Commission nationale de l'informatique et des libertés

Délibération n° 2014-432 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 de leurs missions en matière de lutte contre les fautes, abus et fraudes (demande d'avis n° 14021842)

NOR : *CNIX1508678X*

La Commission nationale de l'informatique et des libertés,

Saisie par le ministère 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 œuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement de leurs missions en matière de lutte contre les fautes, abus et fraudes,

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-I (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 LANDEN, 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 le ministère 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 par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement de leurs missions en matière de lutte contre les fautes, abus et fraudes.

Ce projet vise à créer une catégorie de traitements de données à caractère personnel relevant du processus métier « fraude » de l'assurance maladie obligatoire (AMO) 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 d'assurance maladie des travailleurs salariés (CNAMTS), la Mutualité sociale agricole (MSA) et le Régime social des indépendants (RSI).

Le projet soumis à la commission est pris en application de l'article 27-I (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* ».

L'article R. 115-1 du CSS prévoit 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 sont complétées par celles de l'article R. 115-2 qui précise 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 pas la lutte contre les fautes, abus et fraudes.

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

Sur la dénomination et les finalités des traitements :

Le projet autorise les traitements automatisés de données à caractère personnel destinés à l'exercice des missions qui sont confiées par la loi aux organismes gestionnaires des régimes obligatoires de base de l'assurance maladie en matière de lutte contre les fautes, abus et fraudes.

Ces traitements concernant la lutte contre les fautes, abus et fraudes des assurés et de leurs ayants droit, des bénéficiaires de droits, des employeurs, des tiers, des professionnels et établissements de santé, des établissements médico-sociaux, établissements d'hébergement de personnes âgées dépendantes, des laboratoires d'analyses médicales, des fournisseurs et autres prestataires de services, ou de toute autre personne physique ou morale autorisée à dispenser des soins, à réaliser une prestation de service ou des analyses de biologie médicale ou à délivrer des produits ou dispositifs médicaux, ou contre la fraude interne.

L'article 1er du projet explicite le périmètre et les finalités des traitements mis en œuvre dans le cadre des missions précitées.

Ces traitements ont vocation à poursuivre les finalités suivantes :

- effectuer des requêtes et à produire des statistiques et analyser et suivre des situations administratives, des prestations versées, des soins produits et des biens délivrés, afin de diligenter des contrôles, de prévenir ou d'engager des recours contentieux et, le cas échéant, de lutter contre les fautes, abus et fraudes suspectés ou avérés ;
- effectuer les opérations nécessaires au calcul des indus et des sanctions ; élaborer une cartographie des risques de fautes, abus et fraudes permettant de mieux cibler les dossiers à contrôler ;
- communiquer les informations relatives aux fautes, abus et fraudes aux organismes gestionnaires des régimes obligatoires ;
- signaler les fautes, abus et fraudes suspectés ou avérés et, à cet effet, à transmettre :
  - les informations relatives aux fautes, abus ou fraudes présumés ou avérés aux agents de l'Etat ou aux organismes de protection sociale mentionnés à l'article L. 114-16-3 du code de la sécurité sociale, ainsi le cas échéant qu'à l'organisme d'assurance maladie complémentaire de l'assuré concerné en application du deuxième alinéa de l'article L. 114-9 ;
  - les informations relatives aux fautes, abus ou fraudes présumés ou avérés, après anonymisation, à l'autorité compétente de l'Etat, en application de l'article L. 114-9 du CSS ;
- transmettre à l'établissement de santé, par tout moyen permettant de déterminer la date de réception, le rapport de contrôle prévu à l'article R. 162-42-10 du CSS en application de l'article L. 162-22-18 du CSS ;
- produire les informations recueillies susceptibles de constituer un manquement aux règles de déontologie de la part d'un professionnel de santé inscrit à un ordre professionnel et de les communiquer à l'ordre compétent en application de l'article L. 162-1-19 du code de la sécurité sociale ;
- produire le rapport de synthèse prévu à l'article L. 114-9 du code de la sécurité sociale ;
- suivre les signalements de suspicions de fautes, abus et fraudes afin de diligenter les contrôles, mener les investigations et, le cas échéant, d'engager des actions contentieuses ou des mesure d'accompagnement ;
- suivre les actions contentieuses et les actions de prévention et de lutte contre les fautes, abus et fraudes.

La commission rappelle, conformément à l'article 10 de la loi du 6 janvier 1978 modifiée, qu'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 :

Les catégories de données à caractère personnel traitées concernent les personnes auteurs ou concernés par une faute, un abus ou une fraude présumés ou avérés.

L'article 2 du projet énumère les catégories de données à caractère personnel qui feront l'objet d'un traitement :

- les données d'identification (nom, prénom, sexe, date et lieu de naissance, le numéro de pièce d'identité ou de titre de séjour ; le numéro d'agent, dans le cadre d'une recherche de fraude interne ; le numéro d'identification, la catégorie, la spécialité et le secteur de conventionnement, s'agissant des professionnels de santé) ;
- le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) et celui ou ceux qui leur auraient été précédemment attribués, ou, pour les personnes en instance d'attribution d'un numéro d'inscription au répertoire national d'identification des personnes physiques, un numéro identifiant d'attente (NIA) attribué par la Caisse nationale d'assurance vieillesse des travailleurs salariés à partir des données d'état civil, pour l'ensemble des organismes ;
- les coordonnées (adresse poste, téléphone, adresse électronique) ;
- le pays où les soins ont été délivrés ;
- les informations permettant de décrire les caractéristiques de la faute, de l'abus ou de la fraude (notamment la branche, le service, la prestation ou le droit concerné ; la date des faits et de leur découverte, les modalités de détection ; le domaine de risque ; le type de faute, abus ou fraude ; la nature des documents en cause ;

l'évaluation du montant du préjudice subi ou évité, l'identification des tiers concernés, comportant éventuellement le NIR lorsque cette information est utile aux besoins de l'enquête ; toutes les informations utiles relatives à la prestation ou au droit servi dont le numéro identifiant le séjour en établissement dans le cadre du contrôle des établissements ;

– les informations relatives aux actions engagées par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie (notamment la nature des actions engagées ; le cas échéant, l'autorité saisie ; la mention « procédure en cours » ou « clôturée » et, le cas échéant, la date de clôture ; le cas échéant, les mentions « classement sans suite », « non-lieu » ou « relaxe » ; les mentions de notification d'indu, de signature de transaction, de notification d'une pénalité financière, leur montant et, le cas échéant, leur recouvrement ; les sanctions ordinales).

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 de leurs missions de lutte contre la fraude.

Elle rappelle que les catégories de données traitées doivent être adéquates, pertinentes et non excessives au regard de la finalité poursuivie, conformément aux dispositions de l'article 6 (3°) de la loi du 6 janvier 1978 modifiée et 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 par la loi.

La commission prend acte de l'engagement du ministère de modifier le projet de décret, afin de supprimer le NIR des simples témoins de la liste des données traitées dans le cadre d'une enquête sur une faute, un abus ou une fraude suspectée. Elle prend acte en revanche de ce que le NIR de tiers concernés en tant que victimes ou complices de fraudes est utile afin de rattacher les prestations dues à la bonne personne ou rechercher des prestations indues.

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

L'article 3 du projet prévoit les destinataires des données suivants :

– les agents intervenant dans la prise en charge des assurés et soumis à une obligation de confidentialité, individuellement habilités par le directeur de chaque organisme pour l'exercice de leur mission et dans la stricte mesure nécessaire à l'exercice de celles-ci ;
– les agents de l'Etat ou des organismes de protection sociale mentionnés à l'article L. 114-16-3 du code de la sécurité sociale individuellement habilités par le directeur de l'organisme ou de l'administration concernée ;
– l'autorité compétente de l'Etat, après anonymisation des données en application du premier et du troisième alinéa de l'article L. 114-9 du même code.

La commission en prend acte.

L'article 3 précité précise que, le cas échéant, seuls des praticiens conseils et les personnels placés sous leur autorité ont accès aux données à caractère médical.

La commission demande que cette disposition soit complétée, afin de préciser que l'accès de ces personnels s'effectuera dans le respect des règles du secret médical et dans la stricte mesure où elles sont nécessaires à l'exercice des missions qui leur sont confiées.

Elle rappelle, en outre, que l'accès aux données à caractère personnel requiert la mise en œuvre de règles d'habilitation strictes et une traçabilité des accès associée à une analyse de ces traces, de sorte que les accès non autorisés puissent être identifiés.

Sur la durée de conservation des données :

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

« *I. – Les données enregistrées dans les outils de gestion des alertes seront conservées cinq ans.*

II. – Les données de signalement des fautes, abus et fraudes et anomalies sont conservées :

1° Un an pour les dossiers classés sans suite par l'organisme ou ayant fait l'objet d'une décision de non-lieu ou de relaxe à compter de la date de cette décision ;

2° Un an pour les dossiers classés sans suite par le procureur de la République sauf s'ils font encore l'objet d'une procédure de sanction ou conventionnelle ;

3° Cinq ans à compter de la date de clôture de la procédure contentieuse dans les autres cas.

III. – A l'expiration de leur durée de conservation, les données mentionnées aux I et II sont archivées pour une période de cinq ans à l'exception des données relatives aux dossiers classés sans suite.

IV. – Les données issues de requêtes pour la réalisation du ciblage des dossiers à contrôler seront conservées jusqu'au ciblage suivant sur le même type de faute, abus ou fraude ou la même personne, et pendant une durée qui ne peut excéder trois ans.

V. – Les informations relatives à l'identification des agents ayant accédé aux données enregistrées dans les traitements visés à l'article 1er ou les ayant modifiées, ainsi que les dates, heures et types de ces accès ou modifications, sont conservées durant l'année civile au cours de laquelle l'accès ou la modification a eu lieu et les quatre années civiles suivantes. »

La commission prend acte de l'engagement du ministère de compléter le projet d'une disposition précisant que toute alerte qualifiée de « non pertinente » devra être supprimée sans délai.

La commission prend acte de ce que les durées de conservation prévues à l'article 4 du projet constituent des durées maximales. Elle estime que pour chacun des traitements autorisés en application du présent décret, les données seront conservées pendant une durée proportionnée à la finalité poursuivie par le traitement, conformément aux dispositions des articles 6 (5°) et 36 de la loi du 6 janvier 1978 modifiée susvisée.

La commission relève toutefois qu'en l'absence d'éléments de justification de certaines des durées de conservation précitées, notamment celles afférentes aux traces des accès aux données enregistrées, elle n'est pas en mesure d'apprécier la proportionnalité des durées de conservation retenues au regard des finalités poursuivies par les traitements.

Elle prend acte néanmoins de ce que, passées les durées de conservation précitées, les données seront archivées sous une forme anonyme ou supprimées et rappelle que ces opérations doivent être réalisées selon des modalités conformes aux dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée.

Sur l'information des personnes concernées :

La commission prend acte de ce que l'article 5 du projet prévoit que les personnes physiques ou morales sont informées de la mise en œuvre de traitements de données à caractère personnel les concernant destinés au contrôle et à la lutte contre la fraude par diffusion d'une information sur le site internet de l'assurance maladie AMELI et sur les sites internet respectifs des organismes gestionnaires des régimes obligatoires de base de l'assurance maladie. Elle recommande que l'information des personnes concernées s'effectue dans les différents courriers ou courriels adressés aux personnes concernées.

La commission relève que les personnes concernées par les données traitées seront informées de l'existence d'un traitement les concernant, de ses finalités et des modalités d'exercice de leurs droits. Elle rappelle qu'en application de l'article 32 de la loi du 6 janvier 1978 modifiée cette information doit également porter sur l'identité du responsable de traitement, les destinataires ou catégories de destinataires des données, Elle demande que le projet soit complété en ce sens.

Outre cette information générale, la commission estime que, passé un délai maximum de six mois d'investigations, en cas de confirmation de l'anomalie et de décisions produisant des effets juridiques, la personne susceptible d'être inscrite sur une liste de personnes présentant un risque de fraude doit être informée individuellement par écrit desdites conséquences en lui donnant la possibilité de présenter ses observations.

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

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

La commission en prend acte.

L'article 8 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, en l'espèce, aux traitements autorisés par le présent décret.

Sur la sécurité des données et la traçabilité des actions :

La commission prend acte de ce que l'article 9 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 7 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