Commission nationale de l'informatique et des libertés

Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552)

NOR : *CNIX1909667X*

La Commission nationale de l'informatique et des libertés,

Saisie par la ministre des solidarités et de la santé d'une demande d'avis concernant un projet de décret en Conseil d'Etat modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement ;

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 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 ;

Vu la directive 2016-680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données et abrogeant la décision cadre 2008/977/JAI du Conseil ;

Vu le code de procédure pénale, notamment son article 706-135 ;

Vu le code de la santé publique, notamment ses articles L. 1110-4, L. 3212-1, L. 3213-1, L. 3213-7, L. 3214-3

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

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 du 5 mars 2015 portant création d'un traitement automatisé de données à caractère personnel dénommé « Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste » (FSPRT) ;

Vu le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement ;

Vu l'instruction n° SG/2016/14 du 8 janvier 2016 relative au cadre d'intervention des agences régionales de santé s'agissant des phénomènes de radicalisation ;

Vu l'instruction n° SG/2016/377 du 2 décembre 2016 relative à la déclinaison de la stratégie territoriale du ministère des affaires sociales et de la santé par les ARS dans le cadre de la prévention et de la prise en charge de la radicalisation ;

Vu la délibération n° 2018-152 du 3 mai 2018 portant avis sur un projet de décret autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement ;

Vu le dossier et ses compléments ;

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

Émet l'avis suivant :

La Commission a été saisie par la ministre des solidarités et de la santé d'une demande d'avis modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement. Ces traitements, dénommés HOPSYWEB et gérés par les agences régionales de santé (ARS), ont pour finalité d'assurer au niveau départemental le suivi des personnes en soins psychiatriques sans consentement prises en charge en application des articles L. 3212-1, L. 3213-1, L. 3213-7, L. 3214-3 du code de la santé publique et de l'article 706-135 du code de procédure pénale.

Les modifications projetées visent à mettre en relation les traitements HOPSYWEB avec le FSPRT et ainsi permettre notamment aux préfets de département et, à Paris, au préfet de police du lieu d'hospitalisation d'être informés, aux fins de prévention de la radicalisation, de l'éventuelle hospitalisation sans consentement d'une personne qui serait également enregistrée dans le FSPRT.

Si l'interconnexion projetée doit permettre, dans un contexte général de prévention des risques liés à la radicalisation des personnes atteintes de troubles psychiatriques, d'améliorer les modalités de transmission aux préfets des informations relatives aux admissions en soins psychiatriques sans consentement, la Commission souligne la différence profonde d'objet entre les deux fichiers en présence, l'un faisant état d'antécédents psychiatriques d'une certaine gravité, l'autre ayant la nature d'un fichier de renseignement. Une telle mise en relation ne peut être envisagée qu'avec une vigilance particulière.

Elle rappelle par ailleurs que dans la mesure où certaines informations contenues dans HOPSYWEB sont couvertes par le secret médical, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données personnelles doivent être mises en œuvre. La Commission estime à cet égard que des mesures juridiques et techniques adaptées doivent être prévues afin d'assurer un haut niveau de protection des données.

Sur la nouvelle finalité des traitements HOPSYWEB et le régime juridique applicable :

En premier lieu, la Commission rappelle que les traitements HOPSYWEB, sur lesquels elle s'est déjà prononcée, visent à assurer le suivi des personnes faisant l'objet de soins psychiatriques sans consentement en permettant la gestion administrative des mesures associées. Elle indique que cette gestion est confiée aux ARS dans le cadre des protocoles départementaux établis avec les préfets de département et, à Paris, avec le préfet de police.

Or, la Commission relève que le projet de décret vise à modifier les finalités poursuivies par les traitements HOPSYWEB en ajoutant une finalité nouvelle de prévention de la radicalisation. En effet, l'article 1er du décret n° 2018-383 du 23 mai 2018 est ainsi complété : « *ces traitements de données à caractère personnel ont pour finalité le suivi des personnes faisant l'objet de soins psychiatriques sans consentement en permettant (...) l'information du représentant de l'Etat sur l'admission des personnes en soins psychiatriques sans consentement nécessaire aux fins de prévention de la radicalisation, dans les conditions prévues au livre II de la troisième partie du code de la santé publique susvisé et de l'article 706-135 du code de procédure pénale* ». Cette nouvelle finalité se traduit par une interconnexion, prévue par le projet de décret selon les modalités décrites ci-après, entre les traitements HOPSYWEB et le FSPRT

Dans le cadre notamment de la mise en œuvre du plan national pour la radicalisation, le ministère estime en effet que cette information doit permettre au préfet de département et, à Paris, au préfet de police, de savoir de manière rapide et certaine qu'une personne suivie au titre de la radicalisation, y compris dans un autre département, fait l'objet ou a fait l'objet d'une hospitalisation sans consentement dans le ressort départemental dont il a la charge dans un contexte de risque terroriste élevé.

La Commission observe, qu'en pratique, les préfets pourront ainsi être en mesure d'identifier les personnes susceptibles de présenter, en raison d'une pathologie psychiatrique préexistante ayant donné lieu à une mesure d'hospitalisation sans consentement, des risques potentiels d'atteinte à la sûreté des personnes ou à l'ordre public. A ce titre, le ministère a en effet précisé que si cette information vise à améliorer la prévention des risques liés à la radicalisation des personnes atteintes de troubles psychiatriques en assurant un meilleur suivi de ces dernières, elle doit également leur permettre de décider de la mise en place d'actions appropriées à mener au regard des informations déjà enregistrées dans le FSPRT.

Sans remettre en cause la légitimité de cette nouvelle finalité, la Commission estime que le traitement conserve sa finalité principale de suivi des personnes faisant l'objet de soins psychiatriques sans consentement et qu'à cet égard, la prévention des risques liés à la radicalisation des personnes atteintes de troubles mentaux ne constitue qu'une finalité secondaire. L'interconnexion projetée avec le FSPRT n'a pas pour effet de modifier les caractéristiques principales poursuivies par les traitements HOPSYWEB, dont l'objectif général est d'homogénéiser et de sécuriser les pratiques en matière d'hospitalisation sans consentement.

Par suite, l'ajout de la nouvelle finalité et l'interconnexion envisagée n'ont pas pour effet d'attraire les traitements HOPSYWEB dans le champ des traitements intéressant la sûreté de l'Etat ou la défense au sens des dispositions de l'article 26-I-2° de la loi du 6 janvier 1978 modifiée. Les traitements HOPSYWEB n'entrent pas davantage dans le champ d'application de la directive 2016/680 du 27 avril susvisée.

Compte tenu de ce qui précède, la Commission estime que les conditions de mise en œuvre de ces traitements doivent être examinées au regard des dispositions du RGPD précité. Elle rappelle que, conformément à l'article 9-4 du RGPD, des dispositions spécifiques ont été adoptées en droit national s'agissant des traitements portant sur des données de santé. Dans ces conditions, la Commission rappelle qu'il y a également lieu de faire application des dispositions de la loi du 6 janvier 1978.

Sur l'interconnexion des traitements HOPSYWEB avec le FSPRT :

La Commission relève que l'ajout de la nouvelle finalité de prévention des risques liés à la radicalisation des personnes atteintes de troubles mentaux implique que les traitements HOPSYWEB soient interconnectés avec le FSPRT. A ce titre, l'article 2 du projet de décret prévoit qu'aux fins d'information du préfet de département et, à Paris, du préfet de police, pour la prévention de la radicalisation, *« les données d'identification* (des traitements HOPSYWEB) *visées aux 1° de l'article 2* (nom, prénoms, domicile, sexe, date et lieu de naissance) *peuvent faire l'objet d'une mise en relation avec les données d'identification enregistrées dans le traitement automatisé de données à caractère personnel dénommé FSPRT ».*

La Commission prend acte qu'un croisement entre les données enregistrées dans les deux traitements est réalisé, *a minima* toutes les 24 heures. Les traitements FSPRT et HOPSYWEB sont également interrogés, dès lors qu'un nouvel individu est enregistré dans l'un de ces deux traitements.

La Commission prend également acte des précisions apportées selon lesquelles le croisement des données s'effectuera uniquement à partir du nom, du prénom et de la date de naissance de la personne concernée. Elle demande à ce que le projet de décret soit modifié en ce sens. Elle relève par ailleurs que cette interconnexion ne portera que sur un nombre strictement limité de données, faisant l'objet d'une phonétisation et d'un hachage, et uniquement relatives au nom, prénom et date de naissance de la personne concernée.

Dans l'hypothèse d'une concordance, c'est-à-dire si la personne est connue du FSPRT et d'HOPSYWEB, le préfet du département d'hospitalisation peut dès lors procéder à des démarches auprès de l'ARS pour obtenir des informations complémentaires et s'assurer de l'identité de la personne concernée dans le cadre d'une procédure de levée de doute. A cet égard, la Commission prend acte de ce que ces échanges intervenant dans ce cadre se limitent à ce qui est strictement prévu par les dispositions du code de la santé publique et du code de procédure pénale, c'est-à-dire, en pratique, aux dates de début et de fin de mesure, au type de mesure prononcée et, le cas échéant, au lieu d'hospitalisation. Par ailleurs, elle relève que les préfets seront informés qu'ils ne doivent pas, dans le cadre de cette levée de doute, divulguer le fait que la personne concernée est enregistrée dans le FSPRT.

Le ministère a, par ailleurs, indiqué que les informations communiquées dans le cadre de la levée de doute, le seront *via* les canaux de transmission habituels, soit par exemple par téléphone. Il a précisé à cet égard que les agents de l'ARS susceptibles de répondre à de telles demandes sont sensibilisés au caractère confidentiel des informations transmises.

Enfin, il a été précisé que l'ARS est l'interlocuteur privilégié du préfet dans le cadre de la CPRAF (cellule pour la prévention de la radicalisation et l'accompagnement des familles), au sein de laquelle un référent identifié de l'ARS intervient et peut déjà avoir connaissance des cas de radicalisation.

Si la Commission ne remet pas en cause la nécessité pour les préfets de département de vérifier l'identité et de recueillir des informations complémentaires relatives aux

personnes ainsi visées par l'intermédiaire des ARS, elle estime qu'au regard du caractère particulièrement sensible de l'information dont il est question (inscription ou non au FSPRT), les modalités d'échanges des informations précitées avec l'ARS, dans le cadre de la procédure de levée de doute, ne sont pas suffisamment encadrées.

Au regard de ces éléments, la Commission s'interroge sur les conditions dans lesquelles les levées de doute sont amenées à s'opérer. Elle considère que seul le référent identifié au sein de chaque ARS, intervenant dans les CPRAF, devrait procéder à la vérification de l'identité de la personne et communiquer des informations complémentaires, sur sollicitation du préfet de département, et à Paris, du préfet de police. Elle estime qu'une telle mesure serait en effet de nature à limiter les risques conduisant à la connaissance par les agents des ARS du fait qu'une personne est enregistrée dans le FSPRT à l'occasion de la sollicitation du préfet de département, et à Paris, du préfet de police.

La Commission souligne que la modification envisagée est, en elle-même, sans incidence sur la gestion des mesures de soins sans consentement et sur la finalité première d'HOPSYWEB. En cas de concordance, seul le préfet du département du lieu d'hospitalisation ou les agents qu'il désigne seront informés de ladite concordance *via* un mail généré par le FSPRT. Par ailleurs, la Commission relève que les préfets et les agents dûment désignés et habilités par ce dernier ne disposeront pas d'un accès à HOPSYWEB et que les accédants et destinataires des traitements HOPSYWEB ne pourront pas accéder au FSPRT.

Sur les destinataires des données :

Le projet de décret prévoit que sont destinataires des données d'identification des personnes concernées par une mesure d'hospitalisation sans consentement et des informations complémentaires le préfet de département et, à Paris, le préfet de police du lieu d'hospitalisation.

La Commission prend acte des précisions apportées par le ministère selon lesquelles, dans le cadre de la procédure de levée de doute, le préfet de département du lieu d'hospitalisation peut ensuite prendre contact, le cas échéant, avec le préfet de département en charge du suivi de la personne radicalisée ou du service chargé de ce suivi. A ce titre il a également été précisé que le préfet compétent en charge du suivi de la personne radicalisée peut également lancer une évaluation plus poussée de l'individu dans le cadre du groupe d'évaluation départementale (GED) ou de la CPRAF ou encore renseigner le FSPRT.

Compte tenu de ces éléments, la Commission estime qu'en pratique il est possible de considérer que tant le préfet en charge du suivi de la personne radicalisée, que les membres du GED et de la CPRAF, ou encore les personnes accédant au FSPRT seront destinataires de l'information selon laquelle une personne déterminée fait l'objet d'une mesure d'hospitalisation sans consentement. Or, la Commission souligne que le présent projet de décret, en ce qu'il permet l'accès de ces personnes, qui n'interviennent pas dans la mise en place de la mesure d'hospitalisation sans consentement, à l'information selon laquelle un individu fait effectivement l'objet d'une telle mesure et à des informations complémentaires en cas de mise en œuvre de la procédure de levée de doute (dates de début et de fin des mesures, type de mesure prononcée, le cas échéant lieu d'hospitalisation), pose question au regard des exigences de secret professionnel en la matière.

La Commission rappelle qu'en vertu de l'article L. 1110-4 du code de la santé publique, les informations recueillies par un établissement de santé, à l'occasion d'un acte de prévention, de diagnostic ou de soins sont protégées par le secret professionnel, excepté dans les cas de dérogation prévus par la loi. De la même manière, elle observe que le principe selon lequel seule une dérogation légale à la règle du secret professionnel autorise un professionnel à accéder aux données couvertes par le secret médical, est également rappelé au titre des instructions des mois de janvier et décembre 2016 susvisées.

Or, les informations relatives aux mesures de soins sans consentement dont a fait l'objet une personne, en particulier les informations complémentaires susceptibles d'être transmises dans le cadre de la procédure de levée de doute, sont susceptibles de relever du secret professionnel prévu à l'article L. 1110-4 du code de la santé publique. Au demeurant, la Commission rappelle que l'information concernant la mise en place d'une mesure d'hospitalisation sans consentement à l'égard d'une personne déterminée constitue une donnée de santé conformément aux dispositions de l'article 4-15) du RGPD, précisément en ce qu'elle peut révéler la nature de l'affection (troubles mentaux) et fournir, par elle-même, des éléments permettant d'en caractériser la gravité.

Ces éléments rappelés, la Commission est réservée sur la possibilité, pour le présent projet de décret, d'introduire une dérogation au secret professionnel qui permettrait, en particulier aux agents accédant au FSPRT, d'être destinataires d'informations couvertes par le secret médical.

Sur les droits des personnes :

La Commission relève qu'il n'est pas prévu d'informer spécifiquement les personnes concernées, à savoir les personnes faisant l'objet d'une mesure d'hospitalisation sans consentement, de la nouvelle finalité qui serait poursuivie par les traitements HOPSYWEB.

Or, la Commission rappelle qu'une telle information est exigée au regard des dispositions des articles 12, 13 et 14 du RGPD.

Indépendamment de ce qui précède, la Commission estime que, compte tenu de l'évolution du cadre juridique applicable à la protection des données à caractère personnel, il revient au ministère de s'assurer que l'information délivrée actuellement par les ARS répond aux exigences des dispositions précitées. A ce titre et compte tenu des enjeux liés à la mise en relation des traitements HOPSYWEB et du FSPRT, elle considère qu'une information spécifique, quant à la nouvelle finalité poursuivie, devrait être délivrée.

Par ailleurs, la Commission relève que le projet de décret ne prévoit aucune disposition sur le droit à l'effacement des informations contenues dans HOPSYWEB, en particulier lorsqu'une mesure de soins sans consentement est ensuite déclarée irrégulière par le juge des libertés et de la détention. De la même manière, la Commission constate que le projet de décret ne précise pas les modalités selon lesquelles l'ARS concernée devra

notifier l'effacement des données au préfet de département du lieu d'hospitalisation conformément aux dispositions de l'article 19 du RGPD.

Si la Commission prend acte que les modalités d'exercice des autres droits demeurent inchangées, elle invite néanmoins le ministère à s'assurer de la complétude des droits mentionnés afin de prendre en compte les apports opérés par le RGPD. En particulier, la Commission estime que le projet de décret devrait être complété s'agissant de la mise en œuvre du droit à la limitation des personnes concernées. De la même manière, elle considère que le projet de décret devrait être modifié s'agissant en particulier des dispositions applicables au droit d'opposition et des raisons conduisant, en l'espèce, à l'écarter dans la mesure où il y a lieu de faire application des dispositions du règlement (UE) 2016/679 susvisé.

Sur la sécurité des données :

A titre liminaire, la Commission relève que les traitements HOPSYWEB étant susceptibles d'engendrer des risques élevés pour les personnes concernées au sens de l'article 35 du RGPD, une analyse d'impact a été transmise par le ministère. Elle souligne toutefois que l'absence d'information précise sur l'architecture et les mesures retenues ne permettent pas d'évaluer la conformité du dispositif à l'exigence de sécurité prévue par les articles 5-1-f) et 32 du RGPD.

De manière générale, elle rappelle que la nature des données traitées au sein des traitements HOPSYWEB requiert que des mesures de chiffrement conformes à l'annexe B1 du référentiel général de sécurité tant au niveau des bases de données que des sauvegardes soient mises en œuvre.

La journalisation des consultations, ajouts, modifications, suppressions dans les traitements HOPSYWEB, jusqu'à présent conservée 15 jours, sera conservée un an. La Commission recommande, s'agissant des données de santé, que les traces soient conservées dans les dossiers des patients et pour une durée égale à la durée de conservation de ces dossiers. Elle recommande également que l'administrateur, qui est en mesure de consulter les traces des accès, n'accède pas aux données de santé.

Les échanges entre les deux systèmes HOPSYWEB et FSPRT sont effectués *via* le protocole HTTPS. Concernant le recours à ce protocole, la Commission recommande d'utiliser la version de TLS la plus à jour possible et d'utiliser des algorithmes et des procédures de gestion de clés conformes à l'annexe B1 du référentiel général de sécurité. De plus, un mécanisme d'authentification mutuelle des serveurs devrait être mis en place.

La méthode de vérification de concordance entre les deux bases met en œuvre un mécanisme cryptographique à clé. La Commission rappelle la nécessité de respecter les recommandations de l'Agence nationale de la sécurité des systèmes d'information en la matière et appelle le ministère à la vigilance quant aux moyens mis en œuvre pour la gestion des clés.

La sensibilité de l'information calculée sur chaque service web HOPSYWEB dans le cas d'un ajout dans FSPRT requiert qu'une analyse de sécurité du dispositif soit effectuée, incluant notamment des tests d'intrusion et un audit de code. La Commission recommande que la ou les personnes responsables de l'administration de ces services

suivent une formation spécifique sur l'impact potentiel de ce service sur les personnes concernées. Enfin, un mécanisme de journalisation de toute action d'administration sur ce système devrait être mis en œuvre de telle manière à ce que ces traces ne soient pas accessibles aux administrateurs susmentionnés.

La Commission prend acte de l'engagement du ministère selon lequel aucune trace des calculs de vérifications ne figurera sur le système. Elle en déduit que seules des traces de connections entre les serveurs ne seront conservées. Dans ce contexte, et dès lors qu'une nouvelle connexion entre les webservices est effectuée à chaque nouvelle entrée dans le FSPRT, la Commission relève que le ministère accepte le risque résiduel consistant à pouvoir déduire des traces techniques de n'importe lequel des systèmes HOPSYWEB qu'une ligne a été ajoutée dans le FSPRT, sans savoir laquelle.

Dans le cadre de la procédure de levée de doute, la Commission souligne la nécessité de mettre en œuvre un processus permettant l'authentification de l'appelant et du répondant avant d'échanger sur toute demande. De plus, le risque que la personne habilitée à répondre à cette levée de doute à l'ARS déduise les raisons de l'appel n'étant pas négligeable, des mesures permettant d'en limiter la gravité devraient être mises en place, par exemple en l'informant des haut taux de faux positifs et en choisissant un interlocuteur habilité, par ailleurs, à manipuler des informations de ce type.

La Commission rappelle en outre que l'exigence de sécurité prévue par les articles 5-1-f) et 32 du RGPD nécessite la mise à jour de l'analyse d'impact relative à la protection des données et de ses mesures de sécurité au regard de la réévaluation régulière des risques. A ce titre, elle souligne que l'ouverture du FSPRT à tous les webservices HOPSYWEB mis en œuvre par chacune des ARS a pour effet d'augmenter la surface d'attaque potentielle et nécessite qu'une attention particulière soit portée au choix des mesures de sécurité effectué.

La Présidente

I. FALQUE-PIERROTIN