Commission nationale de l'informatique et des libertés

Délibération n° 2022-042 du 7 avril 2022 portant avis sur un projet de décret relatif à l'accès aux données non identifiantes et à l'identité du tiers donneur pris en application de l'article 5 de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique (demande d'avis n° 21022168)

NOR : *CNIX2224126V*

La Commission nationale de l'informatique et des libertés,

Saisie par le ministre des solidarités et de la santé d'une demande d'avis concernant un projet de décret relatif à l'accès aux données non identifiantes et à l'identité du tiers donneur pris en application de l'article 5 de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique ;

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 (règlement général sur la protection des données ou RGPD) ;

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

Vu l'article 5 de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique ;

Vu le code de la santé publique ;

Après avoir entendu le rapport de Mme Valérie PEUGEOT, commissaire, et les observations de M. Benjamin TOUZANNE, commissaire du Gouvernement,

Etant rappelés les éléments de contexte suivants :

L'article 5 de la loi n° 2021-1017 du 2 août 2021 relative à la bioéthique (loi relative à la bioéthique) permet à toute personne conçue par assistance médicale à la procréation (AMP) avec tiers donneur, si elle le souhaite, d'accéder à sa majorité à l'identité, aux données « non identifiantes » du tiers donneur ou à l'ensemble de ses informations. Seront concernées par ce dispositif les catégories de personne suivantes :

- les personnes nées d'une AMP avec tiers donneur ;
- les bénéficiaires d'une AMP avec tiers donneur ;
- les tiers donneurs, pour lesquels une sous-distinction peut être opérée entre :
  - les tiers donneurs qui n'étaient pas soumis aux dispositions de la loi relative à la bioéthique au moment de leur don (anciens tiers donneurs). Pour ceux-ci, il est prévu un dispositif leur permettant de consentir ou non à la transmission de leurs données aux personnes nées d'une AMP ;
  - et les tiers donneurs soumis aux dispositions de la nouvelle loi bioéthique au moment de leur don (nouveaux tiers donneurs).

Le don de gamètes et d'embryons sera donc désormais subordonné au consentement du tiers donneur à ce que son identité et ses données « non identifiantes » puissent être révélées à la personne née d'une AMP devenue majeure. Les tiers donneurs non soumis aux nouvelles dispositions législatives au moment de leur don peuvent également consentir à la communication de leurs données. Ceux-ci peuvent se manifester spontanément ou être recontactés lors d'une demande d'accès à ses origines par une personne née d'une AMP.

Le projet de décret organise l'accès à leurs origines des personnes nées d'une AMP avec tiers donneur en créant deux traitements de données distincts.

Un premier traitement, dont l'Agence de la biomédecine (ABM) est responsable en application de l'article L. 2143-4 du code de la santé publique (CSP), permet la collecte et la conservation des données nécessaires à l'accès aux origines des personnes concernées.

Le second traitement permet à la Commission d'accès aux données non identifiantes et à l'identité du tiers donneur (CAPADD), placée auprès du ministre chargé de la santé, de faire droit aux demandes d'accès aux origines formulées en application de l'article L. 2143-5 du CSP. La CAPADD est responsable de ce traitement en application de l'article L. 2143-6 du CSP.

Ces traitements relèvent du RGPD.

Formule les observations suivantes sur le projet de décret

Sur l'économie générale du texte :

La loi relative à la bioéthique a entendu permettre aux personnes nées d'une AMP avec tiers donneur d'avoir accès à certaines informations relatives à ces derniers, ce qui nécessite le traitement de données relatives à la santé. En particulier, concernant les tiers donneurs, l'article R. 2143-12 prévoit notamment la collecte :

- de la taille et du poids ;
- de leur état général au moment du don, dont leur état psychologique.

Le projet de décret précise que les deux traitements envisagés, nécessaires à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont sont investis les responsables des traitements, sont fondés sur l'article 6-1-*e*) du RGPD. En outre, les traitements de données de santé qu'ils impliquent sont justifiés par des « motifs d'intérêt public important », au sens des dispositions l'article 9-2-*g*) du RGPD. La Commission rejoint cette analyse.

S'agissant de chacun des traitements mis en œuvre par l'ABM et par la CAPADD :

Sur l'information et les modalités de consentement des tiers donneurs à la communication de leurs données dites « non identifiantes » et de leur identité :

Les modalités de consentement des tiers donneurs à la communication de leurs données dites « non identifiantes » et de leur identité sont détaillées à la section 4 du projet de décret. Le projet d'article R. 2143-6 du CSP, qui tire les conséquences de l'article L. 1244-2 du même code, prévoit ainsi que le consentement du donneur à la communication de ses données aux personnes nées de don n'est pas révocable dès attribution du don.

Dans l'hypothèse où ils ont donné leur consentement à la transmission de leurs données, ce principe s'applique également aux anciens tiers donneurs qui se sont manifestés auprès de la CAPADD ou qui ont été recontactés, en application des 5° et 6° de l'article L. 2143-6 du CSP. Ainsi, leur consentement n'est plus révocable dès la communication effective de leurs données au centre où a été réalisé le don.

Selon les précisions du ministère, les tiers donneurs seront informés au moment du don des traitements de données les concernant, ainsi que de l'impossibilité de révoquer leur consentement à la communication de ces dernières après attribution du don. **La Commission invite le ministère à prévoir la transmission de ces mêmes informations aux anciens tiers donneurs par la CAPADD, préalablement à la collecte de leurs données par le centre de don.**

Sur les droits des personnes concernées :

S'agissant de la limitation des droits à l'effacement et d'opposition :

Les projets d'articles R. 2143-16 et R. 2143-21 du CSP écartent *a priori* la faculté pour les personnes concernées de faire exercice de leurs droits à l'effacement des données et d'opposition au traitement. Interrogé sur ce point, le ministère a précisé qu'il entendait faire application de l'article 23-1-*i*) du RGPD.

A cet égard, l'article 23 du RGPD requiert un texte dans le droit de l'Union ou de l'Etat membre pour limiter la portée des droits prévus aux articles 12 à 22 du RGPD, à condition qu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir notamment « *la protection de la personne concernée ou des droits et libertés d'autrui* » (article 23-1-*i*) du RGPD).

Le ministère a précisé que, conformément à l'article 23-1 du RGPD, les droits d'opposition et d'effacement des données pouvaient être écartés dans la mesure où leur limitation est nécessaire aux fins de garantir le droit d'accès aux origines des personnes nées d'une AMP avec tiers donneur. Il a souligné que :

– pour les tiers donneurs, l'exercice de ces droits est incompatible avec la réalisation du don, dans la mesure où celui-ci est désormais subordonné au consentement à la communication de ses données aux personnes nées d'une AMP ;
– pour les bénéficiaires de l'AMP, l'exercice de ces droits est incompatible avec la réalisation de l'AMP, et nécessiterait la révocation du consentement à l'AMP avec tiers donneur.

Ainsi, selon le ministère, l'exclusion de ces droits permet de garantir l'effectivité du droit d'accès aux origines. **La Commission ne remet pas en cause cette analyse dès lors que l'exercice par le donneur des droits d'effacement et d'opposition serait effectivement de nature à faire échec à l'application de la loi, qui est de permettre à la personne née d'une AMP avec tiers donneur de pouvoir, si elle le souhaite à un moment dans sa vie à compter de sa majorité, accéder à ses origines.**

Toutefois, en l'absence de précisions de la part du ministère, la Commission comprend du projet que la limitation des droits s'appliquera également s'agissant des personnes nées d'une AMP avec tiers donneur. **Consciente des conséquences qu'emporterait l'exercice de ces droits par la personne née d'une AMP avec tiers donneur, qui aurait pour effet un renoncement définitif au droit d'accès à ses origines, la Commission en prend acte. Elle rappelle néanmoins que cette limitation devra répondre aux conditions prévues à l'article 23 du RGPD et que le projet devra être complété, afin de contenir les dispositions spécifiques prévues au 2. de ce même article.**

La Commission prend en outre acte de ce que le ministère s'est engagé à modifier le décret afin qu'il précise que les personnes concernées devront être informées des limitations apportées à leurs droits.

S'agissant du droit à la limitation du traitement :

Contrairement à ce qui est mentionné dans l'analyse d'impact relative à la protection des données (AIPD) qui écarte la faculté pour les personnes concernées d'exercer leur droit à la limitation, le projet de décret n'apporte aucune information sur ce point. Selon les précisions du ministère, l'exercice de ce droit, qui rendrait partiellement inaccessibles des données pendant une certaine période, aurait pour conséquence d'empêcher temporairement l'ajout d'un tiers donneur dans la base de données de l'ABM et pourrait conduire à refuser un nouveau don ou l'utilisation d'un don, puisque l'ABM ne serait pas en mesure de s'assurer que le recours au(x) don(s) d'un même donneur ne conduira pas délibérément à la naissance de plus de dix enfants, conformément aux dispositions de l'article L. 1244-4 du CSP.

La Commission s'interroge cependant sur la faculté du ministère d'écarter de manière systématique l'exercice du droit à la limitation du traitement par les personnes concernées à ce motif. Par exemple, le droit à la limitation pourrait permettre à un tiers donneur qui estime que ses données sont inexactes de les faire rectifier avant communication à la personne née d'une AMP. La Commission prend acte de l'engagement du ministère de clarifier le projet de décret en ce sens.

S'agissant des droits d'accès et de rectification :

Les projets d'articles R. 2143-16 et R. 2143-21 du CSP prévoient l'exercice des droits d'accès et de rectification par les personnes concernées. La Commission prend acte du fait que les personnes nées d'AMP avec tiers donneur et les tiers donneurs faisant usage de leur droit d'accès ne peuvent accéder, en dehors du dispositif d'accès aux origines, qu'aux seules informations qui leur sont propres et qu'ils ont eux-mêmes communiquées. Le ministère a précisé que ces modalités concernaient également les bénéficiaires d'une AMP avec tiers donneur. La Commission prend acte de ce que le ministère s'est engagé à modifier le projet de décret sur ce point. Elle l'invite en outre à ajouter aux projets d'articles R. 2143-16 et R. 2143-21 du CSP les termes « le cas échéant » à la suite de « *les tiers donneurs et les personnes nées d'une assistance médicale à la procréation avec tiers donneur faisant usage de leur droit d'accès ne peuvent accéder qu'aux données personnelles qui les concernent* », dans la mesure où les personnes nées d'une AMP avec tiers donneur n'auront pas elles-mêmes communiqué de données les concernant préalablement à l'exercice de leur droit.

S'agissant des accès aux données et des destinataires :

Les projets d'articles R. 2143-14 et R. 2143-19 du CSP précisent les personnes pouvant accéder aux données à des fins d'enregistrement, de traitement et de conservation. La Commission prend acte de ce que le ministère s'est engagé à modifier le projet de décret, afin qu'il précise que les personnes pouvant, sous l'autorité du responsable de traitement, enregistrer, consulter et traiter les données sont des personnes accédant « au traitement » et non « aux données », dans la mesure où elles disposent de droits en écriture.

Sur le traitement de données mis en œuvre par l'ABM :

Sur les finalités du traitement envisagé :

L'article L. 2143-4 du CSP prévoit la mise en œuvre par l'ABM d'un traitement de données à caractère personnel relatives aux tiers donneurs, à leurs dons et aux personnes nées à la suite de ces dons ainsi que l'identité des personnes ou des couples receveurs. Selon le projet d'article R. 2143-10, ce traitement, dénommé « *Registre des donneurs de gamètes et d'embryons* », a pour finalités de permettre aux personnes concernées d'accéder à leurs origines et de permettre la réalisation d'analyses statistiques à partir des données incluses dans le traitement et préalablement pseudonymisées. **La Commission estime ces finalités déterminées, explicites et légitimes au sens de l'article 5 du RGPD.**

Concernant la réalisation d'analyses statistiques, selon les précisions du ministère, ces analyses auront uniquement pour objet des éléments de comptage et de statistique (par exemple, le nombre de donneurs inscrits au cours d'une étude), à partir des données brutes figurant dans la base de données. Aucune extraction de données à caractère personnel n'est envisagée à ce stade.

L'accès à ces indicateurs doit être subordonné au respect du droit d'en connaître des utilisateurs habilités et des habilitations mises en place pour chaque profil, ainsi que de traces fonctionnelles enregistrant l'auteur, la date et l'heure des opérations effectuées.

De manière générale et en dehors de ces analyses statistiques, si les données du traitement devaient être extraites afin de les réutiliser pour des recherches, études ou évaluations dans le domaine de la santé, celles-ci devront faire l'objet de formalités préalables telles que prévues par la loi « informatique et libertés ». La Commission prend acte de ce que l'ABM s'est engagée à déposer une demande d'autorisation auprès de la CNIL si de telles recherches devaient être envisagées.

Sur les données dont le traitement est envisagé :

Le projet d'article R. 2143-11 du CSP décrit les catégories de données à caractère personnel qui seront traitées par l'ABM.

Concernant les « données relatives à l'identité » des personnes concernées :

Le ministère a précisé que seront notamment collectés leurs nom de naissance, prénom, date de naissance, sexe, ainsi que leur pays de naissance. **La Commission demande que la nature exacte des données qui seront collectées soit précisée dans le décret.**

Concernant les données dites « non identifiantes » des tiers donneurs :

Le I du projet d'article R. 2143-12 liste les données « non identifiantes » du tiers donneur qui pourront être communiquées aux personnes nées de don si celles-ci en font la demande. Parmi ces données figurent notamment les motivations de leurs dons.

Dans sa délibération n° 2019-097 du 11 juillet 2019 portant avis sur un projet de loi relatif à la bioéthique, la Commission alertait sur l'utilisation de ces termes, dans la mesure où les données traitées, certes non nominatives, sont, en réalité, indirectement identifiantes, tant pour les tiers donneurs que pour les personnes extérieures à la procédure d'AMP qui pourraient être mentionnées dans les motivations du don (tiers au don). Dès lors, la transmission de ces seules informations à la personne née d'une AMP avec tiers donneur est susceptible de lui permettre de réidentifier le tiers donneur et/ou des tiers au don.

La Commission relève que des mesures visant à prévenir le risque de réidentification ont été envisagées :

– en premier lieu, les tiers donneurs seront informés par le médecin en charge de l'AMP des risques de réidentification attachés à la complétion des champs de texte libre, ainsi que de la procédure de vérification associée ;
– en deuxième lieu, par la vérification par le médecin du centre d'AMP du formulaire complété par le tiers donneur au moment du don ;
– enfin, par la possibilité pour le médecin de saisir la CAPADD en cas de doute concernant le caractère potentiellement réidentifiant des données (projet d'article R. 2143-9 du CSP).

La Commission accueille favorablement que le projet de décret crée une telle procédure pour éviter les risques de réidentification, notamment s'agissant des tiers au don, qui pourraient être mentionnés dans le document détaillant les motivations du don rédigées par le tiers donneur. Elle souligne la nécessité de sensibiliser les médecins ainsi que les personnes exerçant au sein de la CAPADD sur la notion de « données identifiantes » au sens des textes applicables en matière de protection des données.

Sur les conditions d'information des personnes concernées :

Selon le III du projet d'article R. 2143-16 du CSP :

– les tiers donneurs seront informés du traitement de leurs données à l'occasion de leur prise en charge par le centre d'AMP, et au moment du recueil de leur consentement ;
– les bénéficiaires de l'AMP sont informés par le médecin à l'occasion de leur prise en charge dans le cadre de l'AMP.

S'agissant de l'information des tiers donneurs sur le risque de réidentification :

La Commission avait estimé nécessaire, dans sa délibération n° 2019-097 du 11 juillet 2019 portant avis sur un projet de loi relatif à la bioéthique, de prévoir une information claire des tiers donneurs sur le risque possible de réidentification de tiers au don à partir des données « non identifiantes » et notamment lors de la rédaction des motivations du don.

Selon les précisions du ministère, les tiers donneurs seront informés de la nature de l'ensemble des données collectées et de la distinction entre données relatives à l'identité et données « non identifiantes » par l'intermédiaire des brochures d'information. La Commission relève cependant que les brochures d'information ne contiennent pas d'éléments à ce sujet. Elle invite donc le ministère à les compléter.

S'agissant de l'information des personnes nées d'une AMP avec tiers donneur :

S'agissant du traitement des données des personnes nées d'une AMP avec tiers donneur, l'information sera délivrée aux bénéficiaires de l'AMP.

L'article L. 2141-10 du CSP prévoit par ailleurs que les bénéficiaires de l'AMP sont « *incités à anticiper et à créer les conditions qui leur permettent d'informer l'enfant, avant sa majorité, de ce qu'il est issu d'un don* ». La Commission relève qu'aucune disposition ne prévoit de mesures d'information s'agissant des personnes nées d'une AMP avec tiers donneur lorsqu'elles atteignent la majorité.

En outre, une information individuelle sur le traitement de données reviendrait à informer la personne de ce qu'elle est née d'une AMP et semblerait donc ne pas s'inscrire dans la volonté du législateur.

Une information collective sera mise à disposition par l'ABM et la CAPADD. La Commission invite le ministère à veiller à la complétude de cette information et à mettre en œuvre les moyens adaptés pour en permettre une large diffusion.

Sur « l'actualisation » et le droit à la rectification des données :

S'agissant de la possibilité d'actualisation des données prévue par l'article L. 2143-2 du CSP, le projet d'article R. 2143-13 du même code prévoit que les prénoms et le sexe des personnes concernées, ainsi que les données relatives à la situation familiale et professionnelle du tiers donneur, peuvent faire l'objet d'une demande « d'actualisation » auprès des centres d'AMP ou de l'ABM.

Le ministère a précisé que « l'actualisation » visait à permettre la modification de données qui ont pu évoluer compte tenu de la situation du donneur (par exemple changement de situation familiale ou de profession). Est ainsi opérée une distinction entre l'actualisation des données et le droit de rectification qui concerne, selon lui, les données erronées ou incomplètes qui doivent faire l'objet d'une mesure correctrice.

La Commission rappelle néanmoins que le droit à la rectification prévu à l'article 16 du RGPD vise à permettre la rectification des données inexactes ou incomplètes, l'inexactitude pouvant aussi être due à une modification de la situation des personnes concernées. Elle relève, par ailleurs, que d'après le projet de décret, les modalités selon lesquelles une demande d'actualisation peut être effectuée diffèrent de celles prévues concernant l'exercice du droit à la rectification. Prenant acte de l'incertitude du ministère quant à la distinction à opérer entre la possibilité d'actualiser les données et le droit de rectification, elle l'invite à prévoir des modalités de traitement des demandes ne nécessitant pas que les personnes concernées se trouvent contraintes de multiplier leurs démarches.

Sur les durées de conservation des données :

Le projet d'article R. 2143-15 du CSP prévoit que l'ensemble des données collectées dans le cadre du traitement réalisé par l'ABM sera conservé pour une durée de cent-vingt ans, à compter de leur date d'enregistrement.

Le ministère a indiqué que cette durée vise à permettre aux personnes nées d'une AMP d'exercer leur droit d'accès aux origines à tout moment, à compter de leur majorité en tenant compte de l'espérance de vie.

La Commission rappelle néanmoins que les données à caractère personnel doivent être conservées pour une durée limitée répondant aux finalités du traitement conformément aux dispositions de l'article 5-1-*e*) du RGPD. Dans son précédent avis n° 2019-097 du 11 juillet 2019, elle avait suggéré que des hypothèses dans lesquelles la durée de conservation pourrait être réduite soient prévues. A cet égard, la Commission prend acte de ce que le ministère entend préciser dans le décret que les données des personnes concernées seront supprimées une fois que tous les dons d'une même personne auront été utilisés sans donner lieu à une naissance. Elle l'invite cependant à s'assurer que la durée de conservation ne pourrait pas être réduite dans d'autres cas.

Sur la sécurité des données et la traçabilité des actions :

Le traitement envisagé, réalisé à grande échelle et incluant notamment des données sensibles, a fait l'objet d'une AIPD. Le traitement, auquel les tiers donneurs pourront se connecter à distance afin de remplir le formulaire de consentement prévu par le projet d'article R. 2143-6 du CSP, constitue un téléservice au sens de l'ordonnance n° 2005-1516 du 8 décembre 2005 et fera l'objet d'une homologation de sécurité avant sa mise en production.

L'hébergement du traitement sera internalisé au sein de l'ABM, dans les propres centres de données de l'Agence. Selon les précisions du ministère, la sauvegarde des données du traitement sera, quant à elle, réalisée par une société soumise au droit étasunien sur des serveurs situés en France et sans aucun transfert de données en dehors de l'Union européenne. Il appartient à l'ABM, en tant que responsable de traitement, de s'assurer que son sous-traitant présente des garanties suffisantes conformément à l'article 28 du RGPD, en vérifiant notamment si les législations et pratiques locales sont susceptibles de permettre aux autorités étasuniennes d'accéder aux données stockées sur le territoire de l'Union européenne. Un tel accès, s'il n'est pas fondé sur un accord international, pourrait constituer une divulgation non autorisée par le droit de l'Union, en violation de l'article 48 du RGPD. Dans ce cas d'espèce, la Commission estime que les règlementations étasuniennes en matière d'accès aux données des fournisseurs de services Internet et entreprises de télécommunications par les services de renseignement américains s'appliquent aux données traitées, y compris en dehors du territoire des Etats-Unis, par la société intervenant dans cette sauvegarde de données. En l'état, la Commission considère donc qu'il existe un risque d'accès aux données par les autorités étasuniennes. En conséquence, dans la mesure où le traitement envisagé est réalisé à grande échelle et comporte des données sensibles, la Commission demande que le responsable de traitement ait recours à un prestataire exclusivement soumis au droit européen, ou bien mette en œuvre des mesures empêchant tout accès aux données par le prestataire et donc par les autorités étasuniennes, telles que le chiffrement des données sauvegardées par des algorithmes à l'état de l'art et la non-transmission des clés de chiffrement au prestataire.

Des mesures de chiffrement permettant d'assurer l'intégrité et la confidentialité des données traitées seront mises en place dans le cadre du traitement, tant concernant les postes utilisateur, les flux d'accès que les échanges de données. La Commission rappelle la nécessité d'un chiffrement au repos des données stockées, qui semble être opérationnel selon les documents fournis par le ministère. Elle rappelle également que les mécanismes techniques mis en œuvre pour ces traitements devront être conformes à l'état de l'art, et notamment aux préconisations du référentiel général de sécurité (RGS).

La Commission prend acte de ce que les tiers donneurs et les professionnels de santé ne pourront se connecter au traitement « ABM » qu'au moyen d'une authentification forte, comprenant au moins deux facteurs différents d'authentification. Si l'un de ces facteurs est un mot de passe, la Commission recommande de mettre en œuvre une politique de mots de passe conforme à la délibération n° 2017-012 du 19 janvier 2017 portant adoption d'une recommandation relative aux mots de passe, ou à toute autre mise à jour ultérieure de cette recommandation, et de choisir un facteur d'authentification différent robuste afin d'assurer une meilleure fiabilité de l'authentification et, partant, d'assurer une traçabilité adéquate des accès de ces utilisateurs.

Concernant l'habilitation des personnes pouvant accéder aux données traitées, la Commission accueille favorablement la mise en œuvre de profils d'habilitation permettant des restrictions d'accès à certaines fonctionnalités et à la visibilité des données en fonction du périmètre du profil et de l'opération effectuée.

La Commission relève que des mécanismes de contrôle proactif des comportements malveillants seront mis en place par l'ABM. La durée de conservation des traces fonctionnelles est en cours de définition par le responsable de traitement. La Commission rappelle qu'une conservation des traces fonctionnelles conforme à ses recommandations consiste à conserver ces traces pendant une durée minimum de six mois et maximum d'un an à partir de la génération de la trace fonctionnelle, ou d'apporter une justification particulière démontrant un risque élevé pour les personnes concernées nécessitant de conserver ces traces au-delà de la durée recommandée, notamment en cas de possibilité de détournement de finalité du traitement. Elle prend acte de ce que ces traces ne comporteront pas de données de santé ou de données nominatives.

Sur le traitement de données mis en œuvre par la CAPADD :

L'article L. 2143-6 du CSP prévoit la mise en œuvre par la CAPADD d'un traitement de données à caractère personnel dont elle est responsable, dont les finalités sont précisées par le projet d'article R. 2143-17 du CSP, à savoir l'enregistrement, la conservation, et le suivi des demandes et le recueil et l'enregistrement du consentement de certains tiers. **La Commission estime ces finalités déterminées, explicites et légitimes au sens de l'article 5 du RGPD.**

Sur les données dont le traitement est envisagé :

Le projet d'article R. 2143-18 du CSP décrit les catégories de données à caractère personnel qui seront traitées par la CAPADD.

En outre, l'AIPD portant sur le traitement de données de la CAPADD détaille les données traitées pour chacune des catégories de personnes concernées. A titre d'exemple, les données relatives à l'identité des personnes nées d'une AMP avec tiers donneur comprendront : la nationalité française, la civilité, les noms de naissance et d'usage, les prénoms, la date et le lieu de naissance ainsi que les coordonnées (postales et électroniques).

La Commission s'interroge sur la nécessité de collecter la nationalité française des personnes concernées, dans la mesure où l'ensemble du dispositif de don de gamètes et d'embryons n'est pas conditionné à la nationalité des personnes concernées.

La Commission prend acte de ce que le ministère s'est engagé à ne pas collecter cette information. Elle demande en outre que la nature exacte des données qui seront collectées soit précisée dans le décret.

S'agissant de la collecte des données des anciens tiers donneurs :

Selon l'AIPD transmise par le ministère, le répertoire national d'identification des personnes physiques (RNIPP) et le répertoire national interrégimes des bénéficiaires de l'assurance maladie (RNIAM) seront consultés dans le cadre de la procédure de recontact des anciens tiers donneurs. Selon le ministère, les numéros d'identification, et plus particulièrement le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) des anciens tiers donneurs, seront échangés entre la CAPADD et l'Institut national de la statistique et des études économiques (INSEE), la Caisse nationale d'assurance maladie ainsi que les caisses primaires d'assurance maladie *via* des messageries sécurisées. Il est également prévu que les données seront supprimées à l'issue de la procédure de recontact.

La Commission, qui rappelle que tout traitement du NIR doit s'effectuer conformément aux dispositions de l'article 30 de la loi « informatique et libertés », invite le ministère à préciser dans le décret que cette donnée sera traitée.

Elle demande également que les anciens donneurs recontactés soient informés que le RNIPP et le RNIAM ont été consultés afin d'utiliser leur NIR pour les retrouver.

Enfin, selon les précisions du ministère, seule la date et le résultat de la procédure de recontact seront conservés (consentement, refus ou absence de réponse du tiers donneur). La Commission demande à ce que cela soit précisé dans le décret.

S'agissant de la collecte des données des « nouveaux » tiers donneurs :

Le ministère, interrogé sur les personnes concernées par le traitement de données de la CAPADD, a confirmé que seraient également traitées, en cas de demande d'accès aux origines, les données relatives aux nouveaux tiers donneurs. **Le ministère s'est engagé à compléter le projet de décret sur ce point. La Commission en prend acte.**

Sur les conditions d'information des personnes concernées :

Selon les précisions du ministère, une information générale sera mise à disposition du public sur le site web de la CAPADD et renseignera les caractéristiques du traitement de données mis en œuvre par celle-ci.

La Commission recommande que la campagne d'information collective mette en évidence la possibilité pour les personnes d'obtenir la transmission d'une note d'information complète et les modalités de cette demande, qui ne devront pas renvoyer exclusivement à des moyens électroniques. Les notes d'information spécifiques, conformes aux dispositions du RGPD, devront pouvoir être consultées en amont de toute démarche auprès de la CAPADD.

Sur les durées de conservation des données :

La Commission rappelle que les données à caractère personnel doivent être conservées pour une durée limitée répondant aux finalités du traitement conformément aux dispositions de l'article 5-1-*e*) du RGPD.

S'agissant des données relatives aux demandes d'accès aux origines par les personnes nées d'AMP avec tiers donneur :

Le premier alinéa du projet d'article R. 2143-20 du CSP prévoit une conservation des données pour une durée de cinquante ans à compter de la date de leur enregistrement. Selon les précisions du ministère, cette durée est fixée en prenant en compte l'espérance de vie résiduelle d'une personne née d'AMP avec tiers donneur pendant laquelle elle peut être amenée à formuler des demandes d'accès, soit de sa majorité à environ 70 ans.

Par ailleurs, la Commission prend acte des précisions du ministère selon lesquelles il est envisagé de faire droit à toute demande des personnes nées d'une AMP avec tiers donneur, y compris dans l'hypothèse où elle aurait déjà été formulée. Rappelant que les données permettant de répondre aux demandes sont par ailleurs conservées par l'ABM, la Commission s'interroge sur la nécessité, pour la CAPADD, de conserver les données relatives aux demandes pendant une telle durée. Elle invite en tout état de cause le ministère à prévoir une stricte application du principe de minimisation des données.

S'agissant des données relatives aux anciens tiers donneurs :

Le second alinéa du projet d'article R. 2143-20 du CSP prévoit une conservation des données relatives aux anciens tiers donneurs pour une durée de cent ans, à compter de la date de leur enregistrement dans le traitement.

Selon les précisions du ministère, cette durée de conservation est justifiée au regard des dispositions de l'article L. 2143-6 (5°) du CSP qui confie à la CAPADD la mission de recueillir et d'enregistrer l'accord des anciens tiers donneurs à la transmission de leurs données « non identifiantes » et de leur identité aux personnes nées de don. Il précise à cette fin que, pour la réalisation de cette mission, la CAPADD devra conserver l'information selon laquelle l'ancien tiers donneur consent ou non à la transmission de son identité et de ses

données « non identifiantes » aux personnes nées de don, notamment afin de ne pas recontacter à plusieurs reprises les anciens tiers donneurs ayant préalablement refusé une telle transmission.

La Commission invite le ministère à prévoir des cas dans lesquels cette durée de conservation peut être réduite, dans la mesure où certaines situations ne semblent pas nécessiter une conservation si longue au regard des finalités poursuivies.

Sur la sécurité des données et la traçabilité des actions :

Le traitement envisagé, réalisé à grande échelle et incluant notamment des données sensibles, a fait l'objet d'une AIPD. Cette AIPD transmise par le ministère et portant sur le traitement de données mis en œuvre par la CAPADD semble en l'état incomplète, dans la mesure où la vraisemblance des risques n'a pas été évaluée ; la Commission rappelle donc que l'AIPD devra être complétée avant la mise en œuvre du traitement. Par ailleurs, la Commission prend acte de ce que le traitement fera l'objet d'une homologation de sécurité avant sa mise en production.

L'hébergement du traitement sera réalisé par un prestataire externalisé certifié hébergeur de données de santé (HDS) et non soumis à des réglementations extra-européennes.

Des mesures de chiffrement permettant d'assurer l'intégrité et la confidentialité des données traitées seront mises en place dans le cadre du traitement, selon les mêmes modalités que le traitement mis en œuvre par l'ABM. Les données sensibles seront chiffrées au repos. Les mécanismes techniques mis en œuvre pour ces traitements devront être conformes à l'état de l'art, et notamment aux préconisations du référentiel général de sécurité (RGS).

De même que pour le traitement mis en œuvre par l'ABM, la Commission prend acte de ce que les accès des utilisateurs seront protégés par une authentification forte comportant au moins deux facteurs d'authentification différents. La Commission rappelle ses recommandations susmentionnées concernant le choix de ces facteurs d'authentification.

Concernant l'habilitation des personnes pouvant accéder aux données traitées, la Commission accueille favorablement la mise en œuvre de profils d'habilitation permettant des restrictions d'accès à certaines fonctionnalités et un accès aux données uniquement nécessaires à l'utilisateur.

La durée de conservation des traces fonctionnelles est en cours de définition par le responsable de traitement. La Commission rappelle qu'une conservation des traces fonctionnelles conforme à ses recommandations consiste à conserver ces traces pendant une durée minimum de six mois et maximum d'un an à partir de la génération de la trace fonctionnelle, ou d'apporter une justification particulière démontrant un risque élevé pour les personnes concernées nécessitant de conserver ces traces au-delà de la durée recommandée, notamment en cas de possibilité de détournement de finalité du traitement.

Un centre opérationnel de sécurité collectera et analysera les traces et événements produits par les équipements réseau du traitement. La Commission recommande que les traces applicatives et événements collectés et analysés soient conservés pendant une durée conforme à ses préconisations et prend acte de ce que ces traces ne comporteront pas de données de santé ou de données nominatives. Elle recommande également la mise en œuvre d'un mécanisme d'analyse proactive des traces fonctionnelles générées par le traitement.

Enfin, les échanges dématérialisés entre l'ABM et la CAPADD, ainsi qu'entre les différentes entités pouvant intervenir lors d'une demande d'accès aux origines, s'effectueront grâce à des messageries sécurisées de santé assurant la confidentialité des échanges. Lorsque certaines de ces entités ne sont pas éligibles à ce mode de communication, la Commission rappelle que le corps des messages ne devra comporter aucune donnée à caractère personnel et se limiter au strict nécessaire. Elle prend acte de ce que les pièces jointes seront chiffrées par des algorithmes à l'état de l'art.

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

La présidente,
M.-L. Denis