Commission nationale de l'informatique et des libertés

Délibération n° 2014-429 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 prévention, d'indemnisation et de tarification des accidents du travail et maladies professionnelles (demande d'avis n° 14021842)

NOR : *CNIX1508684X*

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 œuvre par les organismes gestionnaires des régimes obligatoires de base de l'assurance maladie pour l'accomplissement de leurs missions en matière de prévention, d'indemnisation et de tarification des accidents du travail et maladies professionnelles,

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 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 10 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 de leurs missions en matière de prévention, d'indemnisation et de tarification des accidents du travail et maladies professionnelles.

Ce projet vise à créer une catégorie de traitements de données à caractère personnel relevant des missions en matière d'accidents du travail et de maladies professionnelles 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 de l'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* ».

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 de la relation avec les bénéficiaires de la législation accidents du travail et maladies professionnelles, 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 décret en Conseil d'Etat pris après avis de la CNIL, en application de l'article 27-I (1°) précité.

Sur la dénomination et la finalité des traitements :

Le projet est relatif à la mise en œuvre de traitements de données à caractère personnel destinés à la prise en charge des victimes d'accidents du travail et des maladies professionnelles, à la tarification des cotisations des entreprises et au développement de la prévention.

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 :

« 1° D'assurer la réception et l'enregistrement des informations utiles au traitement des certificats médicaux, des déclarations d'accidents de travail ou des déclarations de maladie professionnelle ;

2° D'assurer la gestion de la relation avec les bénéficiaires de la législation accidents du travail et maladies professionnelles, par courrier postal ou électronique, par messages téléphoniques, par services d'accueil téléphonique ou physique et par télé-services ;

3° D'assurer la tarification du risque accident du travail et maladies professionnelles et le versement des prestations dues en cas d'accident du travail et de maladie professionnelle ;

4° De contribuer à la sécurité du versement des prestations et à la prévention et à la lutte contre les fautes, abus et fraudes ainsi qu'à la gestion et au suivi des recours gracieux et des actions contentieuses ;

5° De permettre la mise en œuvre d'échanges d'informations entre organismes gestionnaires d'un même régime et avec les autres organismes intervenant dans le domaine de la protection sociale, de l'assurance vieillesse, de l'indemnisation du chômage, du recouvrement, ainsi qu'avec les services des ministères chargés de la sécurité sociale, de l'agriculture et du travail et avec l'administration fiscale.

6° D'effectuer des requêtes et de produire des statistiques à partir des données relatives aux accidents du travail et maladies professionnelles, dans un but de pilotage, de mise en œuvre de la politique ou des politiques de gestion du risque et de prévention, d'analyse des prestations versées et des soins pris en charge, d'évaluation de la qualité du service rendu aux usagers, de contrôle, de prévention et de traitement des recours gracieux et contentieux, et le cas échéant, de lutte 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 prend acte de ce que le projet de décret sera complété sur ce point.

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

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.

Sur les catégories de données à caractère personnel enregistrées :

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

Ces catégories de données à caractère personnel concernent les victimes d'accidents du travail ou de maladies professionnelles, leurs ayants droit et les bénéficiaires de l'article 41 de la loi n° 98-1194 du 23 décembre 1998, les professionnels de santé, les employeurs et les personnes mentionnées à l'article L. 752-1 du code rural et de la pêche maritime, les tiers impliqués ou témoins d'accidents.

L'article 2 du projet prévoit le traitement des catégories de données à caractère personnel suivantes :

– des informations d'identification des victimes d'accidents du travail ou de maladies professionnelles, leurs ayants droit et les bénéficiaires de l'article 41 de la loi 98-1194 du 23 décembre 1998 (leurs noms de famille, d'usage, prénoms, sexe, date et lieu de naissance, le cas échéant, la date de décès et la justification de la qualité d'ayant droit, le NIR ou NIA, la nationalité lorsqu'elle est détermine l'application d'une convention bilatérale ou la qualité de ressortissant d'un pays de l'Union européenne ou d'un pays non-membre de l'Union européenne, l'adresse postale et électronique, numéro de téléphone, des informations relatives à l'organisme de rattachement, au régime d'affiliation et à l'étendue des droits au remboursement, à l'assurance maladie complémentaire, les données de santé nécessaires à la mise en œuvre des finalités définies à l'article 1er du projet, les données relatives à la vie professionnelle nécessaires à la mise en œuvre des finalités définies à l'article 1er du projet, les données relatives aux salaires nécessaires à la détermination du montant des prestations, les coordonnées bancaires et numéro de sinistre) ;
– des informations d'identification des professionnels de santé (nom, prénom et adresse professionnelle, numéro d'identification professionnel, situation conventionnelle, profession et spécialité) ;
– des informations d'identification des employeurs et des personnes mentionnées à l'article L. 752-1 du code rural et de la pêche maritime (leurs nom, prénom, la raison sociale, le numéro SIRET, l'adresse

professionnelle, ta catégorie de risque « accident du travail » de l'entreprise ou de la victime, le nombre de salariés de l'entreprise, le montant de la masse salariale de l'entreprise) ;

– des informations d'identification relatives aux tiers impliqués ou témoins d'accidents (leur nom, prénom, adresse et coordonnées de leur compagnie d'assurance du tiers impliqué) ;
– des informations relatives aux circonstances de l'accident de travail et de trajet (l'heure et lieu de l'accident, l'activité liée à l'accident, la tâche effectuée au moment de l'accident, l'élément matériel, le mouvement, la nature et le siège de la lésion) ;
– des informations relatives aux maladies professionnelles (ia maladie professionnelle, l'agent causal, la durée d'exposition au risque et la profession de la victime) ;
– des informations relatives aux conséquences des accidents et maladies professionnelles (la date de guérison ou de consolidation, le résumé des séquelles, le taux d'incapacité permanente, le taux d'incapacité révisé et sa date de révision, la date de guérison et de rechute).

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 en matière de prévention, d'indemnisation et de tarification des accidents du travail et maladies professionnelles.

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 par la loi.

La commission rappelle qu'en application des dispositions 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 des 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, d'une part, que 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 aux données relatives à la santé des bénéficiaires nécessaires à la mise en œuvre des finalités décrites à l'article 1er (ces données sont visées à l'article 2 (1°, *g*).

La commission estime que l'article 3 pourrait être complété par les mentions « dans le respect des règles relatives au secret médical ». L'article 3 précise, d'autre part, que, dans la stricte mesure où ces données sont indispensables à l'accomplissement de leurs missions en matière d'accident du travail et de maladie professionnelle, les personnels administratifs des organismes d'assurance maladie obligatoire chargés de telles missions accèdent à ces données.

La commission rappelle que les accès aux données doivent s'effectuer dans des conditions conformes à la loi du 6 janvier 1978 modifiée.

La commission relève qu'en matière d'avis d'arrêts de travail le volet comportant les éléments d'ordre médical est adressé au service médical de l'organisme dont dépend l'assuré social.

Elle relève, en outre, que, dans sa décision n° 99-422 DC du 21 décembre 1999 relative à la loi de financement de la sécurité sociale pour 2000, le Conseil constitutionnel a jugé, s'agissant de l'article L. 162-4-1 du CCS, que la motivation médicale des prescriptions d'arrêts de travail et de transports sanitaires ne constitue pas en soi une atteinte au secret médical constitutive d'une violation du principe du respect de la vie privée. Le Conseil constitutionnel considère que, sous réserve de l'accès limité aux médecins-conseils des caisses et des modalités d'acheminement assurant la confidentialité des données, l'article L. 162-4-1 ne porte pas atteinte au respect de la vie privée.

Dès lors, la commission s'interroge sur la rédaction telle que prévue dans le projet de décret en ce qu'elle ne soumet pas l'accès par les personnels administratifs aux données de santé nominatives contenues dans les certificats médicaux au même formalisme que celui prévu par les dispositions relatives aux arrêts de travail.

La commission 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.

En outre, l'article 5 du projet prévoit l'échange des informations et des données visées à l'article 2 entre les organismes chargés de la gestion d'un régime de protection sociale, les organismes chargés de la gestion de prestations de nature sociale, les services du ministère chargé de la sécurité sociale, du ministère chargé de l'agriculture, du ministère du travail ou de l'administration fiscale.

La commission, si elle ne peut que souscrire à la légitimité des objectifs poursuivis par le projet, s'interroge sur la légitimité de la transmission de certaines informations à certains des organismes précités.

Elle prend acte, d'une part, de ce que le projet, dans sa version transmise le 10 octobre 2014, précise que les services de l'administration fiscale ne seront pas destinataires du NIR, ni du NIA et, d'autre part, qu'il résulte des échanges entre ses services et ceux du ministère que la direction générale du travail (DGT), la direction de la sécurité sociale (DSS) et la direction de la recherche, des études, de l'évaluation et des statistiques (DRESS), ainsi que des organismes placés sous leur tutelle, reçoivent des données agrégées relatives aux accidents du travail et

maladies professionnelles. La commission prend également acte de ce que la DGT et les inspecteurs du travail peuvent être destinataires de données non agrégées (en particulier des déclarations d'accident du travail).

La commission rappelle toutefois que les échanges d'informations ne devront porter que sur les données strictement nécessaires et proportionnées à la finalité poursuivie dans le cadre des missions des organismes précités et que ces échanges devront s'effectuer dans des conditions conformes aux lois et règlements en vigueur. Elle prend acte de ce que le projet sera complété afin de préciser, par catégories de destinataires, la liste des données à caractère personnel auxquelles ces derniers auront accès et rappelle que ceux-ci devront être individuellement habilités, au sein de leurs organismes d'appartenance, à recevoir des données.

Sur la durée de conservation des données :

L'article 4 du projet prévoit les durées de conservation suivantes :

– vingt ans après le décès de la victime, en l'absence d'ayant droit ;
– cinq ans après l'extinction des droits du dernier survivant parmi les ayants droit de la victime ;
– cinq ans après l'expiration des délais de recours, dans le cadre de la gestion du contentieux.

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 projet et relève que certaines d'entre elles n'ont pas été justifiées.

La commission rappelle que, pour chacun des traitements autorisés en l'espèce, les données doivent être conservées pendant une durée proportionnée à la finalité poursuivie par le traitement, conformément aux dispositions des articles 6 (5°) de la loi du 6 janvier 1978 modifiée susvisée.

Elle rappelle également 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. Elle prend acte de ce que le projet sera complété sur ce point.

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 6 du projet prévoit que le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 modifiée ne s'applique pas aux traitements autorisés par le présent décret.

L'article 6 du projet prévoit que les droits d'accès et de rectification s'exercent auprès du directeur de l'organisme de rattachement.

La commission prend acte de ce que la mention « prévus aux articles 39 et 40 de la loi du 6 janvier 1978 susvisée » sera ajoutée au projet.

Sur la sécurité des données et la traçabilité des actions :

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