Commission nationale de l'informatique et des libertés

Délibération n° 2016-325 du 3 novembre 2016 portant avis sur un projet d'arrêté relatif au traitement automatisé de données à caractère personnel dénommé « Portail de signalement des événements sanitaires indésirables » (demande d'avis n° 16016139)

NOR : *CNIX1706773X*

La Commission nationale de l'informatique et des libertés,

Saisie par la ministre des affaires sociales et de la santé d'une demande d'avis concernant un projet d'arrêté relatif au traitement automatisé de données à caractère personnel dénommé « Portail de signalement des événements sanitaires indésirables » ;

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 de la santé publique ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 27-II (4°) ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 modifiée relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

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 ;

Vu le décret n° 2016-1151 du 24 août 2016 relatif au portail de signalement des événements sanitaires indésirables ;

Après avoir entendu M. Alexandre LINDEN, commissaire, en son rapport, et Mme Nacima BELKACEM, commissaire du Gouvernement, en ses observations,

Emet l'avis suivant :

La Commission a été saisie par la ministre des affaires sociales et de la santé d'un projet d'arrêté relatif au « Portail de signalement des événements sanitaires indésirables » (ci-après « le projet »), en application de l'article D. 1413-58 du code de la santé publique (CSP) créé par le décret n° 2016-1151 du 24 août 2016 relatif au portail de signalement des événements sanitaires indésirables. Le projet est par ailleurs accompagné d'un second projet d'arrêté fixant la liste des systèmes de vigilance, veille et surveillance sanitaires réglementés pour lesquels la déclaration des effets ou événements indésirables, manifestations nocives chez la personne, peut s'effectuer au moyen du« Portail de signalement des événements sanitaires indésirables », qui constitue un téléservice au sens des dispositions de l'article 27-II (4°) de la loi du 6 janvier 1978 modifiée (ci-après la « loi Informatique et Libertés »).

Sur les finalités du traitement :

L'article 1er du projet prévoit que le traitement a pour finalités :

« 1° De promouvoir le signalement d'événements indésirables sanitaires en mettant à la disposition du public et des professionnels un service d'information sur les vigilances, les déclarations et de manière générale sur la veille et la sécurité sanitaire ;

2° D'orienter le public, les professionnels des secteurs sanitaire et médico-social et les industriels vers le formulaire permettant de déclarer l'événement sanitaire constaté et relevant des systèmes de vigilances, veille et surveillance réglementés figurant sur la liste mentionnée au premier alinéa de l'article D. 1413-58 du code de la santé publique ou vers le formulaire destiné à recueillir les déclarations d'événements sanitaires ne relevant pas d'un système de vigilances, de veille ou de surveillance réglementé et relevant de la compétence des agences régionales de santé ;

3° De transmettre les signalements ainsi déclarés aux professionnels chargés de leur traitement ou évaluation ;

4° D'assurer l'information des déclarants sur le traitement de leur déclaration et, s'il s'agit de professionnels de santé, de mettre à leur disposition un espace personnel comprenant un historique de leurs déclarations. »

La Commission relève que le portail n'a pas pour finalité de permettre à l'ASIP Santé d'assurer une mission de vigilance, qui reste ainsi dévolue aux organismes compétents pour connaître des effets et événements sanitaires indésirables.

A ce titre, la Commission rappelle que les traitements réalisés par les agences et organismes chargés de la gestion des déclarations doivent faire l'objet de formalités préalables spécifiques auprès d'elle.

Elle considère, par ailleurs, que les finalités prévues par le projet sont déterminées, légitimes et explicites conformément aux dispositions de l'article 6-2° de la loi Informatique et Libertés.

Sur les données à caractère personnel traitées :

L'article 2 du projet envisage le traitement des données à caractère personnel suivantes :

« *1° Données contenues dans les formulaires de signalement des événements déclarés dans le cadre des systèmes de vigilances, veille et surveillance réglementés figurant sur la liste mentionnée* à *l'article D. 1413-58 du code de la santé publique et comprenant notamment :*

a) *Données relatives* à *l'identification de la personne faisant l'objet du signalement de l'événement indésirable ou numéro d'identification de la personne permettant de garantir son anonymat, description de l'événement et de sa gravité, de sa cause potentielle et tout élément nécessaire à assurer l'évaluation ou le traitement de l'événement ;*

b) *Données relatives à l'identification des déclarants : adresse électronique et numéro de téléphone, nom, prénoms et numéro d'inscription au répertoire partagé des professionnels de santé (RPPS), le cas échéant.*

2° Données contenues dans les espaces personnels des utilisateurs :

a) *Données relatives à l'identification des déclarants mentionnées au* b *du 1° ;*

b) *Données relatives à l'identification du professionnel chargé de l'évaluation ou du traitement de l'événement : adresse électronique et numéro de téléphone, nom, prénoms et numéro d'inscription au répertoire partagé des professionnels de santé (RPPS), le cas échéant, et structure de rattachement ;*

c) *Données relatives à l'identification des gestionnaires de compte et administrateurs : adresse électronique et numéro de téléphone, nom, prénoms et structure de rattachement.* »

La Commission suggère de supprimer le terme « notamment » dans le 1° de l'article 2, afin que la liste de catégories de données établie par le projet d'article 2 soit limitative. Elle propose également qu'une distinction soit opérée entre les données d'identification et les autres catégories de données susceptibles de faire l'objet d'un traitement et que le projet soit complété afin d'y voir figurer l'ensemble des catégories de données pouvant faire l'objet d'un traitement dans le cadre de la mise en œuvre du portail.

La Commission observe en outre que le 1-a de l'article 2 du projet fait référence à un « *numéro d'identification de la personne permettant de garantir l'anonymat* » des personnes concernées. Or, si le portail ne permet pas un accès à des données directement identifiantes, les personnes sont identifiées par le biais d'un numéro d'identification détenu par le déclarant.

Elle prend acte de ce que le ministère s'est engagé à remplacer, dans l'article 2-1-a du projet, le terme d'anonymat par ceux de protection de la vie privée.

En outre, la Commission relève que le 2° de l'article 2 entend dresser la liste des données contenues dans les espaces personnels des utilisateurs. Or, les données énumérées par la suite sont relatives à l'identification du déclarant, à l'identification du professionnel chargé de l'évaluation ou du traitement de l'événement et à l'identification des administrateurs fonctionnels et techniques.

Elle suggère de compléter le projet afin que le 2° de l'article 2 mentionne l'ensemble des catégories de données traitées dans les espaces personnels, en ajoutant les données des formulaires de déclaration accessibles pour les professionnels de santé chargés de l'évaluation de l'événement.

Sous ces réserves, la Commission considère que ces données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, conformément aux dispositions de l'article 6-3° de la loi Informatique et Libertés.

Sur les destinataires des données :

L'article 3 du projet prévoit que sont destinataires des données à caractère personnel, à l'exception des données relatives à l'identification des gestionnaires de comptes et des administrateurs, les agents nommément désignés et habilités par le directeur ou le responsable des établissements publics et organismes visés par le projet, soumis au secret professionnel, dans la stricte mesure où elles sont nécessaires à l'exercice des missions qui leurs sont confiées.

Les établissements publics et organismes visés sont les suivants :

- l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES) ;
- l'Agence nationale de santé publique (ANSP) ;
- l'Agence de la biomédecine (ABM) ;
- les agences régionales de santé (ARS) ;
- l'Agence nationale de sécurité du médicament et des produits de santé (ANSM) ;
- les organismes composant le réseau régional de vigilances et d'appui mentionné à l'article L. 1435-12 du code de la santé publique pour le traitement des signalements, composé de :
  - l'Institut national de veille sanitaire (INVS), qui a fusionné avec l'Institut national de prévention et d'éducation pour la santé (LNPES) et l'Etablissement de préparation et de réponse aux urgences sanitaires (EPRUS) pour constituer I'ANSP ; et
  - l'ensemble des agences susmentionnées.

Les agents visés sont nommément désignés et habilités à cet effet par le directeur ou le responsable de chacun de ces organismes, dans la stricte mesure où l'accès à ces données est nécessaire à l'exercice des missions qui leur sont confiées.

A cet égard, l'article 3 du projet indique que l'accès aux données intervient dans le respect des règles garantissant la confidentialité des informations couvertes par le secret médical.

Ce même article prévoit en outre que l'ASIP Santé est autorisée à accéder aux données mentionnées au 2° de l'article 2 relatives aux utilisateurs possédant un espace personnel, aux données de traçabilité des actions effectuées dans le portail et aux données nécessaires à l'élaboration des indicateurs de pilotage et de suivi du fonctionnement du portail.

Ces destinataires n'appellent pas d'observation de la part de la Commission.

Sur l'information et les droits des personnes concernées :

L'article 6 du projet prévoit que l'ASIP Santé met en œuvre une information du public sur la création du traitement, ses finalités et les droits des personnes concernées et précise que les droits d'accès et de rectification des données s'exercent auprès de l'ASIP Santé.

A cet égard, la Commission prend acte de ce que le ministère s'est engagé à compléter le projet afin qu'il mentionne que les droits d'accès et de rectification pourront être exercés auprès du correspondant informatique et libertés de l'ASIP Santé, conformément aux dispositions de l'article 29-2° de la loi Informatique et Libertés.

L'article 6 du projet précise également que le droit d'opposition prévu à l'article 38 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ne s'applique pas au présent traitement.

Sur la conservation des données :

L'article 4 du projet prévoit que *« les données contenues dans les formulaires de déclaration des effets ou événements indésirables et les données relatives à l'identification des déclarants sont conservées pendant la durée nécessaire à leur transmission au professionnel chargé de leur évaluation ou de leur traitement, à l'exclusion des données relatives au numéro RPPS, au type de déclaration, à la date de déclaration et au service en charge de l'évaluation, qui sont conservées pendant une durée d'un an afin de permettre au déclarant disposant d'un espace personnel de consulter l'historique des déclarations qu'il a effectuées »*.

Les données d'historique sont ensuite archivées à titre de preuve pendant une durée correspondant à la durée de la prescription en matière de responsabilité médicale.

Concernant les données contenues dans les formulaires de déclaration, elles ne sont pas conservées par le portail au-delà de sa fonction de collecte et de transmission. Leur archivage relève, comme c'est le cas actuellement, de chaque évaluateur, dans le respect du délai applicable à la vigilance concernée.

Concernant la durée de conservation des traces relatives à l'utilisation du portail, la Commission prend acte de ce que le ministère s'est engagé à compléter le projet afin qu'il mentionne la durée de six mois établie dans le dossier technique joint au projet.

La Commission considère que ces durées ne sont pas excessives au regard des finalités du traitement, conformément aux dispositions de l'article 6-5° de la loi Informatique et Libertés.

Sur la sécurité :

Compte tenu de la sensibilité des données traitées dans le cadre de la mise en œuvre du portail, la Commission rappelle qu'il convient d'être particulièrement vigilant sur les mesures de sécurité envisagées.

La Commission rappelle tout d'abord que le traitement étant un téléservice d'une autorité administrative au sens de l'ordonnance n° 2005-1516 du 8 décembre 2005 susvisée, il doit être conforme au référentiel général de sécurité (RGS) prévu par le décret n° 2010-112 du 2 février 2010 susvisé. Elle rappelle qu'il revient au responsable de traitement d'attester formellement de la sécurité de celui-ci au travers d'une homologation RGS et d'en publier l'attestation d'homologation sur le site du téléservice.

Le portail est un système flexible disposant de plusieurs modes de fonctionnement structurés par un questionnaire d'orientation du déclarant. En fonction du type de signalement, déterminé grâce aux questions, et de l'existence de dispositifs pour sa prise en charge, le portail a tout d'abord un rôle d'orientation de l'utilisateur vers un service de télédéclaration existant ou vers un acteur habilité à utiliser ce dernier.

Dans les autres cas, le portail propose des formulaires de saisie dédiés et se charge d'acheminer les informations recueillies vers les acteurs adéquats. Cette transmission peut alors se faire de trois manières :

- par échange automatisé de données avec le système d'information destinataire (pour l'instant, ce mode est prévu à destination des ARS uniquement) ;
- par envoi via la messagerie sécurisée de santé (MSSanté) de l'ASIP Santé, à destination d'un utilisateur nommé ou d'un compte de service dont les accès sont nominatifs et gérés par le responsable du service ;
- par envoi d'un courriel invitant le destinataire à se connecter à son espace personnel sur le portail pour y récupérer les données.

Dans ce dernier cas, un mécanisme de relance du destinataire est prévu afin d'éviter une conservation des déclarations sur une durée indéterminée.

Différents profils d'utilisateurs sont identifiés en fonction des rôles :

- déclarants {grand public ou professionnels de santé) ;
- évaluateurs devant traiter les déclarations ;
- gestionnaire de comptes ;
- administrateur du portail.

L'article 5 du projet prévoit que *« les moyens d'authentification des personnes habilitées à accéder aux données en application de l'article 3 sont spécifiques* à *chaque catégorie d'utilisateurs du Portail* ».

Les modes d'accès, d'authentification et d'habilitation sont ainsi adaptés aux profils d'utilisateurs et aux fonctionnalités proposées :

– déclaration simple pour le grand public, sans création d'un espace personnel mais avec un accusé de transmission précisant les structures destinataires ;
– espace personnel « déclarant » pour la saisie et de suivi des déclarations, avec authentification par carte de professionnel de santé (CPS) ;
– espace personnel « évaluateur » (hors échanges automatisés et MSSanté) pour l'acquittement des déclarations reçues et leur récupération par exportation des données, avec authentification forte par CPS ou une alternative par identifiant, mot de passe et *One Time Password* (OTP).

A cet égard, la Commission relève que l'article L. 1110-4 du code de la santé publique issu de la loi du 26 janvier 2016 de modernisation de notre système de santé ne prévoit plus l'authentification par CPS ou dispositif équivalent agréé par l'ASJP Santé et que le nouvel article L. 1110-4-1 du même code renvoie ces modalités d'authentification à la conformité à des référentiels d'interopérabilité et de sécurité approuvés par le ministre en charge de la santé après avis de la CNIL.

Dans l'attente de la publication des textes réglementaires permettant l'entrée en vigueur de ces nouvelles dispositions, la Commission suggère que l'authentification des professionnels de santé intervienne au moyen d'une CPS ou d'un dispositif équivalent agréé par I'ASIP santé.

Les comptes des évaluateurs sont gérés par des gestionnaires de comptes porteurs de CPS ou de carte de personnel autorisé (CPA). Ces gestionnaires ont accepté la responsabilité de la fiabilité des données et moyens d'authentification des personnes dont ils gèrent le compte et peuvent ainsi créer des comptes pour des évaluateurs non équipés d'une CPS.

Les comptes des gestionnaires de comptes sont gérés par l'ASIP Santé en tant qu'administrateur du portail, depuis son réseau privé. A ce titre, l'ASIP Santé dispose également d'un accès aux indicateurs de pilotage et d'évaluation du fonctionnement du portail (nombre de déclarations par vigilance, par région, etc.) afin de réaliser des statistiques et des tableaux de bord.

La Commission recommande que les permissions d'accès soient attribuées pour une durée déterminée, après validation hiérarchique, qu'elles soient supprimées pour tout utilisateur n'étant plus habilité et qu'une revue globale des habilitations soit opérée régulièrement.

Elle recommande également de formaliser les obligations et les conditions de sécurité de données chez les destinataires des déclarations, par le biais de l'acceptation des conditions générales d'utilisation par les utilisateurs et par des conventions signées avec les structures auxquelles ils appartiennent.

L'accès au téléservice est sécurisé au moyen du protocole HTTPS/TLS et la messagerie de santé utilise des canaux de communication chiffrés. Les données du portail sont stockées chez un hébergeur agréé de données de santé (HDS), soustraitant de l'ASIP Santé. Les données et les sauvegardes sont chiffrées par l'hébergeur.

L'article 5 prévoit également que « *les données permettant l'authentification des personnes habilitées à accéder aux données en application de l'article 3 sont strictement séparées* des *autres données. Le système assure la traçabilité des actions effectuées sur ces données* ».

Une journalisation des opérations de consultation, création, modification et suppression du traitement est réalisée. Les traces techniques sont en lecture seule et leur intégrité est vérifiée par un calcul d'empreinte avec une fonction de hachage.

En complément, la Commission recommande de réaliser un contrôle des traces de manière automatique, afin de détecter les comportements anormaux et lever des alertes.

Elle rappelle également que les mesures de sécurité doivent être matérialisées dans une politique de sécurité propre au traitement et faire l'objet de contrôles et de révisions réguliers au vu des évolutions du traitement, de son usage et de son environnement.

Les autres dispositions du projet n'appellent pas d'observations de la part de la Commission.

La présidente,
I. FALQUE-PIERROTIN