Disponible en ligne sur
ScienceDirect
www.sciencedirect.com

Elsevier Masson France
EM|consulte
www.em-consulte.com

MÉDECINE & DROIT
INFORMATION ÉTHIQUE ET JURIDIQUE DU PRATICIEN

Médecine & Droit 2019 (2019) 103–111

Protection de la personne – Exercice professionnel

Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données

Health research, protection of personal data and General Data Protection Regulation

Frédérique Lesaulnier (Docteur en Droit, Déléguée à la protection des données de l'Inserm)

101, rue de Tolbiac, 75654 Paris cedex 13, France

Résumé

La France dispose d'un cadre juridique très riche qui définit les conditions d'accès, d'utilisation et de partage des données de santé à des fins de recherche scientifique et en assure la protection. Ce cadre juridique est aujourd'hui en cours de refonte. Le Règlement du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, directement applicable dans les États membres depuis le 25 mai 2018, doit être articulé avec les autres dispositions de l'UE applicables à la recherche et avec le droit national. Cela fait du RGPD un règlement sui generis à mi-chemin entre un règlement et une directive.

Mots clés : Données personnelles (protection) ; Protection des données de santé ; RGPD ; Loi Informatique et liberté ; Recherche scientifique (protection des données) ; Recherche dans le domaine de la santé (protection des données) ; Système national des données de santé (SNDS)

Abstract

France has a very rich legal framework, which defines the conditions of access and use of health data for scientific research purposes and ensures their protection. Currently, this legal framework is undergoing revision. The European regulation of April 27th 2016 on protection of natural persons in relation to the processing of personal data came into effect in EU member states since 25th May 2018 and substitute a rationale of administrative process for a rationale that empowers the researchers to document and prove compliance with the regulation ("accountability"). This regulation must be coordinated with the other regulation applicable to research in UE and with national law.

Keywords: Personal data (protection); Protection of personal data concerning health; GDPR; French Law "Informatique et Liberté"; Scientific research (data protection); Research in the field of health (Data protection); National Health Data System (NHDS)

La recherche dans le domaine de la santé connaît une révolution numérique du fait des masses considérables de données disponibles, collectées dans des environnements multiples et de la possibilité d'en extraire des corrélations et des connaissances grâce aux technologies capables d'augmenter les capacités de stockage et de traitement. Qu'il s'agisse de donneés scientifiques, de données issues du soin et du système de santé, de données médico-administratives recueillies initialement à des fins gestionnaires ou de données issues de l'utilisation d'objets connectés ou de l'usage d'internet, les données personnelles de santé sont un enjeu de premier plan pour la recherche dans le domaine de la santé. Elles sont le matériau de recherche de base pour les scientifiques et ces données représentent un fort potentiel de contribution à la santé individuelle et collective. C'est pourquoi le progrès de la connaissance au service de la santé et de la société passe par l'accès, l'utilisation et le partage de ces données dans le respect de la protection des personnes. Cela suppose que ces données sensibles soient exploitées avec la plus grande rigueur, l'expertise et l'esprit critique nécessaires et dans le respect du cadre éthique, légal et réglementaire.

Adresse e-mail : Frederique.lesaulnier@inserm.fr

https://doi.org/10.1016/j.meddro.2018.10.001
1246-7391/

Or, le contexte normatif dans lequel s'inscrivent les activités de recherche est en plein bouleversement. La réglementation relative à la protection des données personnelles est emblématique de ces « turbulences normatives » tant au plan européen que national.

Le Règlement européen 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 (ci-après RGPD[1]) est devenu le texte de référence dans l'ensemble des États membres de l'Union européenne (UE) depuis le 25 mai 2018. Grâce à la disposition relative au « ciblage », les acteurs situés en dehors de l'UE ne pourront pas s'affranchir de ces règles dès lors qu'ils traitent des données relatives aux résidents européens.

Ce règlement est applicable directement sans transposition nationale. Toutefois, il laisse d'importantes marges de manœuvre aux États membres pour maintenir ou adopter des spécificités nationales pour certains types de traitements parmi lesquels les traitements qui portent sur les données de santé, les données génétiques, le numéro d'identification national et les traitements à des fins de recherche scientifique (RGPD, art. 9.4 éclairé par le considérant 156). Le législateur français a fait usage de ce pouvoir de subsidiarité. La loi fondatrice du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés)[2] a été modifiée par la loi du 20 juin 2018 relative à la protection des données personnelles[3] et ainsi adaptée au nouveau cadre européen.

La loi Informatique et Libertés consacre désormais un nouveau chapitre IX aux traitements de données à caractère personnel dans le domaine de la santé applicable aux recherche, études et évaluations dans ce domaine. La bonne compréhension du cadre juridique suppose donc d'**articuler le RGPD avec la loi nationale**. La technique retenue aboutit à un résultat peu satisfaisant en termes de lisibilité du droit pour les acteurs. C'est pourquoi le Gouvernement a été autorisé à effectuer par voie d'ordonnance ultérieure une mise en cohérence de l'ensemble de la législation applicable en matière de protection des données personnelles (LIL, art. 32).

En outre, en matière de recherche dans le domaine de la santé, la nouvelle loi Informatique et Libertés doit elle-même être articulée avec les autres dispositions de l'UE applicables à la recherche, notamment le Règlement européen du 16 avril 2014 relatif aux essais clinique de médicaments,[4] et le cadre national applicable et, notamment, les dispositions du code de la santé publique issues de la loi du 26 janvier 2016 de modernisation de notre système de santé[5] qui crée le Système National des Données de Santé (SNDS) et la réglementation applicable aux recherches impliquant la personne humaine (RIPH) issue de la loi du 5 mars 2012[6] et de l'ordonnance du 16 juin 2016[7].

Il en résulte un cadre juridique relatif à la protection des données personnelles applicable à la recherche dans le domaine de la santé complexe et difficile à appréhender pour les communautés de recherche qui, accompagnées des institutions dont elles relèvent, doivent s'y conformer.

1. Le RGPD et la place que les activités de recherche scientifique y occupent

1.1. Vers une responsabilisation accrue des acteurs

Le RGPD est un acte normatif de portée générale qui n'est propre ni à la santé, ni à la recherche.

Ce texte modifie l'approche de la protection des données personnelles en s'invitant au cœur de la stratégie, de la gouvernance et de l'organisation des acteurs et en instaurant une nouvelle façon d'appréhender la protection des données personnelles. Alors que le régime de protection des données antérieur reposait en grande partie sur l'existence de formalités préalables, le RGPD repose sur une **logique de conformité et de responsabilité**. Il ne s'agit plus seulement pour les acteurs d'effectuer des demandes d'autorisation auprès de la CNIL, ils doivent aussi s'assurer, au moment du montage d'un projet qui implique un traitement de données personnelles, puis tout au long de la vie du projet du respect des principes de protection des données et, surtout, ils doivent à tout moment être en mesure de le démontrer en cas de contrôle de la CNIL.

Cela suppose le développement de politiques de conformité (dites d'« accountability ») placées sous le pilotage d'un délégué à la protection des données (DPD), dont la désignation est obligatoire pour les autorités et organismes publics, pour les organismes dont les activités principales les amènent à réaliser un suivi régulier et systématique à grande échelle des personnes concernées ou à traiter à grande échelle des données de santé qui font partie des catégories particulières de données mentionnées à l'article 9 du RGPD (art. 37).

Ces politiques doivent se traduire concrètement par le développement d'une gouvernance de la donnée, un travail documentaire, la mise en œuvre et la formalisation de procédures, l'utilisation d'outils et la réalisation d'audits, la mise en place de mesures de sensibilisation et de formation permettant d'attester du niveau de conformité. Le règlement met en effet à la charge des responsables de traitement, ainsi que des sous-traitants, des obligations nouvelles et alourdit fortement les sanctions administratives que pourront prononcer les autorités de contrôle en cas de manquements ou de violations des nouvelles règles

[1] 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 »).

[2] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[3] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[4] Règlement (UE)536/2014 du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE. Règlement (UE) 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux.

[5] Loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, art. 193.

[6] Loi n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine.

[7] Ordonnance n° 2016-800 du 16 juin 2016 relative aux recherches impliquant la personne humaine.

(jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial d'une entreprise).

1.2. Une évolution plus qu'une révolution dans la régulation

Pourtant, il faut voir dans le RGPD **une évolution bien plus qu'une révolution**. Il existe un cadre juridique riche et ancien qui définit les conditions d'accès et d'utilisation des données personnelles de santé et qui traduit le **caractère sensible** de ces données.

Ce cadre général de la protection des données repose en Europe sur le principe selon lequel la protection des données à caractère personnel est un droit fondamental inscrit dans la loi (Charte des droits fondamentaux de l'Union européenne, art. 8§1).

L'application de ce cadre juridique est subordonnée, d'une part, à l'**existence de données à caractère personnel**, susceptibles de permettre d'identifier la personne, que cette identification soit directe ou indirecte par référence à un identifiant ou tout élément qui lui soit propre et qui, seul ou avec d'autres (un faisceau de données), permet de remonter à son identité[8]. Aux termes du considérant 26, le Réglement n'est pas applicable aux données anonymes, qu'elles le soient initialement ou qu'il s'agisse de données à caractère personnel qui ont donné lieu à une anonymisation. La possibilité d'identifier les personnes s'apprécie en Europe au regard des moyens **raisonnablement** susceptibles d'être utilisés par le responsable de traitement ou par toute autre personne. Elle passe par la prise en considération de facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, les technologies disponibles, présentes mais aussi à venir, ce qui suppose de la part des acteurs des réévaluations régulières de la robustesse de l'anonymat et la documentation des analyses. L'application de ce cadre juridique suppose, d'autre part, **une action sur ces données**, un traitement de données entendu au sens large.

Les **données de santé**, parce qu'elles relèvent de l'intimité de la vie privée des personnes, sont des données qui doivent faire l'objet d'une protection particulière. À ce titre, le droit leur reconnaît un statut particulier et impose le respect de règles ayant pour objet de garantir leur confidentialité. Elles sont ainsi soumises à un principe d'interdiction de traitement, sauf pour un certain nombre d'exceptions qui permettent ce traitement, prévues par la loi et assorties de garanties (de fond et de procédure) au respect desquelles une autorité administrative indépendante veille.

Ces principes de fond sont les suivants : une finalité de traitement déterminée, explicite et légitime, des données adéquates, pertinentes et proportionnées au regard de l'objectif poursuivi (principe de minimisation des données), une durée de conservation déterminée à l'avance et dont la pertinence est appréciée au regard de cette finalité (droit à l'oubli), le respect des droits des personnes qui passe en premier lieu par le principe de loyauté et de transparence à l'égard de la personne concernée et enfin, la mise en place de mesures de sécurité de nature à garantir la confidentialité des données.

Les principes posés demeurent pour l'essentiel inchangés dans le RGPD (art. 5) (Fig. 1).

À noter toutefois que la sécurité des données personnelles est érigée par le RGPD en condition de licéité des traitements et le renforcement des règles en la matière accentue fortement cette dimension[9] (art. 5.1.f). C'est une composante majeure de la conformité des traitements à la législation de protection des données s'agissant du traitement de données de santé à caractère personnel.

Les données de santé figurent toujours dans la liste des « catégories particulières de données »[10] et les données génétiques, qui étaient considérées par la CNIL comme des données sensibles, y sont désormais expressément mentionnées (art. 9). La nouveauté est que l'on y trouve désormais **une définition très large des données de santé à l'échelle européenne**. Les « données concernant la santé » sont ainsi définies comme « *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* » (RGPD, art. 4 éclairé par le considérant 35). Celles-ci ne concernent plus seulement les données qui permettent d'indiquer la pathologie dont peut être atteint un individu (données de santé « par nature »). Elles sont étendues à toute donnée sur l'état de santé physique et mentale, présent, passé ou futur de la personne, toute information sur l'identification du patient dans le système de soins, toutes les prestations de services de santé, toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source (données de santé « par destination »). Les données génétiques sont également définies comme « *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* » (art. 4.13).

Sur la pseudonymisation dont il donne une définition, le Règlement est très clair : **les données pseudonymisées sont des données à caractère personnel indirectement identifiantes**[11]. Par conséquent, la pseudonymisation des données (qui n'est pas une anonymisation) ne conduit pas à soustraire ces données à l'application du règlement[12]. En outre, parce que c'est

[8] Sur la notion de donnée à caractère personnel, F. Lesaulnier, *L'information nominative*, thèse Paris II, 2005 ; F. Lesaulnier, La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles : Dalloz IT/IP 2016, 573.

[9] Obligation de mener des analyses d'impact sur la vie privée et les libertés (PIA) pour les traitements qui présentent un risque élevé pour les droits et libertés des personnes ; Privacy by design, privacy by default.

[10] J. Bossi-Malafosse, Le traitement des données de santé et le Règlement européen sur la protection des données du 27 avril 2016, Communication Commerce électronique, avril 2018, nº 4, étude nº 12.

[11] Considérant 26.

[12] Considérant 28.

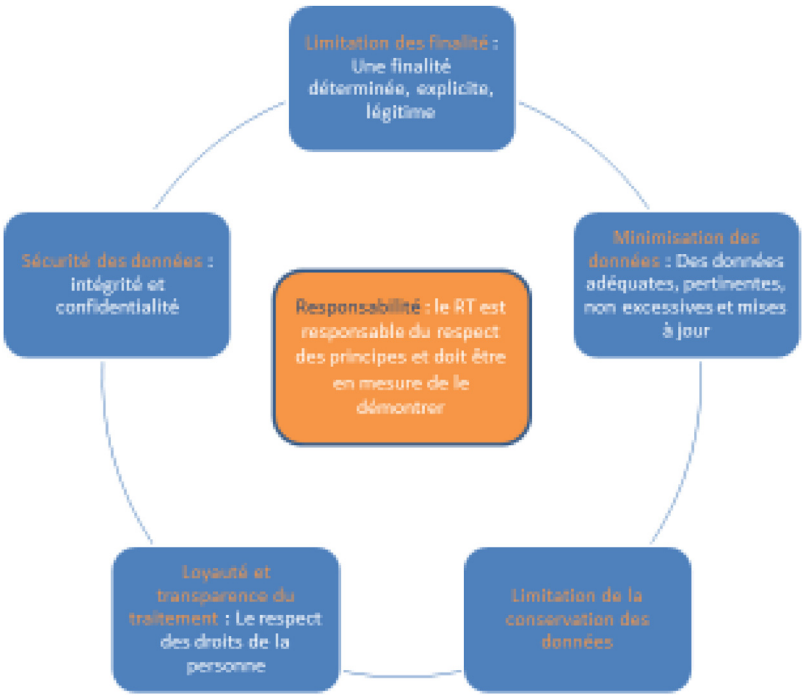

Fig. 1. Principes fondamentaux de la protection des données personnelles reconduits et renforcés.

un moyen de réduire les risques pour les personnes[13], plusieurs dispositions du Règlement témoignent des faveurs du législateur européen pour la pseudonymisation apparaît comme une garantie inhérente aux traitements de données à des fins de recherche scientifique dès lors qu'elle est compatible avec la finalité du traitement (art. 89).

La « pseudonymisation » est définie comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable* » (art. 4, 5).

La pseudonymisation est donc un traitement qui consiste à dissimuler l'identité, sans la faire disparaître. Elle suppose deux conditions cumulatives :

- une conservation séparée des clés de réidentification ;
- des mesures techniques et organisationnelles tendant à empêcher la réidentification.

Cette définition permet de couvrir différentes techniques couramment utilisées en matière de recherche en santé :

- le recours à une table de correspondance entre le jeu de données pseudonymes et les données d'identité conservées séparément, classiquement utilisée dans les essais cliniques ;
- les fonctions de hachage utilisées avec un secret qui permettent de chaîner des données relatives à un individu dans le temps sans permettre de l'identifier, sont centrales dans le domaine de la recherche en santé et la CNIL en a encouragé le développement. Ainsi le suivi épidémiologique du sida dans les années 1985–1990 s'est fait sous l'égide de l'Institut national de Veille Sanitaire (devenue Santé Publique France) sous la garantie d'un haut niveau de sécurité obtenu par un double dispositif de hachage des éléments d'identité des personnes. Il en va de même du Système National d'Information Interrégimes de l'Assurance Maladie (SNIIRAM) qui est une base nationale créée en 1998 par la loi, qui recense tous les actes médicaux, les prestations effectuées et les pathologies en ville et à l'hôpital pour mieux connaître l'évolution des dépenses de santé[14].

1.3. Place des activités de recherche scientifique dans le RGPD

Plusieurs dispositions du RGPD témoignent d'une prise en considération des enjeux de la recherche scientifique et en favorisent la réalisation.

Le considérant 159 donne une définition très large de ce que recouvre la notion de « recherche scientifique » : « *Aux fins du présent règlement, le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé. Il devrait, en outre, tenir compte de l'objectif de l'Union*

[13] Considérants 28 et 29.

[14] CNIL, Délibération n° 01-054 du 18 octobre 2001.

mentionné à l'article 179, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, consistant à réaliser un espace européen de la recherche. Par fins de recherche scientifique, il convient également d'entendre les études menées dans l'intérêt public dans le domaine de la santé publique ».

1.3.1. Une dérogation au principe d'interdiction de traiter des catégories particulières de données au bénéfice de la recherche scientifique

Le RGPD reprend le principe d'interdiction de traitement des données « sensibles » ainsi que les dérogations à ce principe (prévues à l'article 9.2) parmi lesquels on retrouve les motifs d'intérêt public y compris dans le domaine de la santé publique et la recherche scientifique et les statistiques, moyennant un certain nombre de garanties mentionnées à l'article 89 (art. 9-2-j).

Le RGPD souligne explicitement l'importance et l'intérêt pour la société des traitements effectués à des fins de recherche scientifique ou historique (considérants 156 et 157[15]) et le texte insiste sur la légitimité des activités de recherche, à condition qu'elles respectent les garanties appropriées prévues dans le droit de l'Union ou le droit des États membres.

1.3.2. Une présomption de compatibilité de la finalité de recherche scientifique avec une finalité initiale différente et la possibilité de conservation à ces fins au-delà de la réalisation de la finalité du traitement

Le RGPD exige que les données soient « *collectées pour des finalités déterminées, explicites et légitimes* », *et ne soient pas*« *traitées ultérieurement de manière incompatible avec ces finalités* ». Toutefois, il pose le principe d'une **présomption de compatibilité des traitements ultérieurs à des fins** statistiques, **de recherche scientifique** ou historique moyennant certaines garanties (RGPD, art. 5 b). La loi « Informatique et Libertés » contient une disposition similaire (art. 6. 2).

Cette présomption dispense les chercheurs de collecter eux-mêmes les données sur la base du consentement des personnes pour le nouveau traitement mis en place, ce qui ne les dispense pas d'informer les personnes concernées et d'obtenir une autorisation s'il y a lieu.

De la même manière, la durée de conservation initiale des données peut être prolongée pour répondre aux fins de recherche scientifique. Le RGPD prévoit que les données ne peuvent être conservées « *sous une forme permettant l'identification des personnes concernées* » que pendant « *une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* » Néanmoins, une dérogation est admise à ce principe de limitation de la durée de conservation lorsque les traitements sont réalisés à des fins de recherche scientifique sous réserve de la mise en œuvre de mesures techniques et organisationnelles appropriées (art. 5-1-c).

1.3.3. Des modalités d'exercice des droits adaptées aux enjeux de la recherche scientifique

Les **droits des personnes concernées** sur les données qui les concernent sont **réaffirmés et renforcés** par le RGPD et participent des principes de **transparence** et de **loyauté** à leur égard (art. 12).

Il est rappelé à titre liminaire que l**e consentement des personnes n'est pas systématiquement requis pour les traitements de données à des fins de recherche scientifique**. Comme la loi Informatique et libertés, le Règlement prévoit que chaque traitement de données personnelles repose sur un ou plusieurs conditions qui en fondent la licéité dont la liste est énumérée à l'article 6. Le consentement est l'une de ces bases légales au même titre que l'exécution d'une mission d'intérêt public, le respect d'une obligation légale. . . Le point de savoir si le consentement de la personne est requis dépend donc de la qualification réglementaire de la recherche et le consentement lorsqu'il est requis ne constitue pas pour autant nécessairement la base légale du traitement.

Le RGPD permet le recueil d'un consentement « pour une ou plusieurs finalités spécifiques » (art. 6.1.a) ce qui suppose que les finalités aient été déterminées et que la personne concernée en ait été informée. Il résulte de la lecture du considérant 33 du Règlement qu'une finalité spécifique est compatible avec un consentement global. Ce considérant prévoit, en effet, que les personnes concernées devraient pouvoir donner leur consentement « *pour ce qui concerne certains domaines de la recherche scientifique dans le respect des normes éthiques reconnues en matière de recherche scientifique* ». La personne concernée serait alors en mesure d'accepter que ses données soient utilisées dans le cadre de différents projets de recherche susceptibles d'être menés dans une branche ou un domaine particulier. À noter toutefois que les considérants apportent des précisions qui permettent d'éclairer sur l'esprit du texte mais ne priment pas sur les articles du Règlement.

Lorsque les recherches sont, en raison de leur qualification réglementaire, soumises à un régime d'opposition, la personne concernée a le droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant, toutefois une dérogation est prévue lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public (art. 21.6).

Ces dispositions doivent être conciliées avec le principe d'une **information individuelle et spécifique à chaque projet**. L'information délivrée à la personne qui participe à la recherche doit être délivrée de façon concise, transparente, compréhensibles et aisément accessibles, en des termes clairs et simples et

[15] C. 156 : « *En combinant les informations issues des registres, les chercheurs peuvent acquérir de nouvelles connaissances d'un grand intérêt en ce qui concerne des problèmes médicaux très répandus tels que les maladies cardiovasculaires, le cancer et la dépression. Sur la base des registres, les résultats de la recherche peuvent être améliorés car ils s'appuient sur un échantillon plus large de population. Dans le cadre des sciences sociales, la recherche sur la base des registres permet aux chercheurs d'acquérir des connaissances essentielles sur les corrélations à long terme existant entre un certain nombre de conditions sociales telles que le chômage et l'éducation et d'autres conditions de vie. Les résultats de la recherche obtenus à l'aide des registres fournissent des connaissances fiables et de grande qualité qui peuvent servir de base à l'élaboration et à la mise en œuvre d'une politique fondée sur la connaissance, améliorer la qualité de vie d'un certain nombre de personnes et renforcer l'efficacité des services sociaux. Pour faciliter la recherche scientifique, les données à caractère personnel peuvent être traitées à des fins de recherche scientifique sous réserve de conditions et de garanties appropriées prévues dans le droit de l'Union ou le droit des États membres* ».

elle doit comporter l'ensemble des mentions figurant aux articles 13 et 14 du RGPD qui **renforcent les obligations de transparence que les données soient collectées auprès de la personne concernée ou non** (collecte indirecte des données).

Le rôle des patients ou des personnes à l'origine des données est majeur et leurs droits à être informés et à donner leur accord à la réutilisation des données et échantillons doit être respecté. Pourtant, l'exigence d'une information individuelle et spécifique à chaque projet issu de ces données et/ou échantillons est difficilement compatible avec les projets reposant sur une réutilisation secondaire renouvelée et réitérée de données ou d'échantillons biologiques faiblement identifiants, collectés à cette fin. C'est le cas des biobanques ou des cohortes, notamment celles financées par le programme investissement d'avenir, qui ont vocation à mettre leurs données à la disposition de la communauté des chercheurs. Une telle information, dans le cadre de ce type d'infrastructure, ne permet pas à la personne constamment sollicitée de disposer d'une vue d'ensemble de l'utilisation des données qui la concernent.

C'est pourquoi il est indispensable de concevoir des modalités d'exercice des droits souples et dynamiques, susceptibles de permettre aux infrastructures de répondre aux enjeux d'une meilleure compréhension des mécanismes pathologiques par exemple, tout en garantissant une meilleure maîtrise par les personnes de leurs données, ce qui participe de la confiance indispensable des personnes concernées. Il est également souhaitable que les patients ou leurs représentants intègrent les structures de gouvernance des infrastructures qui permettent l'utilisation secondaire des données (cohorte, biobanques) et participent à l'élaboration du projet, des principes directeurs et des procédures d'accès mises en place.

Comme le souligne Georges Dagher au sujet des biobanques, « *(. . .) il est temps de repenser le rôle des personnes-sources plus largement en termes de participation et de contribution à la recherche (. . .). Le nouveau paradigme développé par l'utilisation des collections biologiques et visant à créer une ressource pour la recherche invite à une évolution du cadre réglementaire et éthique qui régit la question de la participation des patients aux projets de recherche (. . .)* »[16].

Il faut saluer l'évolution de la doctrine de la CNIL sur ce point, illustrée par le projet de méthodologie de référence MR004[17]. Celle-ci admet que des données et/ou des échantillons biologiques puissent faire l'objet d'une réutilisation et que l'information puisse être considérée comme valablement délivrée dès lors que les personnes avaient été informées de la réutilisation possible de leurs données et/ou échantillons biologiques lors de la collecte initiale et que l'information initiale renvoie à un dispositif spécifique d'information tel qu'un site internet auquel les personnes pourront se reporter avant la mise en œuvre d'un nouveau traitement. Ce type d'approche qui apparaît conforme au rapport du Comité international de bioéthique (CIB) du 15 septembre 2017[18], apparaît de nature à favoriser l'utilisation des données en recherche tout en préservant l'autonomie des patients qui deviennent des parties prenantes au projet.

À noter également le **maintien de la possibilité de déroger à l'obligation d'information individuelle en cas de réutilisation secondaire des données** lorsque la fourniture des informations « *se révèle impossible ou exigerait des efforts disproportionnés* », ou dans la mesure où l'obligation d'information « *est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement* » sous réserve de garanties appropriées, notamment de pseudonymisation (art. 14.5.b). Le considérant 62 précise que devraient être pris en considération le nombre de personnes concernées, l'ancienneté des données, ainsi que les garanties appropriées éventuelles adoptées. Cette disposition peut trouver à s'appliquer pour les méta-analyses sur données individuelles par exemple. Toutefois, l'absence d'information des personnes rendra la recherche non éligible aux méthodologies de référence en l'état de leur rédaction.

Le droit à l'effacement des données est susceptible d'entrer en contradiction avec les exigences méthodologiques d'une recherche, la sécurité des participants à des essais cliniques ou des obligations légales qui incombent au responsable de la recherche. Aux termes de l'article 17 du RGPD, et du considérant 65, le « **droit à l'effacement** » **ne s'applique pas** et la conservation ultérieure des données à caractère personnel déjà collectées peut être licite dès lors que le traitement le traitement des données personnelles est nécessaire à des fins de recherche scientifique, conformément à l'article 89, **dès lors que** « ***l'exercice de ce droit risque de rendre impossible ou de compromettre gravement la réalisation des objectifs du traitement*** »(art. 17.3 d)[19].

Cela suppose la mise en œuvre de garanties appropriées pour les droits et libertés des personnes qui peuvent comprendre la pseudonymisation, voire l'anonymisation des données, dans la mesure où les finalités peuvent être atteintes de cette manière et par une information des personnes concernées sur ce point au moment où elles donnent leur accord pour participer à l'étude.

1.3.4. La promotion de codes de conduites sectoriels élaborés en lien avec les communautés scientifiques concernées

Le RGPD fait la promotion des codes de conduite sectoriels, construits avec les acteurs de terrain et fondés sur les retours d'expérience (art. 40). Les organismes de recherche en lien avec les communautés scientifiques ont un rôle majeur à jouer afin de bâtir avec le régulateur une co-régulation exigeante et efficace

[16] Le Monde paru dans le supplément Sciences & Santé du mercredi 8 juillet 2015.

[17] Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004).

[18] http://unesdoc.unesco.org/images/0024/002487/248724f.pdf.

[19] L'article 28.3 du Règlement (UE) n° 536/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux essais cliniques de médicaments à usage humain et abrogeant la directive 2001/20/CE prévoit : « *Sans préjudice de la directive 95/46/CE, le retrait du consentement éclairé n'a pas d'incidence sur les activités déjà menées et sur l'utilisation des données obtenues sur la base du consentement éclairé avant que celui-ci ne soit retiré* ».

qui prenne en compte les évolutions scientifiques et techniques de la recherche et qui soit conforme aux réalités du terrain. En ce sens, la CNIL mène des concertations auprès des acteurs de la recherche sur l'élaboration de projets de méthodologies de référence destinés à encadrer les pratiques. L'Inserm s'est ainsi avec d'autres acteurs de la recherche fortement mobilisé en lien avec les communautés de recherche pour apporter une réponse à la consultation lancée par la CNIL aux projets de méthodologies de référence[20] et s'implique activement dans l'élaboration de codes de conduites.

2. L'impact de la loi du 6 janvier 1978 modifiée en 2018 sur la recherche dans le domaine de la santé

La France a usé des marges de manœuvre laissées aux États membres en prévoyant dans le cadre de la nouvelle loi « Informatique et Libertés » un nouveau chapitre IX intitulé « Traitements de données à caractère personnel dans le domaine de la santé ». Ce nouveau chapitre introduit un régime général applicable à l'ensemble des traitements de données de santé (section 1) ainsi que des dispositions spécifiques additionnelles applicables aux traitements réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé (section 2).

Les traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé sont soumis aux dispositions de ces deux sections, sauf dérogations des dispositions spécifiques de la section 2 aux dispositions générales de la section 1.

2.1. Le maintien d'un régime d'autorisation pour les traitements réalisés à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé

Les procédures administratives d'accès aux données nécessaires aux traitements relatifs à la recherche dans le domaine de la santé demeurent complexes malgré les avancées de la loi de modernisation de notre système de santé et de la loi Informatique et libertés modifiée.

Un régime d'autorisation est maintenu pour les recherches, études et évaluations dans le domaine de la santé, à moins que les traitements ne soient réalisés par des personnels soumis au secret professionnel assurant le suivi médical afin d'effectuer des études destinées à leur usage exclusif (art. 53). D'autres types de recherche telles que les recherches en sciences humaines et sociales (sur l'insertion professionnelle, les discriminations, la diversité ethnique. . .) ou les recherches menées sur internet à partir de données qui ne sont pas sensibles a priori mais qui peuvent le devenir pas recoupement (données prédictives de comportement) ne sont pas soumises à un régime semblable.

Le maintien par la loi précitée de cette procédure complexe spécifique à la recherche *dans le domaine de la santé* qui fait intervenir des organismes distincts selon que la recherche implique ou non la personne humaine (CPP[21], CEREES[22] et INDS[23] le cas échéant) (LIL, art. 64), contraste avec l'esprit d'allègement des formalités porté par le Règlement. Elle vient en complément de l'auto-régulation des pratiques qui incombe désormais aux acteurs et pose, en l'état, la question des moyens nécessaires à cette double exigence.

Toutefois, trois évolutions notables méritent d'être soulignées :

- la possibilité pour la CNIL d'homologuer des référentiels, règlements types et méthodologies de référence en concertation avec les organismes publics et privés représentatifs (et avec l'INDS qui se substitue au CEREES) est maintenue et ces normes deviennent le principe. À terme, avec la multiplication des normes de simplification homologuées par la CNIL, les démarches à effectuer auprès d'elle vont diminuer. Il est nécessaire de poursuivre l'élaboration de nouvelles normes simplifiées qui s'inscrivent dans l'esprit du RGPD en concertation avec les organismes de recherche représentatifs et que les acteurs développent en interne des outils permettant de garantir et de documenter la conformité à ces normes ;
- le silence de la CNIL après deux mois, renouvelables une fois, vaut acceptation à condition toutefois que l'avis ou les avis rendus préalablement soient « expressément favorables » (art. 54). À cet égard, il est précisé qu'un avis favorable avec recommandations reste un avis expressément favorable ;
- l'article L. 1131-1-1 du Code de la santé publique et la loi Informatique et Libertés ont été mis en cohérence sur les modalités de l'accord de la personne à l'utilisation secondaire d'échantillons génétiques pour examen des caractéristiques génétiques à des fins de recherche scientifique (art. 63). Il est rappelé que ce texte institue une dérogation aux dispositions des articles 16-10 du Code civil et L. 1131-1 du Code de la santé publique afin de dispenser les chercheurs, sous des conditions très encadrées, de requérir le consentement exprès d'une personne pour examiner ses caractéristiques génétiques à partir d'un échantillon biologique prélevé à d'autres fins dans le cadre de projets susceptibles de présenter un intérêt sur le plan scientifique. Cette mise en cohérence avait été préconisée par le Conseil d'État dans son étude sur « La révision des lois de bioéthique »[24].

2.2. Des conditions d'accès et de sécurité particulières pour le système national des données de santé

L'article 193 de la loi du 26 janvier 2016 de modernisation de notre système de santé crée le système national des données de santé (SNDS) qui rassemble différentes bases médico-administratives et prévoit des règles particulières d'accès et d'appariement à ces données pour des finalités d'intérêt public moyennant un renforcement des règles de sécurité[25].

[20] Publiées au JO du 13 juillet 2018.
[21] Comité de protection des personnes.
[22] Comité d'Expertise pour les Recherches, les Études et les Évaluations dans le domaine de la Santé (CEREES).
[23] Institut national des données de santé.
[24] La Documentation française, 2009, p. 77 à 82.
[25] M. Girard et D. Polton, *La nouvelle réglementation sur l'accès aux données de santé et sa mise en œuvre deux ans après la loi de modernisation de notre*

Piloté par le ministère de la santé et géré par la Caisse nationale de l'assurance maladie des travailleurs salariés (Cnam), le SNDS permettra de chaîner les données de l'assurance maladie (base SNIIRAM[26] gérée par la Cnam), les données des établissements de santé (base PMSI[27] gérée par l'ATIH[28]), les données des causes médicales de décès (base gérée par l'INSERM), les données relatives au handicap (en provenance des MDPH[29], gérée par la CNSA[30]), un échantillon de données en provenance des organismes complémentaires d'assurance maladie (CSP, art. L. 1461-1-I).

Les données du SNDS couvrent la totalité de la population française. Elles offrent la possibilité d'un suivi sans nécessité de réinterroger directement les personnes et permettent de disposer d'informations sur les personnes « perdues de vue » lors d'un suivi longitudinal.

Elles offrent un potentiel pour la santé publique et la recherche considérable que les données soient utilisées seules ou appariées à d'autres sources de données, telles que les cohortes ou les registre de morbidité.

À cet égard, la loi de modernisation de notre système de santé (art. 193) a consacré une réelle avancée pour la recherche en santé en substituant, pour l'utilisation du NIR à des fins de recherche, une autorisation de la CNIL prise sur le fondement du chapitre IX de la loi Informatique et Libertés à un décret en Conseil d'État pris après avis de la CNIL[31]. En effet, la clé d'accès aux fichiers de l'assurance maladie et de l'assurance vieillesse est le numéro d'inscription au Répertoire national d'identification des personnes physiques (NIR), communément appelé « numéro de sécurité sociale » (ou un dérivé). Disposer du NIR des personnes enquêtées permet donc de reconstituer le pseudonyme utilisé dans le SNDS et de faciliter l'appariement des données de l'enquête avec les données du SNDS.

Un accès aux données à caractère personnel du SNDS ne peut être autorisé que pour permettre des traitements à des fins de recherche, d'étude ou d'évaluation répondant à un motif d'intérêt public et contribuant à l'une des finalités prévues par la loi parmi lesquelles figure la recherche, les études, l'évaluation et l'innovation dans les domaines de la santé et de la prise en charge médico-sociale.

Deux finalités de traitement sont interdites :

- la promotion des produits de santé en direction des professionnels de santé ou d'établissements de santé ;
- l'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque.

Il existe deux types d'accès aux données potentiellement identifiantes concernant le SNDS :

- des accès permanents sont reconnus aux « services de l'État, établissements publics et organismes » (listés par décret du 26 décembre 2016[32]) en raison de leurs missions de service public et selon un périmètre défini ;
- des accès « standards », ponctuels spécifiquement liés à un projet de recherche, étude et évaluation, autorisés par la CNIL sur le fondement du chapitre IX section 2 de la loi Informatique et Libertés.

L'accès des entreprises produisant ou commercialisant des produits de santé et des assureurs en santé aux données du SNDS est désormais possible, mais encadré par la loi.

Les données sont traitées et mises à disposition dans des conditions de sécurité conformes à un référentiel de sécurité applicable à tout système destiné à traiter des données du SNDS (SNDS, bases « sources » et bases « filles ») et assurant la confidentialité, l'intégrité des données et la traçabilité des accès et des autres traitements[33]. Un comité d'audit du système national des données de santé (SNDS) est mis en place afin de renforcer la bonne application des règles de sécurité et de protection des données pour le SNDS en complément des contrôles opérés par la CNIL, et dans le respect des missions et des pouvoirs de celle-ci (LIL, art. 65). Sa composition et son fonctionnement ont été précisées par le décret d'application de la loi Informatique et Libertés du 1er août 1978[34].

Le développement de solutions d'hébergement et de mise à disposition sécurisées et mutualisées permettant de garder la maîtrise des données et présentant des garanties de conformité technique et réglementaire certifiées est indispensable, mais suppose un changement de paradigme et d'importants moyens. À cet égard, les attentes sont fortes concernant le Health Data Hub qui s'inscrit dans le cadre du plan national sur l'intelligence artificielle pour valoriser les données de santé dans des environnements sécurisés et pour fluidifier davantage les procédures d'accès[35]. Des adaptations du cadre réglementaire paraissent

système de santé, Journal du Droit de la Santé et de l'Assurance Maladie, 2018, nº 20, p. 28.

[26] Système national d'information inter-régimes de l'Assurance maladie.

[27] Programme de médicalisation des systèmes d'information.

[28] Agence technique de l'information sur l'hospitalisation.

[29] Maisons départementales des personnes handicapées.

[30] Caisse nationale de solidarité pour l'autonomie.

[31] La CNIL a ainsi permis à l'Inserm–ANRS d'apparier les données du SNDS avec les données de la cohorte ANRS CO22 HEPATHER : Délibération CNIL nº 2018-300 du 19 juillet 2018 autorisant la modification du traitement mis en œuvre par l'Inserm ayant pour finalité une étude portant sur les bénéfices et les risques associées aux différentes modalités de prise en charge thérapeutique des hépatites B et C.

[32] Décret nº 2016-1871 du 26 décembre 2016 relatif au traitement de données à caractère personnel dénommé « système national des données de santé ».

[33] Arrêté du 22 mars 2017 relatif au référentiel de sécurité applicable au Système national des données de santé.

[34] Décret nº 2018-687 du 1er août 2018 pris pour l'application de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[35] À la suite de la remise du rapport Villani, le Président de la république avait annoncé que la santé serait un des secteurs prioritaires pour le développement de l'intelligence artificielle. Agnès Buzyn a lancé, le 16 mai 2018, une mission de préfiguration afin de créer un « Health Data Hub » et d'élargir le système national de données de santé. Cette mission a rendu ses conclusions à la ministre le 12 octobre 2018. https://solidarites-sante.gouv.fr/IMG/pdf/181012_-_rapport_health_data_hub.pdf.

ainsi nécessaires pour faciliter les appariements à partir du NIR utilisé comme identifiant national de santé et pour permettre la constitution d'entrepots de données appariées au SNDS à des fins de recherche.

2.3. Le cumul des règles d'application territoriale dans un contexte collaboratif national et et international

Le législateur a choisi d'instaurer un critère de rattachement territorial particulier pour les spécificités françaises. La loi française s'applique « *dès lors que la personne concernée réside en France* », et ce « *y compris lorsque le responsable de traitement n'est pas établi en France* ».

L'article 5-1 vise spécifiquement les règles nationales prise en application du RGPD, dans le cadre des marges de manœuvre laissées par le règlement aux États membres, correspondant notamment aux dispositions du chapitre IX de la LIL.

Ainsi, en application de l'article 5-1 de la LIL, le chapitre IX section 2 a vocation à s'appliquer dès lors qu'une personne concernée par le traitement *réside* en France, quel que soit le lieu d'établissement du responsable de traitement.

Le RGPD quant à lui s'applique dans deux cas :

- l'existence d'un établissement du responsable du traitement ou du sous-traitant sur le territoire de l'Union que le traitement ait lieu ou non sur le territoire de l'Union ;
- le fait que le traitement cible des résidents européens (offre de biens ou de services de personnes dans l'Union ou suivi de leur comportement au sein de l'UE).

Le cumul des règles d'application territoriale est source de complexité pour les responsables de traitement établis à l'étranger, hors de l'Union Européenne ou dans un autre État membre, qui réalisent des traitements de données relatives à des personnes résidant dans plusieurs États membres, et qui doivent appliquer, en plus des dispositions du RGPD (selon les critères de l'article 3 du RGPD), et autres éventuelles dispositions nationales, les dispositions de la loi française si une personne concernée par le traitement **réside** en France.

En outre, un projet de recherche avec des partenaires européens, ne semble pas pouvoir être qualifié de « traitement transfrontalier » si l'on se réfère à la définition donnée par l'article 4, point 23 du RGPD et n'est donc pas susceptible de bénéficier du mécanisme du guichet unique (« one stop shop »), ce qui aurait été un grand progrès en matière de simplification. La mise en place d'une coopération transfrontalière efficace était pourtant nécessaire concernant les projets de recherche en santé.

La recherche en santé se situe de façon croissante dans un contexte collaboratif national et international. Dans ce contexte, les conditions locales de régulation de l'accès aux données constituent un enjeu majeur pour la compétitivité française. Il est donc important qu'une attention particulière soit portée aux lois nationales qui seront applicables aux traitements mis en œuvre à des fins de recherche dans le domaine de la santé dans les autres pays européens afin d'éviter la mise en concurrence des systèmes juridiques au détriment de la recherche française.

Déclaration de liens d'intérêts

L'auteur déclare ne pas avoir de liens d'intérêts.