Délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile »

(demande d'avis n° 21015556)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministère de l'intérieur d'une demande d'avis concernant un projet de décret en Conseil d'Etat autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » ;

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 (règlement général sur la protection des données) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 8-I-4°-a) ;

Après avoir entendu le rapport de M. Claude CASTELLUCCIA, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Emet l'avis suivant :

1. La Commission nationale de l'informatique et des libertés (ci-après « la Commission ») a été saisie, le 27 aout 2021 par le ministère de l'intérieur, d'une demande d'avis relative à un projet de décret en Conseil d'Etat autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (ci-après « SGIN ») et abrogeant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile » (ci-après « ALICEM »).

2. Le présent projet de décret crée un traitement de données à caractère personnel dénommé « SGIN » dont le responsable de traitement est le ministère de l'intérieur. Ce traitement permettrait aux titulaires d'une carte nationale d'identité électronique (ci-après « CNIe »), disponible sur le territoire national depuis le 2 août 2021, de bénéficier d'un moyen d'identification électronique.

3. Comme défini à l'article L. 102 du code des postes et des communications électroniques, un moyen d'identification électronique est un élément matériel ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne.

4. Le moyen d'identification électronique prévu par le présent projet de décret permettrait aux usagers de s'identifier et de s'authentifier auprès d'organismes publics ou privés, en utilisant un téléphone portable doté d'un dispositif permettant la lecture sans contact du composant électronique de la CNIe et d'une application mobile spécifique.-

5. La création et l'utilisation du « SGIN » seraient facultatives pour l'usager, et seraient conditionnées à la détention d'une CNIe et d'un téléphone portable disposant de la technologie de lecture sans contact et compatible avec l'application mobile. Cependant, il s'agira du seul dispositif, pour les prochaines années, accessible à tous les citoyens fournissant une identité numérique de niveau élevé. Dans ce contexte, la Commission souligne l'importance de s'assurer que le dispositif soit le plus simple d'utilisation pour tous les publics, y compris ceux les moins rompus au numérique.

6. Si la Commission estime que ce moyen d'identification électronique permet aux citoyens de bénéficier des avantages offerts par un service d'identité numérique, elle souligne que le caractère facultatif de la création et de l'utilisation de ce moyen d'identification électronique doit être garanti par principe. En effet, ce moyen d'identification électronique ne saurait être imposé pour accéder aux services en ligne, publics comme privés, qui devront donc offrir d'autres modalités d'accès aux services concernés, d'une part par d'autres moyens d'identification électronique et, d'autre part, par un guichet physique afin d'assurer un égal accès au service public à tous les citoyens.

7. Par ailleurs, il convient de préciser que si le présent projet de décret abroge le décret n° 2019-452 mettant en place le traitement « ALICEM », ce dernier utilisait un enrôlement à distance basé sur de la reconnaissance faciale alors que le dispositif « SGIN » présenté utilise le processus d'identification et d'enrôlement mis en œuvre pour la création de la carte nationale d'identité sans étape ou données biométriques supplémentaires. Ainsi, il bénéficie des mesures mises en place pour celles-ci, et donc du contrôle visuel de l'identité du demandeur par un agent de l'Etat sur la base des documents fournis pour la demande, ainsi qu'une comparaison d'empreintes entre le demandeur et les données inclues dans son titre biométrique.

8. A cet égard, il convient de rappeler que si la reconnaissance faciale a été un temps envisagée pour l'enrôlement d'un moyen d'identification électronique de niveau substantiel dans le cadre du projet « ALICEM », le référentiel relatif aux prestataires de vérification de l'identité à distance publié par l'Agence nationale de sécurité des systèmes d'information (ANSSI) le 1er mars 2021 requiert une intervention humaine pour valider l'identité au niveau substantiel. La Commission quant à elle s'était inquiétée, dans sa délibération n° 2018-342 du 18 octobre 2018, d'une utilisation, sans alternative, de la reconnaissance faciale lors de ce processus dans le cadre du dispositif « ALICEM ».

9. Le présent projet de décret autorise le traitement « SGIN » à lire les données enregistrées dans le composant électronique des CNIe, à l'exception de l'image numérisée des empreintes digitales. Même si le dispositif « SGIN » traitera la donnée relative à la photographie de l'usager, le présent projet de décret, en son article 2-II, prévoit que le dispositif ne comporte pas de traitement biométrique de la photographie. La Commission relève qu'aucun traitement supplémentaire de donnée biométrique ne sera réalisé du fait de la mise en œuvre du traitement projeté.

10. Enfin, la Commission prend acte des précisions apportées selon lesquelles il est envisagé, pour fin 2022, une extension du dispositif « SGIN » aux passeports et titres de séjour. Elle rappelle qu'une telle extension devra lui être soumise pour avis.

11. Le traitement « SGIN », en tant que moyen d'identification électronique, sera le support qui permettra de développer, graduellement, les usages numériques en ligne et dans le monde physique de la CNIe sur laquelle la Commission a déjà eu à se prononcer.

12. La Commission prend acte de ce que ce dispositif d'identité numérique permettra une identification de niveau élevé, une possibilité de démontrer seulement certains attributs et de créer des justificatifs d'identité permettant de remplacer le recours aux photocopies de pièces d'identité. A cet égard, il est rappelé que la Commission a toujours été favorable à la création d'une identité numérique d'Etat de haut niveau, de nature à améliorer la sécurité des procédures (en supprimant par exemple la circulation de photocopies de pièces d'état-civil lors de l'accomplissement de démarches administratives) et à faciliter la lutte contre la fraude documentaire. Enfin, la Commission apprécie particulièrement que le ministère ait prévu un dispositif permettant d'assurer la minimisation des données, que ce soit par la divulgation des seuls attributs nécessaires lors de l'utilisation de la CNIe pour l'identification du porteur ou par la possibilité de créer des attestations minimisées contenant les seules informations strictement nécessaires à certaines démarches et pouvant être utilisées hors ligne.

13. La Commission accueille très favorablement ce projet, dont elle note qu'il est l'aboutissement d'échanges nourris avec le ministère et qu'il permet le développement d'une identité numérique régalienne de niveau élevé et respectueuse de la vie privée des usagers.

Sur la finalité du dispositif projeté

14. L'article 1er du projet de décret prévoit notamment que le traitement « SGIN » aura pour finalité de proposer aux titulaires d'une CNIe la délivrance d'un moyen d'identification électronique leur permettant de s'identifier et de s'authentifier électroniquement auprès d'organismes publics ou privés, à savoir des fournisseurs de services liés par convention à « FranceConnect », des fournisseurs de services liés par convention au ministère de l'intérieur ou des tiers *via* des attestations générées par l'usager avec le traitement « SGIN ».

15. La finalité envisagée apparaît déterminée, explicite et légitime conformément à l'article 5 du règlement général sur la protection des données (ci-après « RGPD »).

16. La Commission comprend des précisions apportées que le « SGIN », en tant que moyen d'identification électronique, permettrait à ses utilisateurs de s'identifier et de s'authentifier électroniquement et ainsi :
    - d'accéder aux services en ligne des fournisseurs de services publics ou privés ;
    - de prendre connaissance des données contenues dans la carte et d'en générer des attestations électroniques d'attributs d'identité qu'ils pourront transmettre électroniquement aux tiers de leur choix ou présenter dans le monde physique (par exemple pour apporter la preuve de leur majorité ou de leur âge).

17. Toutefois la Commission s'interroge quant à l'absence de mention explicite au sein du projet de décret de la faculté pour l'usager de générer ses attestations utilisables à la fois en ligne et hors ligne.

Sur les données traitées

18. A titre liminaire, il est relevé que l'article 3-II du projet de décret prévoit que lorsque les usagers s'identifient et s'authentifient électroniquement, ils peuvent accéder à la quasi-totalité des données d'identité traitées et les transmettre aux personnes physiques ou morales de leur choix. La Commission encourage ce type de dispositif qui doit rester à la main de l'usager.

19. L'article 2 du projet de décret liste les informations qui peuvent être traitées et enregistrées dans le traitement « SGIN ». Parmi celles-ci figure la photographie de l'usager extraite du composant électronique du titre d'identité. La Commission prend acte des précisions apportées par le ministère selon lesquelles le traitement de cette donnée permettrait à l'usager de faire apparaître sa photographie sur son attestation électronique d'attributs d'identité ou conjointement à un code QR afin de l'authentifier. La Commission prend acte de ce que cette donnée, qui transitera par le serveur du « SGIN », sera conservée uniquement de manière chiffrée au sein du téléphone portable de l'usager.

20. Ce même article prévoit également que les données relatives à l'historique des transactions réalisées par l'usager seront traitées dans le cadre du dispositif « SGIN ». Si la Commission prend acte des précisions apportées, à savoir que ne seront traitées que les cinq dernières transactions de l'usager, elle estime que l'article 2 du présent projet de décret pourrait être complété sur ce point en mentionnant explicitement le nombre exact des dernières transactions qui seront traitées ou, à tout le moins, en mentionnant que cet historique est limité par un nombre maximal de transactions conservées en mémoire, déterminé par le responsable de traitement. Dans un objectif de transparence et de contrôle par les utilisateurs de leur moyen d'identification électronique, mais aussi afin de détecter le plus tôt possible une éventuelle usurpation du moyen d'identification, la Commission recommande qu'une notification par un canal séparé (courriel, par exemple) soit adressée à l'utilisateur à chaque utilisation du dispositif, sur le modèle de ce qui est fait pour « FranceConnect ».

21. Les autres données traitées dans le cadre du dispositif « SGIN » n'appellent pas d'observations de la part de la Commission.

Sur les destinataires des données

22. L'article 3-II du projet de décret prévoit que peuvent être destinataires de certaines données traitées par le dispositif « SGIN », dans la limite du besoin d'en connaître, les personnes physiques ou morales choisies par l'usager, le téléservice « FranceConnect », les fournisseurs de services liés par convention à « FranceConnect » et les fournisseurs de services liés par convention au ministère de l'intérieur.

23. **Dans un premier temps**, la Commission prend acte de ce que lorsque l'usager entend transmettre à un tiers une attestation électronique d'attributs d'identité, il a la possibilité, *via* son application mobile, de sélectionner les données à faire apparaître sur ce document en fonction des exigences du destinataire concerné. Cette divulgation sélective d'attributs et la possibilité de preuves sur des attributs sont fortement encouragées par la Commission.

24. **Dans un second temps**, la Commission prend acte de ce que seules les données dites « pivot » (nom, nom d'usage, prénom(s) date de naissance, lieu de naissance et sexe) ainsi que l'adresse de courrier électronique de l'usager seront transmises au téléservice « FranceConnect », à charge pour ce dernier de ne transmettre aux fournisseurs de services avec lesquels il a une convention que les attributs qui leur sont nécessaires et qu'ils ont expressément demandés, tel que prévu dans ses conditions générales d'utilisation.

25. De manière générale, la Commission rappelle que les conventions liant les fournisseurs de services à « FranceConnect » et au ministère de l'intérieur doivent être conformes à la règlementation en matière de protection des données.

Sur les durées de conservation

26. A titre liminaire, la Commission tient à souligner que le ministère a fait un travail de minimisation pour ne conserver sur le serveur qu'une liste de données à caractère personnel succincte. Elle regrette néanmoins que la rédaction de l'article 4 du projet de décret n'en fasse pas mention.

27. En premier lieu, la Commission prend acte de ce que les données à caractère personnelle sont supprimées à l'issue d'une période d'inactivité du moyen d'identification électronique de deux ans. Cette durée a été établie au regard de l'utilisation moyenne envisagée du moyen d'identification électronique calquée sur l'utilisation actuelle du téléservice « FranceConnect ». Cette suppression porte tant sur les données contenues dans le téléphone portable de l'usager que sur celles contenues au sein du serveur du responsable de traitement.

28. En second lieu, la Commission prend acte de ce que les données à caractère personnel relatives aux cinq dernières transactions de l'usager sont conservées, sur le terminal de l'usager, pour une durée maximum de cinq ans. Dans le cas où l'usager supprime son moyen d'identification électronique, si celui-ci expire, ou si l'usager désinstalle l'application, ces données seront immédiatement supprimées du téléphone portable de l'usager.

29. Par ailleurs, les données relatives à la création du moyen d'identification électronique seront conservées en base active par le ministère durant cinq ans. Bien que la durée envisagée semble pertinente au regard des finalités et des obligations relatives à la création d'un tel moyen d'identification électronique, la Commission s'interroge sur la pertinence de conserver ces données en base active durant toute la durée de conservation. Elle encourage le ministère à évaluer s'il est possible de, et à partir de quand, conserver ces données en base archive.

30. Enfin, le ministère conserve pendant trois ans sur le serveur les traces concernent les opérations de création, de consultation, d'utilisation, de révocation et de suppression du moyen d'identification électronique. Au vu de l'impact potentiel sur les personnes concernées, la Commission considère comme proportionnée la durée de conservation des journaux, relatifs aux opérations de création, de consultation, de révocation et de suppression du moyen d'identification électronique.

31. La Commission s'interroge cependant sur la conservation à si long terme des traces d'utilisation du moyen d'identification électronique, dès lors qu'il serait utilisé pour des services non-régaliens. La Commission encourage le ministère à réévaluer la pertinence et l'équilibre (au regard du suivi que cela implique) de conserver ces traces sur trois ans pour les services commerciaux.

Sur l'interrogation avec le fichier national de contrôle de la validité des titres (« DOCVERIF »)

32. La Commission prend acte de ce que le traitement projeté « SGIN » interrogera le fichier national de contrôle de la validité des titres (ci-après « DOCVERIF »).

33. L'interrogation du fichier « DOCVERIF » impliquerait de traiter le numéro du titre, le type du titre et sa date de délivrance. Cette interrogation du fichier retournerait le statut de validité administrative du titre (valide, invalide ou inconnu).

34. Cette interrogation aura lieu afin de vérifier la validité des titres présentés lorsque le moyen d'identification électronique sera utilisé avec un niveau de garantie élevé, ainsi que pour la génération d'attestations, mais pas lorsqu'il sera utilisé comme moyen d'identification ou d'authentification avec les niveaux de garanties substantiel ou bas.

35. Si les interconnexions, mises en relation et rapprochements de base de données n'ont pas obligatoirement à figurer dans l'acte réglementaire, la Commission recommande vivement aux responsables de traitement publics, pour les traitements correspondant à des bases de données importantes, de décrire sur leur site web l'ensemble des mises en relation réalisées avec d'autres bases de données.

Sur les mesures de sécurité

36. Le ministère a fourni à la Commission une analyse d'impact relative à la protection des données (ci-après « AIPD ») démontrant sa bonne prise en compte des risques sur les personnes concernées liés au dispositif.

37. En particulier, la Commission a pris note à la fois de l'intégration, dès que possible, de briques logicielles ayant fait l'objet d'un visa de sécurité par l'ANSSI, ainsi que la mise en œuvre d'un processus d'homologation, de certification et/ou de qualification pour l'ensemble des éléments du processus, application comprise.

38. Concernant la génération d'attestations, bien que la qualification de ces attestations soit effectuée seulement dans un second temps, la Commission a bien noté qu'une certification de sécurité de premier niveau (CSPN) est prévue à court terme. La Commission tient à souligner l'importance d'évaluer la solution en prenant en compte l'impact potentiel des utilisations frauduleuses, notamment par un tiers, d'une telle attestation, en vérifiant notamment que des mesures adaptées sont mises en œuvre (par exemple avec un dispositif de date maximale d'utilisation pour chaque attestation et un système de révocation d'attestation par l'utilisateur en un clic).

39. En ce qui concerne les identifications et authentification à des fournisseurs de services partenaires, donc en dehors du système « FranceConnect », la Commission prend acte de ce que la minimisation des données à caractère personnel sera intégrée aux conventions afin d'assurer que seules les données nécessaires soient demandées. N'ayant pas eu accès au schéma technique détaillé, la Commission encourage le ministère à vérifier que les solutions choisies fournissent une garantie technique à la hauteur des garanties juridiques prévues.

40. Ainsi, les mesures de sécurité décrites par le responsable de traitement semblent conformes à l'exigence de sécurité prévue par les articles 5.1.f et 32 du RGPD ainsi que l'article 4-6 de la loi du 6 janvier 1978 modifiée. La Commission rappelle toutefois que cette obligation nécessite la mise à jour de l'AIPD et de ses mesures de sécurité au regard de la réévaluation régulière des risques.

La Présidente

Marie-Laure DENIS