

Délibération n° 2023-127 du 7 décembre 2023 portant décision unique et autorisant l'Agence nationale de santé publique à mettre en œuvre des traitements automatisés de données à caractère personnel dans le cadre de l'élaboration du « Baromètre de Santé publique France »

(Saisine n° 923201)

La Commission nationale de l'informatique et des libertés,

Saisie par l'Agence nationale de santé publique d'une demande d'autorisation concernant des traitements automatisés de données à caractère personnel ayant pour finalité la mise en œuvre d'études portant sur le suivi des principaux comportements, attitudes et perceptions liés aux prises de risque et à l'état de santé de la population résidant en France dans le cadre de l'élaboration du « Baromètre de Santé publique France » ;

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, notamment ses articles 66, 72 et suivants (loi « informatique et libertés ») ;

Vu l'avis favorable du Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé du 15 juin 2023 ;

Vu le dossier et ses compléments ;

Sur la proposition de Mme Valérie PEUGEOT, commissaire, et après avoir entendu les observations de M. Damien MILIC, commissaire du Gouvernement,

Formule les observations suivantes :

Sur le responsable de traitement	L'Agence nationale de santé publique (ANSP)
Sur le sous-traitant	Le traitement des données par la société IPSOS devra être régi par un contrat ou un acte juridique conformément à l'article 28 du RGPD.

Sur l'opportunité du recours à la décision unique	Dans le cadre de l'élaboration de son baromètre, l'ANSP souhaite réaliser, à intervalles réguliers, une étude visant à enrichir les connaissances sur l'état de santé de la population française. Pour ce faire, un échantillon représentatif de la population sera tiré au sort tous les deux ans. Outre le fait de poursuivre une même finalité, les traitements envisagés par l'ANSP présentent des caractéristiques similaires : - la nature des données collectées au moyen d'un questionnaire standardisé ; - les mêmes catégories de destinataires : les personnes habilitées par le responsable de traitement et son sous-traitant. Ces traitements, relevant du régime prévu par les dispositions des articles 66 et 72 et suivants de la loi « informatique et libertés », la CNIL estime opportun, au vu des éléments présentés dans le dossier de demande, de faire application des dispositions de l'article 66 IV, qui lui permettent, par décision unique, de délivrer à un même demandeur une autorisation pour des traitements répondant à une même finalité, portant sur des catégories de données identiques et ayant des catégories de destinataires identiques.
Sur la licéité des traitements et les conditions permettant de traiter des données concernant la santé	Les traitements envisagés par l'ANSP ont vocation à suivre les comportements de santé de la population française et leurs déterminants. Ces traitements, réalisés à des fins de recherche scientifique, sont nécessaires à l'exécution de la mission d'intérêt public dont est investie l'ANSP. Ces traitements sont, à ce titre, licites au regard de l'article 6.1.e) du RGPD et remplissent la condition prévue à l'article 9.2.j) du RGPD permettant de traiter des données concernant la santé.
Sur les points de non-conformité à la MR-004	Le dossier de demande mentionne que les traitements envisagés sont conformes aux dispositions de la méthodologie de référence MR-004, à l'exception des modalités d'information des personnes concernées et des destinataires des données directement identifiantes.

Sur la finalité des traitements et leur caractère d'intérêt public	Le Baromètre de santé publique France (ci-après « le baromètre ») a pour finalité le suivi des principaux comportements, attitudes et perceptions liés aux prises de risque et à l'état de santé de la population résidant en France. Pour ce faire, sera réalisée tous les deux ans une étude visant à : - suivre les comportements de santé de la population française et leurs déterminants ; - documenter des enjeux de santé publique ou orienter une décision politique, notamment via l'interrogation des connaissances et des opinions de la population en vue de la mise en place ou de l'évaluation d'actions de prévention ou de politiques publiques ; - enrichir les connaissances sur l'état de santé de la population française, pour des indicateurs non couverts par d'autres enquêtes par d'autres systèmes de surveillance. Ce projet a reçu le label d'intérêt général et de qualité statistique à caractère obligatoire par le Comité du label, conformément aux dispositions de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. La finalité des traitements est déterminée, explicite et légitime, conformément à l'article 5.1.b) du RGPD et présente un intérêt public, conformément à l'article 66.I de la loi « informatique et libertés ».
Sur la réutilisation de données de bases existantes	Tous les deux ans, les participants au baromètre seront tirés au sort par l'Institut national de la statistique et des études économiques (INSEE), à partir de la base de données dénommée « Fideli » (Fichier démographique d'origine fiscale sur les logements et les personnes), qu'il détient. La taille de l'échantillon tiré au sort sera d'environ 60 000 à 75 000 personnes. Seules les données strictement nécessaires et pertinentes au regard des objectifs du baromètre devront être transmises par l'INSEE : - à la société IPSOS, afin que cette dernière contacte les personnes tirées au sort pour leur proposer de participer au baromètre. Cette base de données ne contiendra aucune donnée relative à la santé des bénéficiaires ; - à l'ANSP, afin de réaliser de corriger la non-réponse et de réaliser des pondérations (redressements). À cet égard, les filtrages seront réalisés en amont de cette transmission par l'INSEE.

Sur les catégories particulières de données traitées	Les données suivantes seront traitées dans le cadre du baromètre : - les données nominatives et les coordonnées (postales, électroniques et téléphoniques) des personnes tirées au sort ainsi que, le cas échéant, celles des référents fiscaux dont les coordonnées sont présentes dans la base de données Fideli, aux fins de suivi des participants ; - la vie sexuelle des participants, dont la collecte a été scientifiquement justifiée dans le dossier de demande. Les données dont le traitement est envisagé sont adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités du traitement, conformément aux dispositions de l'article 5.1.c) du RGPD.
Sur l'information et les droits des personnes	<i>S'agissant des modalités d'information :</i> <i>S'agissant des personnes susceptibles d'être tirées au sort et des référents fiscaux dont les coordonnées sont présentes dans la base de données Fideli :</i> En application de l'article 69 de la loi « informatique et libertés » et de l'article 14.5.b) du RGPD, l'obligation d'information individuelle de la personne concernée peut faire l'objet d'exceptions, notamment dans l'hypothèse où la fourniture d'une telle information se révélerait impossible, exigerait des efforts disproportionnés ou compromettrait gravement la réalisation des objectifs du traitement. En pareils cas, le responsable de traitement prend des mesures appropriées pour protéger les droits et libertés, ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles. En l'espèce, il sera fait exception au principe d'information individuelle des personnes et des mesures appropriées seront mises en œuvre, notamment par la diffusion d'une information relative : - à la réutilisation des données issues de la base Fideli sur les site web du Conseil national de l'information statistique et du Comité du secret ; - aux projets de recherche sur le site web du responsable de traitement du « Baromètre de Santé publique France ». Ces modalités d'information seront mises en œuvre avant la constitution des bases de données par l'INSEE permettant la réalisation du tirage au sort. <i>S'agissant des personnes tirées au sort :</i> Elles recevront une note d'information individuelle par voie postale ou électronique.

	Toutes les notes d'information devront comporter l'ensemble des mentions prévues par l'article 13 du RGPD. <i>S'agissant des modalités d'exercice des droits :</i> <i>S'agissant du droit d'opposition :</i> Conformément aux dispositions de l'article 74 de la loi « informatique et libertés », les personnes disposent du droit de s'opposer au traitement de leurs données à des fins de recherche dans le domaine de la santé. Les personnes ayant refusé de participer au baromètre suite à la campagne d'information réalisée en amont du tirage au sort ne devront pas être contactées et leurs données ne pourront être traitées, y compris à des fins de redressement. Par ailleurs, les personnes s'opposant au traitement de leurs données au cours de l'étude ne devront pas être recontactées. <i>S'agissant du droit à l'effacement :</i> Conformément aux dispositions de l'article 17 du RGPD, le droit à l'effacement s'applique lorsque la personne concernée exerce son droit d'opposition et demande également l'effacement des données la concernant déjà collectées. Sous réserve d'une information préalable appropriée par le responsable de traitement, certaines données préalablement collectées peuvent cependant ne pas être effacées, si cette suppression est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs de la recherche. Ces modalités d'exercice des droits seront clairement décrites dans les différentes notes d'information. Les personnes concernées pourront exercer leurs droits auprès du délégué à la protection des données du responsable de traitement pendant toute la durée des traitements.
Sur les catégories de destinataires des données	Des documents tenus à jour indiquent la ou les personnes compétentes pour le responsable de traitement et le sous-traitant permettant de délivrer l'habilitation à accéder aux données, la liste des personnes habilitées à accéder à ces données, leurs profils d'accès respectifs et les modalités d'attribution, de gestion et de contrôle des habilitations. Ces catégories de personnes sont soumises au secret professionnel dans les conditions définies par les articles 226-13 et 226-14 du code pénal. La qualification des personnes habilitées et leurs droits d'accès doivent être régulièrement réévalués, conformément aux modalités décrites dans la procédure d'habilitation établie par le responsable de traitement et ses sous-traitants.

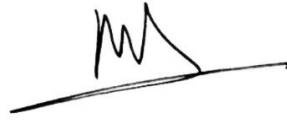
	<i>S'agissant des accédants aux données pseudonymisées :</i> Les membres du personnel de l'ANSP auront accès aux données de santé pseudonymisées des participants afin de réaliser l'analyse des données pour les besoins du baromètre. <i>S'agissant des destinataires des autres données :</i> Les employés de la société IPSOS auront accès aux données administratives d'identification (les données nominatives ainsi que les coordonnées postales, électroniques et téléphoniques) et de santé des participants pour : - réaliser l'information des participants ; - assurer le suivi des inclusions et le recueil des données à travers la passation des questionnaires. Les participants en sont informés. Les données directement identifiantes doivent être traitées et transmises de façon séparée des données de santé et être enregistrées dans une base de données distincte. En outre, seul un nombre strictement limité de personnes habilitées et soumises au secret professionnel pourront accéder aux données directement identifiantes. Les courriers électroniques adressés aux participants ne devront révéler aucune information sur leur état de santé réel ou supposé. Par ailleurs, les données administratives d'identification (nom, prénom, coordonnées téléphoniques, électroniques et postales) des participants acceptant d'être recontactés pour des études ancillaires seront conservées afin de leur proposer de participer à des études ultérieures. Aux fins de confidentialité, ces données devront être conservées uniquement par la société IPSOS.
--	--

Sur la sécurité des données et la traçabilité des actions	Le dossier de demande mentionne que le traitement envisagé est conforme aux mesures de sécurité prévues dans la MR-004. Le responsable de traitement a réalisé et transmis à l'appui de la demande d'autorisation une analyse d'impact relative à la protection des données spécifique aux traitements envisagés. Celle-ci devra être mise à jour pour tenir compte des différentes phases du baromètre (et notamment le redressement des données), préciser les mesures techniques et organisationnelles ainsi que le plan d'action retenu. Le responsable de traitement s'engage à ce que les serveurs internes utilisés soient conformes à l'état de l'art, notamment à des mesures de sécurité équivalentes aux exigences mentionnées dans le référentiel « entrepôt de données dans le domaine de la santé », pour constituer le baromètre. Des espaces projets devront être prévus pour toute mise à disposition des données. Seules des données anonymes pourront faire l'objet d'export hors de ces espaces. Si ces conditions ne sont pas réunies, aucune donnée du baromètre ne pourra être hébergée sur les serveurs internes du responsable de traitement. Les données seront alors consolidées, analysées et mises à disposition sur la plateforme du Centre d'accès sécurisé aux données (CASD). Le responsable de traitement devra s'assurer du respect des exigences de sécurité à toutes les étapes des traitements opérés par les différents organismes participants, y compris pour les fiches papier. Des pseudonymes aléatoires sont attribués aux participants. Ceux-ci seront dédiés à chaque typologie d'acteurs et distincts pour les différents flux de données. Toute table de correspondance devra être supprimée dans les meilleurs délais après consolidation de la base et génération de nouveaux pseudonymes aléatoires pour celle-ci. Pour toute mise à disposition, des pseudonymes dédiés à chaque espace projet devront être générés. Les échanges de données seront réalisés via des canaux de communication chiffrés et assurant l'authentification de la source et du destinataire. Les algorithmes de chiffrement utilisés et les procédures de gestion des clés devront être conformes à l'annexe B1 du référentiel général de sécurité. Les mesures de sécurité, qui devront être opérationnelles lors de la mise en œuvre du traitement, devront répondre aux exigences prévues par les articles 5.1.f) et 32 du RGPD, compte tenu des risques identifiés par le responsable de traitement.
--	---

	Il appartiendra au responsable de traitement de procéder à une réévaluation régulière des risques pour les personnes concernées et une mise à jour, le cas échéant, de ces mesures de sécurité. Le responsable de traitement devra s'assurer que son prestataire IPSOS mette en œuvre les mesures de sécurité nécessaires pour protéger la base de données nominatives transmises par l'INSEE.
Sur les transferts hors Union européenne	La présente décision ne vaut pas autorisation de transfert de données en dehors de l'Union européenne vers un pays ne présentant pas un niveau de protection adéquat.
Sur la durée de conservation des données	<i>S'agissant des personnes refusant de participer au baromètre malgré son caractère obligatoire :</i> Leurs données administratives d'identification (nom, prénom, coordonnées téléphoniques, électroniques et postales) devront être détruites au moment de leur refus. <i>S'agissant des données des personnes participant au baromètre et refusant d'être de nouveau contactées pour une étude ancillaire :</i> Leurs données administratives d'identification (nom, prénom, coordonnées téléphoniques, électroniques et postales) seront détruites dans un délai de six mois après la collecte des données. <i>S'agissant des données des personnes participant au baromètre et acceptant d'être de nouveau contactées pour une étude ancillaire :</i> Leurs données administratives d'identification (nom, prénom, coordonnées téléphoniques, électroniques et postales) seront détruites par la société IPSOS dans un délai d'un an après la passation des questionnaires. Les autres données du Baromètre de Santé publique France seront conservées en base active pour une durée de trente ans. À l'issue de ce délai, les données seront archivées pour une durée de cinquante ans puis versées aux Archives nationales, conformément aux dispositions du code du patrimoine. Eu égard aux caractéristiques du baromètre, ces durées de conservation des données n'excèdent pas les durées nécessaires aux finalités pour lesquelles elles sont collectées et traitées, conformément aux dispositions de l'article 5.1.e) du RGPD.

Autorise, conformément à la présente délibération, l'Agence nationale de santé publique à mettre en œuvre les traitements décrits ci-dessus pendant une durée de huit ans.

La Présidente

A handwritten signature in black ink, consisting of a stylized 'M' followed by a horizontal line that extends to the right.

Marie-Laure DENIS