Afin de garantir la sécurité du dispositif « e-carte Vitale », certaines informations techniques de cette délibération ont été supprimées, conformément à la réglementation applicable en matière d'accès aux documents administratifs.

Délibération n°2021-031 du 18 mars 2021 portant avis sur un projet de décret prorogeant et étendant l'expérimentation d'une « e-carte d'assurance maladie »

(demande d'avis n° 20020687)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre des solidarités et de la santé d'une demande d'avis concernant un projet de décret prorogeant et étendant l'expérimentation d'une « e-carte d'assurance maladie » ;

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 ou RGPD) ;

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

Après avoir entendu Mme Valérie PEUGEOT, commissaire, en son rapport, et M. Benjamin TOUZANNE, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

1. Le projet de décret vise à apporter des modifications au décret n°2019-528 du 24 mai 2019 relatif à l'expérimentation d'une e-carte d'assurance maladie.

Sur la responsabilité de traitement :

2. L'analyse d'impact relative à la protection des données (AIPD) relative à la modification projetée précise que sont responsables conjoints du traitement de l'expérimentation la caisse nationale d'assurance maladie (CNAM) ainsi que la caisse centrale de la mutualité sociale agricole (CCMSA). La Commission invite le ministère à compléter le projet de décret sur ce point, comme demandé dans sa délibération n°2018-328 du 11 octobre 2018.

Sur l'extension de l'expérimentation :

3. Le projet d'article 1er du décret vise à prolonger jusqu'au 31 décembre 2022 et à étendre à dix départements la phase d'expérimentation, soit douze au total. Le ministère précise que cette extension est nécessaire afin de pouvoir disposer d'éléments permettant de garantir un bilan significatif de l'expérimentation, ce dont la Commission prend acte.

Sur la modification de la base légale :

4. Le projet de décret modifie la base légale du traitement de données mis en œuvre dans le cadre de l'expérimentation, jusqu'alors fondée sur le consentement des professionnels et des patients participants tel que prévu par l'article 6.1.a du RGPD.

5. Selon le ministère, l'expérimentation sera désormais fondée sur l'exécution de la mission d'intérêt public dont est investie la Caisse nationale d'assurance maladie (CNAM) par le code de la sécurité sociale (CSS), conformément à l'article 6.1.e du RGPD. Le ministère a indiqué que le consentement ne semble pas constituer un fondement juridique adéquat, la finalité principale du traitement étant liée aux obligations de service public auxquelles est tenue la CNAM et la gestion des droits des personnes liés au consentement (portabilité notamment) est impossible au regard de ses missions.

6. La Commission en prend acte et relève néanmoins que la participation à l'expérimentation demeure volontaire et n'emporte aucune conséquence sur l'effectivité de la prise en charge des personnes concernées.

Sur les données traitées :

7. Le projet d'article 13 bis du décret précise que l'e-carte d'assurance maladie contient l'identifiant national de santé mentionné à l'article L. 1111-8-1 du code de la santé publique (CSP) afin de permettre l'identification électronique des patients dans le cadre de leur prise en charge conformément à l'article L. 1110-4 du même code.

8. En outre, le projet d'article 13 ter prévoit, lors de la délivrance de l'e-carte d'assurance maladie, la vérification de l'identification des assurés pourra être réalisée au moyen de téléservices conçus par la CNAM en application de l'article R. 1111-8-6 du CSP.

S'agissant de la mise en œuvre d'un traitement de données biométriques lors de l'installation de l'application e-carte vitale :

9. Le projet d'article 13 quater du décret prévoit la création, par les organismes gestionnaires de l'assurance maladie obligatoire mentionnés à l'article L. 160-17 du CSS, d'un traitement comprenant des données biométriques lors de l'installation de l'application e-carte vitale par les assurés. La Commission relève que le projet de décret ne mentionne ni le terme « biométrie » ni le terme « traitement de gabarit biométrique ». Elle rappelle cependant que la photographie ne constitue généralement pas, par elle-même, une donnée biométrique permettant l'identification d'une personne de façon unique. Le traitement biométrique de la photographie nécessitera la création de « gabarits », qui constituent une donnée distincte et ayant le caractère de « donnée biométrique » au sens des articles 4 et 9 du RGPD. Comme elle l'a déjà fait par le passé, la Commission demande au ministère d'indiquer explicitement, dans la liste des données traitées, la présence de telles données (délibération n° 2020-064 du 25 juin 2020).

10. Il est prévu le traitement de la photographie du titre d'identité des participants ainsi que la prise de vue de leur visage, réalisées par eux après le téléchargement de l'application e-carte vitale. Ce traitement a pour objectif, au moyen de gabarits biométriques, de vérifier la concordance entre les deux images afin d'attester de l'identité de la personne ayant téléchargé l'application. Cette concordance sera vérifiée de façon automatique, ou validée par une intervention humaine, avant de permettre l'activation de l'e-carte d'assurance maladie.

11. Selon les précisions du ministère, la collecte de la photographie utilisée dans le traitement de données biométriques se fonde sur les dispositions de l'article 9.2.b du RGPD, et est nécessaire pour le respect des dispositions :
    - de l'article R. 161-33-1 du code de la sécurité sociale qui impose la présence d'une « photographie en couleur de face, tête nue, récente et parfaitement ressemblante » sur la carte vitale « physique » ;
    - de l'article R. 161-33-3 du code de la sécurité sociale qui prévoit que les assurés doivent fournir « une photocopie d'une pièce d'identité comportant une photographie » afin de permettre aux organismes servant les prestations d'un régime d'assurance maladie de délivrer « une carte d'assurance maladie aux personnes qui lui sont rattachées, en s'assurant de l'identité du titulaire de la carte ».

12. En outre, il est prévu que l'e-carte vitale puisse, à la différence de la carte vitale « physique », être utilisée par les patients comme moyen d'identification électronique afin de bénéficier des services et outils numériques visés à l'article L.1110-4-1 du CSP. Cette utilisation constitue, selon le ministère, une autre justification du traitement de données biométriques à des fins de vérification de l'identité des assurés par l'intermédiaire d'un dispositif de reconnaissance faciale.

13. La Commission souligne que les opérations liées à l'activation de l'e-carte vitale, avec les vérifications d'identité impliquées, et les opérations liées à l'utilisation de cette e-carte pour bénéficier de services et outils numériques en ligne constituent, contrairement à ce que peut laisser entendre l'article 13 quater du décret, un seul et même traitement mis en œuvre dans un cadre expérimental. La vérification de l'identité ne constitue en effet, dans le cadre du décret, non une finalité en elle-même pour un traitement autonome, mais un moyen d'atteindre les objectifs de l'expérimentation. La Commission invite donc le ministère à clarifier l'article 13 quater sur ce point.

14. Le projet d'article 13 quater prévoit que la durée de conservation des données biométriques est de trois mois à compter de l'activation de la e-carte vitale au terme duquel elles sont détruites. La Commission prend acte des précisions suivantes apportées par l'AIPD selon lesquelles :
    - les données servant au traitement biométrique (photographie présente sur la pièce d'identité, flux vidéo et photographie du visage de l'utilisateur ainsi que leur gabarit) sont supprimées immédiatement à l'issue d'un rapprochement automatique positif, mais conservées sept jours à l'issue d'un rapprochement manuel pour permettre d'auditer ces opérations ;
    - le fichier de preuve du rapprochement (identité du demandeur, numérisation et score d'authenticité de la pièce d'identité, causes de rejet, score de la comparaison biométrique) est conservé à des fins de suivi du

marché (trente jours) et de traitement des contestations (soixante jours). La Commission relève que le projet de décret mentionne que les données traitées sont conservées pendant une durée maximale de trois mois à compter de l'activation de l'e-carte. Elle demande que les durées du décret soient harmonisées avec celles plus réduites détaillées dans l'AIPD.

15. Tout en comprenant la nécessité de vérification du dispositif au début de l'expérimentation, la Commission recommande que d'autres moyens soient étudiés pour la réalisation de ces audits ou pour augmenter la fiabilisation du dispositif. Elle estime en outre que dans l'hypothèse où le dispositif serait pérennisé, les données biométriques devront être supprimées dès le rapprochement réalisé, qu'il soit automatique ou manuel, positif ou débouchant sur un rejet.

16. Elle relève également que le fichier de preuve contenant la photographie de la pièce d'identité ne pourra pas être réutilisé à des fins de traitement biométrique.

S'agissant des données relatives aux participants potentiels :

17. L'article 2 du projet de décret prévoit de supprimer l'article 7 du décret qui détaille les données à caractère personnel relatives aux potentiels participants qui se verront proposer de participer à l'expérimentation. Le ministère a indiqué que cette suppression était justifiée par le changement de base légale du traitement. Cependant, la Commission relève que, selon les précisions du ministère, les assurés éligibles seront destinataires de courriels d'information les invitant à participer à l'expérimentation. La Commission en déduit qu'un traitement de données des potentiels participants sera mis en œuvre et invite donc le ministère à maintenir dans le décret la liste les données à caractère personnel pouvant être traitées dans ce cadre.

Sur l'information et les droits des droits des personnes concernées :

18. La Commission rappelle que les personnes concernées devront être informées dans les conditions prévues par l'article 13 du RGPD et estime que l'information ne pourra se limiter à l'affichage de conditions générales d'utilisation (CGU) lors du téléchargement de l'application et devrait être complétée par des informations disponibles sur le site de la CNAM auxquelles les personnes pourront se reporter pendant toute la durée du traitement.

19. La Commission relève par ailleurs que le projet d'article 13 quater indique que le traitement portant sur des données biométriques ne fera pas l'objet d'une information distincte du traitement relatif à l'e-carte d'assurance maladie.

20. La Commission suggère l'utilisation de « l'approche à plusieurs niveaux dans un environnement numérique » recommandée par le CEPD dans ses lignes directrices relatives à la transparence : l'information pourrait ainsi être détaillée au fur et à mesure du parcours de l'utilisateur dans l'application e-carte vitale, lui permettant de disposer des informations relatives au traitement biométrique avant d'effectuer les prises de vue.

S'agissant des participants déjà inclus :

21. Selon le ministère, les personnes déjà incluses dans l'expérimentation seront informées des nouvelles modalités de celle-ci par l'affichage des nouvelles CGU lors de la mise à jour de l'application e-carte vitale. Les personnes pourront donc choisir de les accepter ou de désinstaller l'application, ce qui entrainera la suppression des données personnelles de l'assuré liées à l'application et sa sortie de l'expérimentation.

22. La Commission demande que les personnes soient informées de manière extrêmement claire de ces évolutions et estime qu'un résumé des modifications substantielles, telles que l'ajout d'un traitement de données biométriques et le changement de base légale, devrait leur être transmis indépendamment et en amont de l'accès aux CGU et complété d'un renvoi vers ces dernières indiquant clairement les évolutions prévues afin de leur permettre d'anticiper leur sortie de l'expérimentation, le cas échéant.

23. Le changement de base légale du traitement emporte des conséquences sur les libertés et les modalités d'exercice des droits des personnes, à plus forte raison pour celles qui ont déjà été incluses dans l'expérimentation (droit à la portabilité, retrait du consentement, etc.). La Commission invite donc le ministère à permettre à ces dernières de retirer leur consentement, ce qui entraînera leur sortie de l'expérimentation, et exercer leurs droits préalablement à l'entrée en vigueur du décret.

S'agissant des nouveaux participants :

24. S'agissant du droit d'opposition, le projet d'article 13 quater du décret précise que le droit d'opposition prévu à l'article 56 de la loi « informatique et libertés » ne s'applique pas au traitement de données biométriques visant à vérifier l'identité des personnes. La Commission en déduit, en l'absence de mention d'un dispositif alternatif de vérification de l'identité, que la participation à l'expérimentation est conditionnée au traitement des données biométriques.

25. La Commission prend acte de ce que la participation à l'expérimentation est volontaire, que le traitement de données biométriques est propre à cette expérimentation et de ce que les personnes ne souhaitant pas voir leurs données biométriques traitées pourront toujours bénéficier d'une prise en charge au moyen d'une carte vitale « physique ». Elle demande que cela soit clairement indiqué dans la note d'information à destination des personnes concernées.

26. La Commission relève enfin que le projet de décret ne mentionne pas le droit d'opposition ou d'effacement des personnes concernant le fonctionnement de l'e-carte vitale. Selon les précisions du ministère, le droit d'opposition ne peut être exercé pour le traitement des données issues de l'usage de l'application car celles-ci sont nécessaires à la réalisation des missions de la CNAM (liquidation, contrôles, etc.).

27. La Commission analyse ces exclusions comme la mobilisation des dispositions de l'article 23 du RGPD qui permet de limiter les droits des personnes pour garantir, notamment, des objectifs importants d'intérêt public dans le domaine de la sécurité sociale.

28. La Commission comprend que les personnes pourront s'opposer au traitement de leurs données à caractère personnel au moment de l'affichage des CGU de l'application e-carte vitale, ce qui entraînera le refus d'entrée dans l'expérimentation. Afin de garantir la transparence du traitement vis-à-vis des personnes, la Commission invite le ministère à préciser les limitations et les modalités d'exercice du droit d'opposition et d'effacement dans le décret.

Sur les mesures de sécurité :

29. Concernant les services et outils numériques visés à l'article L. 1110-4-1 du CSP qui seront accessibles à l'aide de l'e-Carte Vitale, le ministère a précisé que le dossier médical partagé (DMP) sera concerné en premier lieu et que le projet « espace numérique de santé » (ENS) devrait également intégrer cette modalité au début de l'année 2022. Les plateformes de téléconsultation et les services à destination des transporteurs compléteront cette première vague.

30. Plus largement, la e-Carte Vitale vise à devenir un fournisseur d'identité de niveau eIDAS substantiel pour les fournisseurs de service destinés aux assurés tels que les portails web et les applications mobiles de l'assurance maladie, de la sphère santé-sociale, et ceux utilisant FranceConnect. A cet égard, la Commission considère que la vérification d'identité en ligne doit reposer sur des mécanismes techniques minimisant et sécurisant les données traitées. Les travaux actuels autour de l'identité numérique doivent permettre d'améliorer les techniques de vérification qui reposent aujourd'hui sur l'analyse de pièces « papier » au profit de mécanismes reposant sur des composants électroniques, des mécanismes cryptographiques et des flux d'échanges sécurisés (CNIe, passeport, ALICEM, France Connect), qualifiés au sens d'eIDAS.

31. La Commission relève que l'AIPD détaille de manière très complète l'ensemble des aspects techniques liés à l'application et à ses usages, ainsi que les risques et les mesures pour les réduire. Le ministère a également répondu aux demandes de compléments émises par les services de la Commission. Il en ressort que les modifications portées par le projet de décret ont fait l'objet d'une approche de « *Privacy by design* » très poussée.

32. La Commission relève néanmoins quelques points d'attention, exposés ci-dessous.

33. L'enrôlement biométrique pourra faire l'objet d'un contrôle manuel en cas de doute signalé par le système, voire un contrôle manuel systématique si le référentiel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) venait à l'exiger à l'avenir pour la qualification eIDAS.

34. La Commission considère que le fichier de preuve contenant la numérisation de la pièce d'identité ne devra pas être conservé par le prestataire de vérification d'identité au-delà de sa transmission au responsable de traitement, et que ce fichier devra faire l'objet de mesures garantissant sa confidentialité et interdisant sa réutilisation ultérieure à des fins de traitement biométrique.

35. La photographie de l'utilisateur qui sera retenue après l'enrôlement biométrique sera issue de la prise de vue de son visage et non de sa pièce d'identité.

36. Les identifiants du système mobile et de l'application e-carte vitale (ApCV) de l'utilisateur seront générés aléatoirement (selon la norme UUID version 4) et celui du professionnel de santé sera son identifiant national.

37. L'identifiant de l'assuré dans le système central de l'ApCV sera son NIR pseudonymisé.

39. Concernant les risques liés à une indisponibilité de l'ApCV, il a été précisé que celle-ci devra pour l'instant être considérée comme un support complémentaire à la carte vitale physique, qui continuera à être délivrée et devra être conservée par les assurés ; ceci tient compte également du temps nécessaire pour la mise à jour des logiciels des nombreux professionnels de santé en ville et des établissements de santé. La Commission en prend acte et estime en outre nécessaire, au regard de ces risques mais également des enjeux d'inclusion numérique, de garantir la délivrance d'une carte vitale physique en cas de pérennisation du dispositif.

40. La Commission relève qu'aux fins de protection des données et pour éviter l'usurpation d'identité en cas de vol du ordiphone, l'ApCV sera protégée par un code secret spécifique et toutes ses données locales seront chiffrées.

42.

46. Enfin, concernant l'usage de l'ApCV avec les services web pour les professionnels de santé (AmeliPro, WebDMP PS), le ministère a indiqué que la CNAM en a validé le principe et inscrit les travaux d'adaptation de ces portails dans leur feuille de route 2021. La Commission rappelle que les analyses d'impact sur la protection des données devront être mises à jour en conséquence pour l'ApCV et pour ces portails.

48. La Commission demande aux responsables de l'expérimentation de s'assurer que le prestataire de vérification d'identité et les autres sous-traitants intervenant dans le cadre de l'expérimentation relèvent exclusivement des juridictions de l'Union européenne.

49. L'analyse d'impact devra être complétée sur ces points.

50. Enfin, la Commission demande, comme elle a eu l'occasion de le mentionner dans sa délibération n°2018-328 du 11 octobre 2018, qu'un bilan détaillé de l'expérimentation lui soit communiqué avant toute éventuelle généralisation du dispositif d'eCarte d'assurance maladie. Elle estime nécessaire que l'apport de l'utilisation de données biométriques y soit démontré, et que l'articulation du dispositif ApCV avec le reste de l'écosystème des titres eIDAS devra y être explicité et justifié, notamment vis-à-vis de la CNIe, d'ALICEM et de France Connect. En outre, le bilan devra détailler la manière dont les référentiels applicables publiés par l'ANSSI, notamment celui concernant les prestataires de vérification d'identité à distance (PVID), sont suivis, et notamment la prise en compte des « recommandations aux commanditaires » de ce dernier référentiel.

51. La Commission regrette enfin que l'extension de l'expérimentation n'ait pas fait l'objet de rapports intermédiaires.

La Présidente

Marie-Laure DENIS