Commission nationale de l'informatique et des libertés

Délibération n° 2014-430 du 23 octobre 2014 portant avis sur un projet de décret en Conseil d'Etat autorisant les traitements de données à caractère personnel mis en œuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement des missions de leurs services médicaux (demande d'avis n° 14021842)

NOR : *CNIX1508677X*

La Commission nationale de l'informatique et des libertés, saisie par la ministre des affaires sociales, de la santé et des droits des femmes d'une demande d'avis concernant un projet de décret en Conseil d'Etat autorisant les traitements de données à caractère personnel mis en oeuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement des missions de leurs services médicaux ;

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 la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code rural et de la pêche maritime ;

Vu le code de la sécurité sociale ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 27-1-1° ;

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 ;

Après avoir entendu M. Alexandre LINDEN, commissaire, en son rapport, et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

La commission a été saisie, le 28 juillet 2014 et par saisine rectificative le 8 octobre 2014, par la ministre des affaires sociales, de la santé et des droits des femmes d'une demande d'avis concernant un projet de décret en Conseil d'Etat (ci-après « le projet ») autorisant les traitements de données à caractère personnel mis en œuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement des missions afférentes à leurs services médicaux en matière de prise en charge des prestations maladie, maternité, invalidité, inaptitude, accident du travail et maladie professionnelle.

Ce projet vise à créer une catégorie de traitements de données à caractère personnel relevant des missions des services médicaux de l'assurance maladie obligatoire (AMC) portant notamment sur le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) des assurés sociaux.

Ces traitements seront mis en œuvre par la Caisse nationale de l'assurance maladie des travailleurs salariés (CNAMTS), la Mutualité sociale agricole (MSA) et le Régime social des indépendants (RSI).

Le projet de texte soumis à la commission est pris en application de l'article 27-1 (1°) de la loi du 6 janvier 1978 modifiée qui prévoit que *« sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés »,* les traitements de données à caractère personnel mis en œuvre pour le compte d'une personne morale de droit public *« qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ».*

Les articles R. 115-1 et suivants du code de la sécurité sociale (CSS) prévoient que *« Les organismes et administrations chargés de la gestion d'un régime obligatoire de base de sécurité sociale et, le cas échéant, les organismes habilités par la loi ou par une convention à participer à la gestion de ces régimes »* sont autorisés à utiliser le NIR. Ces dispositions précisent que *« l'autorisation donnée à l'article R. 115-1 vaut exclusivement pour les traitements mis en œuvre dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 »* pour des finalités au nombre desquelles ne figurent ni la gestion individualisée de la relation avec les bénéficiaires de prestations et les producteurs de soins et prestataires de services ni l'offre de téléservices.

Dès lors que ces traitements sont substantiellement différents de ceux qu'autorisent les dispositions réglementaires en vigueur, ils doivent être autorisés par un décret en Conseil d'Etat pris après avis de la CNIL, en application de l'article 27-1 (1°) précité.

Sur la dénomination et les finalités des traitements :

Le projet est relatif à la mise en œuvre de traitements de données à caractère personnel destinés à l'exercice des missions des services médicaux des organismes gestionnaires des régimes obligatoires de base de l'assurance maladie.

L'article 1er du projet explicite le périmètre et les finalités des traitements mis en œuvre dans le cadre des activités précitées de l'assurance maladie.

Ces traitements ont vocation à permettre de

« 1° déterminer l'étendue des droits aux prestations dues en cas d'accident du travail et de maladie professionnelle des assurés et ayants droit, ouvrir ces droits et verser les prestations correspondantes ;

« 2° analyser et contrôler les activités des professionnels de santé et des établissements de santé ;

« 3° permettre la gestion individualisée de la relation avec les bénéficiaires de prestations et les producteurs de soins et prestataires de services, par courrier postal ou électronique, par messages téléphoniques, par services d'accueil téléphonique ou physique et par téléservices ;

« 4° contribuer à la sécurité du versement des prestations et à la prévention et à la lutte contre les fautes, abus et fraudes et à la gestion et au suivi des actions contentieuses ;

« 5° communiquer aux autres organismes gestionnaires des régimes obligatoires de base de l'assurance maladie les informations nécessaires à l'accomplissement de leurs missions dans le respect du secret professionnel et médical ;

« 6° produire des statistiques et piloter et mettre en œuvre la politique de gestion du risque et de prévention, analyser les prestations versées et les soins produits, évaluer la qualité du service rendu aux usagers, suivre les relations conventionnelles avec les professionnels de santé, contrôler, prévenir les recours contentieux et, le cas échéant, lutter contre les fautes, abus et fraudes. »

S'agissant de la production de statistiques, la commission prend acte de ce que les analyses statistiques porteront sur des données préalablement anonymisées, d'une part, et uniquement sur des données strictement nécessaires et proportionnées à la finalité poursuivie par le traitement considéré, d'autre part. Elle demande que le projet soit complété en ce sens.

La commission observe que le projet poursuit également une finalité de lutte contre la fraude et rappelle à cet égard que, conformément à l'article 10 de la loi du 6 janvier 1978 modifiée, aucune décision produisant des effets juridiques à l'égard des personnes concernées par des données traitées dans le cadre de la lutte contre la fraude ne peut être prise sur le seul fondement de traitements automatisés de données destinés à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Dès lors, les requêtes ou alertes détectées automatiquement doivent donner lieu à une analyse non automatisée par le personnel habilité de l'organisme auquel il appartient ; le cas échéant des investigations complémentaires pourront être diligentées. Enfin, la personne concernée doit être mise en mesure de présenter ses observations si une décision produisant des effets juridiques est prise à son égard dans le cadre de la conclusion ou de l'exécution d'un contrat.

La commission considère, sous réserve des observations précédentes, que la création des traitements précités et les finalités ainsi poursuivies sont déterminées, explicites et légitimes.

Sur les catégories de données à caractère personnel enregistrées :

L'article 2 du projet prévoit le traitement des catégories de données à caractère personnel relatives, d'une part, aux assurés sociaux et leurs ayants droit et, aux professionnels de santé, d'autre part.

S'agissant des assurés sociaux et leurs ayants droit, les données concernent :

– l'identification des personnes (le NIR ou NIA et date d'attribution, les nom de famille, d'usage, prénoms, sexe, civilité et qualité d'assuré ou d'ayant droit le cas échéant, le lien familial avec l'assuré, date et lieu de naissance, rang de naissance, date de décès le cas échéant, le numéro de pièce d'identité ou de titre de séjour, l'adresse postale et électronique, numéro de téléphone) ;
– des informations relatives à la couverture sociale (le ou les organismes de rattachement, exonération du ticket modérateur, date et nature de l'exonération, identification de l'organisme complémentaire, le bénéfice de la couverture maladie universelle, de la couverture maladie universelle complémentaire ou de l'aide à l'acquisition d'une complémentaire santé) ;
– des informations relatives à l'identification du médecin traitant s'il a été désigné (ses identifiants, nom, prénom, spécialité, adresse et numéro de téléphone) ;
– des données relatives à l'état de santé du bénéficiaire (les données relatives à l'état de santé présent et passé le cas échéant, l'information relative à la résidence en établissement de personnes âgées dépendantes, la nature des actes et médicaments ou produits de santé et leurs codages détaillés, l'existence d'une grossesse ou d'une affection de longue durée et les éléments du protocole relatif à cette affection, les informations relatives à l'appareillage, à une cure thermale ou à une prestation soumise à accord préalable, l'existence d'une hospitalisation, ses dates le numéro d'établissement, la discipline médico-tarifaire et le groupe homogène de séjour, le descriptif médical, les résultats des examens complémentaires et les traitements en cours en rapport avec une pathologie à l'origine d'une demande de prestation) ;
– des informations relatives à l'existence d'accidents du travail ou de maladies professionnelles (dates, siège de la ou des lésions, leurs diagnostics, numéros de dossiers, nature de l'avis médical et taux d'incapacité permanente avec le descriptif des séquelles cliniques ou fonctionnelles correspondantes) ;
– des informations relatives à l'existence d'un arrêt de travail et des diagnostics des causes médicales de celui-ci ;
– des informations relatives à l'existence d'une invalidité (sa catégorie, l'existence d'une inaptitude, leurs diagnostics et le versement d'une prestation invalidité) ;
– l'existence d'un recours contre tiers ;

– les documents bureautiques échangés avec les bénéficiaires et les professionnels de santé dans le cadre de la gestion des dossiers et demandes de prestations.

S'agissant des professionnels de santé, les données concernent :

– l'identification (nom, prénom, les numéros ADELI, du répertoire partagé des professionnels de santé, du RFOS ou SIRET, l'adresse postale, numéros de téléphone et adresse électronique) ;
– des informations relatives au statut (profession, spécialité, situation conventionnelle) ;
– des informations relatives à l'activité (les actes prescrits et exécutés avec leur codage détaillé, les montant des honoraires ou rémunérations perçus).

Le ministère indique que les données précitées sont nécessaires aux organismes gestionnaires des régimes obligatoires de base de l'assurance maladie aux fins d'accomplissement des missions dévolues à leur service médical.

La commission souligne que l'utilisation du NIR doit être cantonnée aux finalités limitativement énumérées à l'article 1er du projet aux fins d'exercice par les organismes gestionnaires de régimes obligatoires de base de l'assurance maladie des missions de sécurité sociale qui leur sont confiées.

Elle rappelle qu'en application des dispositions de l'article 6 (3°) de la loi du 6 janvier 1978 modifiée les données traitées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie.

Sur les destinataires ou catégories de destinataires habilités à recevoir communication de ces données :

L'article 3 du projet prévoit que les données traitées sont accessibles aux agents intervenant dans la prise en charge des assurés et soumis à une obligation de confidentialité, individuellement habilités par le directeur de chaque organisme d'assurance maladie pour l'exercice de leurs missions et dans la stricte mesure nécessaire à l'exercice de celles-ci.

L'article 3 du projet précise que seuls les praticiens-conseils des organismes gestionnaires des régimes obligatoires de base de l'assurance maladie et les personnels placés sous leur autorité sont habilités à accéder, dans le respect des règles relatives au secret médical et dans la stricte mesure où elles sont nécessaires à l'exercice des missions qui leur sont confiées, aux données identifiantes mentionnées à l'article 2 du projet lorsqu'elles sont associées à une pathologie diagnostiquée.

L'article 3 du projet ajoute que lorsque les traitements visés à l'article 1er du projet comportent des données de santé, les agents chargés de leur mise en œuvre sont habilités par médecin-conseil chef du service du contrôle médical compétent et placés sous sa responsabilité pendant toute la durée du traitement.

La commission en prend acte.

Sur la durée de conservation des données :

L'article 4 du projet prévoit des durées de conservation distinctes en fonction des données traitées.

– cinq ans après son décès lorsqu'elles concernent les invalidités et inaptitudes ;
– dix ans après son décès lorsqu'elles concernent les accidents du travail et maladies professionnelles ;
– jusqu'à l'expiration des délais de recours en cas de contentieux ou d'affaire litigieuse.

Lorsqu'il existe un recours contre tiers, les données sont conservées jusqu'à l'intervention de la décision définitive.

Les données relatives à une prestation peuvent être conservées trois ans à partir de la date de remboursement. Au-delà de ce délai, elles peuvent être archivées pendant dix ans dans un environnement logique séparé afin d'assurer une meilleure gestion des actions contentieuses, de la lutte contre la fraude et des recours contre tiers.

L'article 4 du projet précise que l'accès aux données de plus de trois ans sera réservé aux seuls utilisateurs habilités conjointement par le médecin-conseil responsable de l'échelon local du service médical et le directeur de l'organisme dans le cadre du pilotage, de la gestion du risque, du contrôle interne, du contentieux, du recours contre tiers, de la lutte contre la fraude et des activités du service médical.

Enfin, l'article 4 précité prévoit également que l'accès simultané aux données relatives aux pathologies et aux identifiants des bénéficiaires n'est possible que pour les personnes placées sous la responsabilité des médecins-conseils.

La commission prend acte de ce que les durées de conservation prévues à l'article 4 du projet constituent des durées maximales. Elle s'interroge toutefois sur la proportionnalité de certaines durées de conservation déterminées par le présent décret et relève que certaines d'entre elles n'ont pas été justifiées. La commission rappelle que pour chacun des traitements autorisés en application du présent décret, les données doivent être conservées pendant une durée proportionnée à la finalité poursuivie par le traitement, conformément aux dispositions de l'articles 6, 5°, de la loi du 16 janvier 1978 modifiée susvisée.

Elle rappelle que la conservation et l'archivage des données doivent être réalisés dans des conditions de sécurité conformes aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

Elle demande que, passées les durées de conservation prévues à l'article 4 du projet, les données soient archivées sous une forme anonyme ou supprimées.

Sur l'information des personnes concernées :

La commission prend acte de ce que l'article 6 du projet prévoit que les personnes auxquelles se rapportent les données mentionnées à l'article 2 sont informées de la mise en œuvre d'un traitement les concernant, autorisé en application de l'article 1er, de ses finalités ainsi que des modalités d'exercice de leurs droits d'accès et de rectification.

Outre l'information par voie de publication du décret au *Journal officiel* de la République française, elle recommande les modalités d'information suivantes, conformément à l'article 32 de la loi du 6 janvier 1978 modifiée :

– une information par voie d'affichage dans les organismes gestionnaires de régime de base de l'assurance maladie et sur leur site internet ainsi que dans les différents courriers ou courriels adressés aux personnes concernées ;
– une mention dans les livrets d'accueil des établissements susmentionnés.

Sur les droits d'accès, de rectification et d'opposition des personnes concernées :

L'article 5 du projet prévoit que les droits d'accès et de rectification prévus aux articles 39 et 40 de la loi du 6 janvier 1978 susvisée s'exercent auprès du directeur de l'organisme de rattachement des personnes concernées.

La commission en prend acte.

L'article 6 du projet prévoit que le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 précitée ne s'applique pas aux traitements autorisés par le présent décret, ces traitements répondant à une obligation légale.

Sur la sécurité des données et la traçabilité des actions :

La commission prend acte de ce que l'article 7 du projet rappelle, d'une part, que les responsables de traitements doivent prendre *« toutes les mesures nécessaires à la préservation de la sécurité des données tant à l'occasion de leur recueil que de leur consultation »,* conformément à l'article 34 de la loi « Informatique et Libertés » et, d'autre part, qu'il appartient aux responsables de traitement d'attester de la conformité des traitements précités au référentiel général de sécurité (RGS) prévu par le décret n° 2010-112 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

La commission observe que le dossier technique joint à la demande d'avis porte exclusivement sur la méthodologie d'intégration de la sécurité dans les projets mis en œuvre par la CNAMTS.

La commission prend acte de l'engagement du ministère, d'une part, de produire, préalablement à la mise en œuvre du traitement par les autres régimes d'AMO, la documentation technique relative à ces régimes et, d'autre part, de tenir compte des observations qui seraient alors susceptibles d'être formulées par la CNIL.

La commission relève que la méthodologie appliquée par la CNAMTS est strictement cantonnée aux risques de sécurité. La commission demande dès lors que cette analyse porte également sur les risques liés à la vie privée des assurés sociaux.

La commission recommande que chacun des organismes gestionnaires des régimes obligatoires de base de l'assurance maladie développe une méthodologie lui permettant de gérer les risques d'une manière globale, et plus particulièrement les risques sur les libertés et la vie privée de leurs adhérents. Elle demande en outre que cette méthodologie lui soit transmise préalablement à la mise en œuvre des traitements.

Enfin, la commission rappelle que ces méthodologies doivent être régulièrement mises à jour, afin de prendre en compte les évolutions des technologies, et que les études de risques menées pour chacun des projets devront également être revues régulièrement afin, le cas échéant, de mettre à jour les mesures de sécurité initialement prévues.

Sur les formalités à accomplir :

L'article 8 du projet prévoit qu'en application des dispositions du IV de l'article 26 de la loi du 6 janvier 1978 susvisée, le responsable de chacun des traitements de données autorisés sur le fondement du présent décret adresse à la Commission nationale de l'informatique et des libertés, préalablement à sa mise en œuvre, un engagement de conformité aux dispositions du présent décret dans les conditions fixées à l'article 8 du décret n° 2005-1309 du 20 octobre 2005.

La commission en prend acte.

Les autres points du projet n'appellent pas, en l'état et au regard de la loi du 6 janvier 1978 modifiée, d'autres observations.

La présidente,
I. Falque-Pierrotin