CNIL se place sur un autre terrain[8] puisqu'elle soutient que le recueil des données biométriques ne pourrait pas être considéré comme « **nécessaire à la fourniture du service** » au sens de l'article 7 du RGPD, dès lors qu'il serait possible de proposer le « même service » sans recourir à un outil automatisé de reconnaissance faciale. Il faut, pour cela, qu'au moment de la création du compte, l'identité de la personne soit **vérifiée en face-à-face par un agent public**, au guichet, par l'envoi d'une vidéo ou via une application de visioconférence par exemple. Vous noterez qu'en vérité, cette modalité de vérification d'identité utilise aussi des données biométriques. La seule différence est que, dans les formules alternatives mentionnées par l'association requérante et la CNIL, le réseau de neurones utilisé pour les exploiter est **humain** – un agent en chair et en os qui compare la personne qu'elle a en face d'elle avec celle du titre biométrique - alors qu'il est **artificiel** dans le cas d'ALICEM, via les algorithmes de reconnaissance faciale et de reconnaissance du vivant.

La question qui vous est posée est substantiellement différente de celle des *cookie walls*, pour lesquels les données sont en général collectées à des fins de ciblage publicitaire, de sorte qu'elles ne sont absolument pas nécessaires à la fourniture du service auquel l'utilisateur souhaite accéder[9]. Ici, la collecte et l'exploitation des données biométriques servent bien à la

[7] Art. 226-4-1 : un an d'emprisonnement et 15 000 euros d'amende.

[8] Elle n'évoque pas non plus le terrain du **déséquilibre manifeste entre le citoyen et l'administration**, ce qui serait vain. Rien n'oblige le premier à créer un compte ALICEM et, au-delà de la perte de l'avantage que nous venons d'indiquer, son refus ne se traduit par aucune forme de sanction ou de représailles de la part de la seconde. Il n'est pas raisonnablement possible d'affirmer, au moins de manière générale, qu'il est « improbable » que les utilisateurs d'ALICEM aient donné librement leur consentement en raison d'une forme de soumission ou de dépendance à l'égard du responsable de traitement public.

délivrance du moyen d'identification électronique dans des conditions de sécurité renforcées, même si ces données ne sont plus utilisées par la suite, lors de l'utilisation de l'application. En revanche, il est vrai qu'on peut faire l'économie de ce traitement de données, tout en proposant les mêmes fonctionnalités d'authentification, en recourant aux modalités alternatives suggérées par la CNIL.

Cette seconde acception de la condition de « nécessité », qui consiste à intégrer dans la réflexion l'ensemble des alternatives organisationnelles possibles, nous paraît toutefois excéder les prévisions du RGPD. Nous pensons en effet que **le caractère « nécessaire à la fourniture du service », au sens du règlement, doit s'apprécier au regard des caractéristiques de ce service telles qu'elles sont définies par le responsable de traitement**, et non telles qu'elles pourraient être dans l'idéal. Autrement dit, il n'y a pas lieu d'inclure dans le test de nécessité la possibilité dont ce responsable disposerait de modifier le contenu ou les modalités de fourniture de son service ou son organisation interne, en recrutant ou en exploitant un réseau de guichets physiques par exemple, pour éviter de recourir à tel ou tel traitement automatisé, biométrique ou non d'ailleurs[10].

Un traitement de données à caractère personnel doit à notre avis être regardé comme non nécessaire à la fourniture d'un service lorsque sa suppression sèche serait sans incidence directe et substantielle sur le principe, le contenu et la qualité du service fourni, ce qui révèle qu'il lui a été artificiellement adjoint et qu'il en est, d'une certaine manière, un passager clandestin. L'enjeu est alors de définir les contours exacts du service proposé et de faire pièce au subterfuge consistant à prétendre que le traitement litigieux en fait partie intégrante. Les lignes directrices du CEPD relatives au consentement exigent un « *lien*

---

[9] Si ce n'est, au plan « macro », à travers son financement - puisque c'est souvent ainsi que l'éditeur du site se rémunère.

[10] Il faut bien voir à cet égard que **le raisonnement de l'association requérante et de la CNIL n'a, juridiquement, rien de spécifique aux données biométriques** ; l'exigence d'un libre consentement vaut pour l'ensemble des traitements de données à caractère personnel qui ne reposent pas sur une autre base légale. La seule exigence supplémentaire propre aux « catégories particulières de données » évoquées à l'article 9, dites « données sensibles », est celle d'un consentement « explicite », notion difficile à cerner mais dont on croit comprendre qu'elle se rapporte à la spécificité et la granularité du consentement, qui devrait être recueilli de manière autonome pour ces données, ou à tout le moins au degré d'exigence dans la clarté et la qualité de l'information délivrée à la personne concernée avant qu'elle donne son consentement, afin de ne laisser planer aucun doute sur ses intentions.

[10] Dans son avis 06/2014, le G29 donnait l'exemple d'un profilage des goûts et du mode de vie de l'utilisateur à partir de son historique de navigation sur un site internet de vente de produits et services. Il considérait que le responsable du traitement des données n'avait pas été chargé, dans le contrat, d'établir un profil mais de fournir des produits et des services, et estimait ainsi que « *même si ces activités de traitement sont expressément mentionnées en petits caractères dans le contrat, elles n'en deviennent pas pour autant « nécessaires » à l'exécution de ce dernier* ».

direct et objectif entre le traitement des données et l'objectif d'exécution du contrat ». Dans son avis 06/2014 du 9 avril 2014 sur la notion d'intérêt légitime (WP 217), auquel ces lignes directrices renvoient, le G29 prescrivait plus précisément de « *déterminer la raison d'être exacte du contrat, c'est-à-dire sa substance et son objectif fondamental, car c'est ce qui permettra de vérifier si le traitement des données est nécessaire à l'exécution du contrat* »[11]. Il ne suffit pas, en effet, de proclamer qu'un service de vidéos en ligne inclut du ciblage publicitaire pour que le recueil de données personnelles nécessaires à ce ciblage, mais superflu pour fournir les vidéos, repose sur un consentement libre. Il s'agit en réalité de deux services totalement distincts, ayant chacun leur finalité propre, dont le couplage du consentement est potentiellement prohibé[12].

En l'occurrence, ALICEM propose un seul et unique service. Il existe un lien direct et objectif entre le test de reconnaissance faciale et l'objectif du service, qui est de proposer un accès à des téléprocédures avec un niveau de garantie élevé ou, au moins, renforcé. Et il est évident que l'Etat ne se sert pas de l'effet d'attraction de ce service pour imposer au citoyen son process de reconnaissance faciale, alors surtout que, comme on l'a dit, il n'exploite pas les données biométriques collectées à d'autres fins ni ne les conserve après la vérification. Au fond, il ne nous paraît pas exact de dire, comme le font l'association et la CNIL, que le « même service » pourrait être fourni par l'Etat sans recourir au traitement litigieux. Exiger de lui qu'il mette en place, pour la validation du compte, une solution guichet ou des modalités alternatives de vérification à distance impliquant une intervention humaine et, le cas échéant, des recrutements, c'est, en réalité, lui demander de mettre en place un **autre service**, ce que la seule exigence d'un consentement libre au sens du RGPD ne peut pas raisonnablement impliquer.

Cette analyse n'est pas contredite par les lignes directrices du CEPD sur le consentement, dont se prévaut la Quadrature du Net, en ce qu'elles admettent que le consentement reste libre lorsque le même responsable de traitement propose, à côté du service impliquant un traitement de données non nécessaire à sa fourniture, un service réellement équivalent ne recourant pas au traitement litigieux[13]. On voit qu'il ne s'agit pas alors de distinguer les traitements nécessaires à la fourniture du service et ceux qui ne le sont pas mais, en aval du

[11] Dans son avis 06/2014, le G29 donnait l'exemple d'un profilage des goûts et du mode de vie de l'utilisateur à partir de son historique de navigation sur un site internet de vente de produits et services. Il considérait que le responsable du traitement des données n'avait pas été chargé, dans le contrat, d'établir un profil mais de fournir des produits et des services, et estimait ainsi que « *même si ces activités de traitement sont expressément mentionnées en petits caractères dans le contrat, elles n'en deviennent pas pour autant « nécessaires » à l'exécution de ce dernier* ».

[12] Où l'on constate, au passage, que, décidément, la question de la granularité est absolument clé dans la problématique du consentement sous l'empire du RGPD…

[13] Guidelines 05/2020 on consent under Regulation 2016/679, V. 1.1, 4 mai 2020, pt. 37, p. 11.

test de nécessité et lorsqu'il est constaté que le traitement n'est pas nécessaire, d'apprécier si le responsable de traitement peut malgré tout être regardé comme offrant un libre choix à la personne concernée à travers un service équivalent, expurgé de ce traitement. Ces considérations ne nous paraissent pas pertinentes ici dès lors que la nécessité du traitement nous paraît avérée[14].

En définitive, les questionnements soulevés par ALICEM dans sa configuration actuelle portent moins, à notre avis, sur la liberté du consentement que sur la **fiabilité de la technologie de reconnaissance faciale**, au regard des performances comparées de l'intelligence humaine et de l'intelligence artificielle dans cet exercice[15] et sur les risques d'exclusion numérique liés à un développement des téléprocédures et une réduction corollaire des possibilités de démarches physiques, comme le relève le rapport de la mission d'information commune de l'Assemblée nationale sur l'identité numérique du 8 juillet dernier. Il n'est d'ailleurs pas exclu, selon la presse spécialisée, qu'ALICEM soit finalement abandonnée dans le cadre du projet de carte d'identité électronique[16].

Nous vous proposons donc d'écarter ce moyen.

---

[14] Ajoutons de surcroît que, à supposer même qu'on considère que le traitement de reconnaissance faciale en litige n'est pas strictement nécessaire à la fourniture du service ALICEM dans les mêmes conditions de sécurité, il n'en résulterait pas pour autant une contrariété automatique au RGPD. Comme nous vous l'avions exposé dans les conclusions que nous avons prononcées dans l'affaire Association des agences-conseils en communication et autres (n° 434684, aux T.), le point 4 de l'article 7 du RGPD ne conduit pas à interdire de manière générale et absolue le recueil du consentement pour la collecte et l'utilisation de données qui ne sont pas nécessaires à la fourniture d'un service, mais appelle une analyse au cas par cas de la réalité de la liberté de choix dont dispose telle ou telle personne, avec un a priori défavorable, qui fait écho à la vigilance dont doit faire preuve le responsable de traitement lorsqu'il recourt à un tel procédé. La décision n° 434684 nous permet entériner ce point de vue, implicitement mais nécessairement– nous dirions, diplomatiquement puisqu'elle fonde l'annulation des lignes directrices de la CNIL, en tant qu'elles interdisaient les *cookie walls*, sur la circonstance que l'autorité a excédé les limites de son pouvoir dans le maniement du droit souple. Mais si les chambres réunies avaient été convaincues que le RGPD prohibe les cookie walls, parce que le consentement ne peut pas être libre en pareil cas, il n'aurait pas été possible de retenir ce terrain de censure, pas plus qu'il n'est possible de reprocher à une administration d'avoir réitéré une norme supérieure (elle-même légale) dans une circulaire. En l'espèce, compte tenu de la nature de l'application et de la possibilité d'accéder aux mêmes téléprocédures sans elle, fût-ce avec un niveau de sécurité moindre, il ne nous paraît pas possible de se fonder sur une telle règle pour annuler le décret.

[15] Compte tenu notamment des biais qui affectent cette dernière. Il faut observer qu'il n'est pas exclu que, dans la procédure de vérification humaine envisagée par la CNIL, l'agent fasse lui-même appel à un outil informatique de reconnaissance faciale. Mais on peine alors à identifier la garantie que cette intervention apporterait au regard de la protection de la vie privée. De ce point de vue, nous préférons qu'aucun être humain, fût-il un agent public dont la probité n'est plus à démontrer, ne sache que nous avons créé un compte ALICEM…

[16] V. par exemple : https://www.nextinpact.com/article/30397/109159-identite-numerique-alicem-cest-fini-bienvenue-a-cnie

Vous pourrez faire de même, plus rapidement, du dernier moyen. Nous ne voyons pas, en effet, parmi les 32 catégories de données énumérées à l'article 7 du décret attaqué, celles qui ne seraient pas adéquates ou pertinentes, ou qui seraient manifestement excessives. Il s'agit de données d'identification de l'usager, de données permettant l'identification du titre biométrique, de celles qui ont trait à l'historique des transactions associées au compte et d'un identifiant unique permettant d'identifier le téléphone mobile. L'association ne vous explique pas clairement en quoi telle ou telle donnée serait superflue, dénonçant essentiellement le caractère massif de la collecte de données. La CNIL n'a émis aucune objection de principe sur ce point dans son avis.

Nous vous invitons donc à rejeter la requête, sans qu'il soit besoin de poser les questions préjudicielles suggérées à la Cour de justice de l'Union européenne.