UNIVERSITÉ DE NANTES
UFR SCIENCES PHARMACEUTIQUES ET BIOLOGIQUES

ANNÉE 2020 **N°**

THÈSE

pour le

DIPLÔME D'ÉTAT

DE DOCTEUR EN PHARMACIE

par

Florian Trisson

Présentée et soutenue publiquement le 19 Octobre 2020

L'utilisation des données personnelles dans le cas des essais cliniques, état des lieux et problématique soulevée par la RGPD

Président : **Mme Véronique SEBILLE-RIVAIN, PU-PH, enseignant chercheur en biostatistiques, modélisation et méthodologie des essais cliniques**

Membres du jury : Mr Jean-Marie BARD, PU-PH de biochimie générale et clinique
Mme Nadège SPARFEL, Pharmacienne

Remerciements

Je remercie Mme Sébille-Rivain qui a accepté la présidence de ma thèse.

Je tiens à remercier tout autant Mr Jean-Marie Bard, pour avoir accepté d'être mon directeur de thèse et pour le temps passé à la revue de ma thèse et l'apport de ses conseils.

Nadège, que je connais et affectionne depuis plusieurs années et qui a accepté de faire partie de mon jury.

Je remercie mes parents sans qui tout cela n'aurait pas été possible. Merci pour votre soutien dans les moments compliqué et d'avoir fait en sorte que je puisse me consacrer pleinement à mes études. Je sais que ça aura été difficile de me motiver sur la fin mais c'est enfin fait.

Je remercie ma sœur qui, malgré nos quelques différents, reste une personne que j'admire beaucoup pour son courage et avec qui j'apprécie toujours de passer de bons moments.

A mon frère et sa famille que je vois assez peu, il est vrai, mais dont les moments que je passe avec sont toujours agréable.

A mes amis Hervé et Erwan qui ont rendu mes années de fac bien plus agréables et avec qui j'ai passé de supers moments aussi bien en ligne qu'IRL. Encore félicitation à toi Erwan pour ta petite fille. Pleins de bonheur à vous et en espérant vous revoir vite.

A mes potes de flag, Jessy, Antoine, Jérémy. Nos soirées resteront toujours un bon souvenir et j'espère que nous continuerons à nous voir de temps en temps malgré la distance.

Et enfin à tous les autres que je n'ai pas cité mais qui ont eu une place dans ma vie, je vous remercie pour avoir contribué à faire de moi celui que je suis aujourd'hui. En quelque sorte, vous avez un peu participé à la réalisation de cette thèse.

ABBREVIATIONS

AFSSAPS	Agence Française de Sécurité Sanitaire des Produits de Santé
AMM	Autorisation de Mise sur le Marché
ANSM	Agence Nationale de Sécurité du Médicament
APD	Autorité de Protection des Données
BCR	Binding Corporate Rules/Règles d'entreprise contraignantes
CCNE	Comité Consultatif National d'Éthique
CE	Communauté Européenne
CEPD	Commissaire Européen de la Protection des Données
CNIL	Commission Nationale Informatique et Libertés
CPP	Comité de Protection des Personnes
CSP	Code de Santé Publique
DCP	Données à Caractère Personnel
DM DIV	Dispositif Médical de Diagnostique *In Vitro*
DNPDP	Dirección Nacional de Protección de Datos Personales/Agence nationale de protection des données personnelles
DoT	Department of Transports/Département des Transports
EDPB	European Data Protection Board/ Comité Européen de Protection des Données
EEE	Espace Économique Européen
FTC	Federal Trade Commission/Commission Fédérale des Échanges
ICF	Informed Consent Form/Fiche de Consentement
ICH	International Council for Harmonization/Commission Internationale d'Harmonisation
ILITA	Israël Law, Information and Technology Authority/Autorité Israëlienne sur la Loi, l'Information et la Technologie
INDS	Institut National des Données de Santé
IVG	Interruption Volontaire de la Grossesse
MR	Méthodologie de Référence
NHS	National Health Service/Société Nationale de la Santé
OPC	Office of the Privacy Comissioner/ Bureau du Responsable de la Sécurité des Données

PIPC	Personnal Information Protection Comission/Commission de protection des données personnelles
RGPD	Réglementation Générale sur la Protection des Données
RIPH	Recherche Impliquant la Personne Humaine
SAFARI	Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus
TFUE	Traité sur le Fonctionnement de l'Union Européenne
UE	Union Européenne
URCDP	Unidad Reguladora y de Control de Datos Personales/Union de régulation et de Contrôle des Données Personnelles

Table des matières

Liste des figures....8
Liste des illustrations....9
Liste des schémas....10
Liste des annexes....11
Introduction....12
I La recherche clinique....14
I.1 Définition....14
I.2 Textes de loi encadrant la recherche clinique....15
I.3 Organisation de la recherche clinique en France....18
II Traitement des données personnelles....21
II.1 Les organismes qui s'occupent de la mise en place, de l'application, et de la surveillance du traitement des données....21
II.1.1 Les principaux organismes mondiaux hors Europe....21
II.1.2 Les organismes des pays de l'Union Européenne....24
II.1.3 L'organisme de contrôle français....26
II.2 Les textes de loi sur le traitement des données personnelles....29
II.2.1 Règlement (UE) 2016/679 (RGPD)....29
II.2.2 Règlement (EU) 2018/1725....35
III RGPD et essais cliniques....37
III.1 La gestion des données dans le cadre d'un essai clinique....37
III.1.1 MR-001....38
III.1.2 MR-002....41
III.1.3 MR-003....43
III.1.4 MR-004....44
III.2 Conflits et solutions entre la RGPD et les textes réglementaires sur les essais cliniques....46
III.2.1 Base juridique des traitements primaires....46
III.2.2 Points concernant le consentement....49

III.2.3 Utilisation secondaire des données en dehors du protocole d'essais clinique à des fins de recherche scientifique.....51
Conclusion.....54
ANNEXES.....58

Liste des figures

Frise chronologique de l'adoption des textes de loi sur la recherche clinique dans le monde, l'Europe et la France.....18
Résumé de la mise en place d'un essai clinique(38).....19

Liste des illustrations

Carte mondiale des pays en fonction de leur adéquation avec la réglementation de l'UE(16).....24

Liste des schémas

Relation entre les différents acteur européens de la protection des données.....28
Solutions proposées par le EDPB concernant les bases de licéité (39).....53

Liste des annexes

Annexe 1 : Rôle et missions du CEPD [28]……..58
Annexe 2 : Résumé de la RGPD [27]……60
Annexe 3 : Outil d'analyse des risques [31……]74

Introduction

A l'époque actuelle, une place de plus en plus importante est consacrée aux données. En effet, l'avènement du « Big Data » aujourd'hui dans la plupart des organismes est le témoignage direct de cette émergence. Ce terme, apparu pour la première fois en 1997 dans un article scientifique, a vécu une véritable démocratisation durant les dernières années.(1,2) Il désigne le « Domaine technologique dédié à l'analyse de très grands volumes de données informatiques (volumes mesurés en petaoctets), issus d'une grande variété de sources, tels les moteurs de recherche et les réseaux sociaux » et démontre bien l'importance des données, et notamment des données personnelles dans le monde d'aujourd'hui.(3)

Une telle quantité de donnée est une manne pour les entreprises de santé, notamment dans le développement de nouveaux traitements de manière plus sûre et efficace, mais aussi de faire plus de profits en rétrocédant ces données, ce que les entreprises de marketing font de plus en plus. Ces données peuvent également être utilisées dans d'autres objectifs de sécurité ou de contrôle pouvant aboutir à des extrêmes jugés non éthiques. Malgré une réglementation de plus en plus détaillée et harmonisée, des dérives peuvent donc apparaître.

En France, la mise en place d'une réglementation nationale et d'organismes de contrôle a débuté en 1974 à la suite d'un scandale relatif au programme de centralisation des données de tous les français nommé SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus). Ce programme était destiné à rassembler toute donnée sur chaque français, sans demande d'accord préalable, afin de les rendre consultables et utilisables par le ministère de la Justice et de l'Intérieur de l'époque. Sa mise en place sans débat public et sa nature contraire à la Constitution française furent à l'époque l'objet de ce scandale.(4)

D'autres scandales tournent plus spécifiquement autour du secteur de la santé. Plusieurs cas ont notamment été rapportés concernant la récupération de données de patients sans leur consentement par l'entreprise Google.

Une première affaire impliquait Google Deepmind qui, en 2016, a signé un partenariat avec la NHS (National Health Service, organisme britannique) pour développer une application permettant aux médecins de monitorer les problèmes rénaux des patients et les insuffisances rénales en particulier en récupérant les données de patients atteints de maladies rénales dans 3 hôpitaux londoniens. Contrairement à ce qui avait été convenu, ce sont des données concernant tous les malades qui ont été récupérées, alors qu'elles étaient susceptibles de contenir un caractère sensible tel un historique d'overdose ou d'IVG (Interruption volontaire de la grossesse).(5)

Une deuxième affaire concernait la collaboration entre Google et Ascension, qui ont souhaité mettre en place un moteur de recherche de patients en ligne baptisé Nightingale afin de faciliter la visualisation des dossiers médicaux par les médecins. Pour cela, Google a récupéré les données possédées par Ascension sans que ni médecins, ni patients n'aient donné leur consentement.(5)

Afin d'améliorer le traitement des données personnelles et ainsi éviter l'apparition de futurs scandales dus à un traitement des données jugé non éthique, la Réglementation Générale sur la Protection des Données (RGPD) a été approuvée par le Parlement Européen et est en cours d'application dans les différents pays d'Europe. Néanmoins, ce texte qui se veut généraliste ne s'accorde pas totalement avec les contraintes de certains secteurs qui traitent les données personnelles de patients de façon particulière, comme les essais cliniques.

Nous verrons donc dans le cadre de cette thèse ce que sont les essais cliniques, comment y est réglementé le traitement des données personnelles, les apports de la RGPD et les conflits qu'elle soulève vis-à-vis de la réglementation française des essais cliniques pour enfin passer en revue différentes solutions envisageables pour pallier les problèmes et leurs limites respectives.

I La recherche clinique

I.1 Définition

La définition du terme de recherche clinique est assez vaste. Celle-ci comprend l'ensemble des études scientifiques réalisées sur des personnes humaines afin de développer les connaissances biologiques ou médicales. (6) Elle peut regrouper différents autres termes qui possèdent un sens qui leur est propre , chacun ayant une certaine nuance par rapport aux autres. Leurs définitions ne sont pas forcement communes dans le monde mais celle utilisée en France et dans l'Europe correspond à celle du règlement 536/2014 (UE). Ce règlement fait la distinction entre les termes « étude clinique », et « essai clinique » qui sont les principales méthodes d'investigation de la recherche clinique, et dont voici les définitions :

- «étude clinique, toute investigation en rapport avec l'homme, destinée :

a) à mettre en évidence ou à vérifier les effets cliniques, pharmacologiques ou les autres effets pharmacodynamiques d'un ou de plusieurs médicaments;

b) à identifier tout effet indésirable d'un ou de plusieurs médicaments; ou à étudier l'absorption, la distribution, le métabolisme et l'excrétion d'un ou de plusieurs médicaments;

dans le but de s'assurer de la sécurité et/ou de l'efficacité de ces médicaments; »(7)

- «essai clinique», une étude clinique remplissant l'une des conditions suivantes:

a) l'affectation du participant à une stratégie thérapeutique en particulier qui est fixée à l'avance et ne relève pas de la pratique clinique normale de l'État membre concerné;

b) la décision de prescrire les médicaments expérimentaux est prise en même temps que la décision d'intégrer le participant à l'essai clinique; ou

c) outre la pratique clinique normale, des procédures de diagnostic ou de surveillance s'appliquent aux participants;(7)

La caractéristique principale de la recherche clinique est donc son application directe à la personne humaine. Cette caractéristique fait que la recherche clinique se doit d'être strictement réglementée et surveillée afin d'éviter des dérives pouvant porter atteinte à la sécurité des sujets participant aux études.

I.2 Textes de loi encadrant la recherche clinique

Au cours de l'histoire, la réglementation encadrant la recherche clinique n'a cessé de se construire et de s'améliorer. Celle-ci est encore l'objet de remaniements de nos jours afin de clarifier certains aspects qui précédemment pouvaient encore prêter à confusion.

Dans un souci d'harmonisation, le développement de cette réglementation s'est produit au niveau international et elle est appliquée de façon conjointe dans les différents secteurs du globe. A l'échelle de l'Europe, des directives et règlements sont produits afin d'être appliqués dans les différents pays dans le but d'avancer vers une simplification et une concordance des procédures entre ces pays (Figure 1).

Le constat de la nécessité d'une réglementation pour la réalisation d'études cliniques s'est fait à la suite de la Seconde Guerre Mondiale durant laquelle de nombreuses études ont été réalisées sans soucis d'éthique ou de bien-être des sujets.

Le premier texte de référence à avoir vu le jour est le Code de Nuremberg qui fut mis en place en 1947 et qui a encore force de loi de nos jours. Celui-ci énumère 10 critères utilisés pour juger les études cliniques réalisées durant la Seconde Guerre mondiale, qu'elles soient ainsi considérées comme crime de guerre ou non. Ce texte pose donc les bases éthiques de la réalisation des études cliniques, et ce à l'échelle mondiale, comme la nécessité d'un consentement éclairé, l'obligation d'un intérêt scientifique dans les recherches menées et la recherche du bien être du sujet. Il fut adapté en français plus tard en 1984 par le Comité Consultatif National d'Ethique (CCNE) et repris en 1988 par le Conseil d'État lors de la création de nouvelles lois sur la conduite des essais cliniques. (8)

Le deuxième texte de référence rédigé fut la déclaration de Helsinki en 1964 par l'AMM (Association Médicale Mondiale). Celui-ci se focalise plus sur l'aspect éthique de la recherche clinique. Il reprend les points énoncés dans le code de Nuremberg tout en apportant quelques

précisions et idées nouvelles. Il est par exemple à l'origine de la création des comités d'éthiques qui sont chargés d'évaluer le respect des règles d'éthique par l'examen des protocoles de recherche et ainsi valider le démarrage d'une étude ou bien en demander sa modification. Il aborde également la question des populations qui ne peuvent pas donner de consentement éclairé de par leur incapacité physique ou mentale. D'autres points sont évoqués comme l'optimisation des essais par l'utilisation des meilleurs traitements disponibles ou le respect de la vie privé des sujets ainsi que la mise à disposition au public des données et résultats des études portant sur les êtres humains.(9)

A la suite de la parution de ces textes à visée mondiale, ce sont davantage les règlements nationaux qui se sont développés. Ils permettaient d'accélérer l'évolution de la réglementation et ainsi pallier plus rapidement les problèmes et questionnements rencontrés, mais entraînaient par ailleurs l'apparition de disparités entre les pays. Ces écarts ont été réduits par la mise en place des recommandations ICH (International Council for Harmonisation) et d'un règlement plus global comme le règlement Européen.

En France, plusieurs lois se sont succédées afin d'organiser la gestion des essais cliniques au sein du pays.

La première d'entre elles est la Loi Huriet-Serusclat de 1988 dite loi relative à la protection des personnes qui se prêtent à la recherche biomédicale (ou loi n°88-1138). Celle-ci pose les bases réglementaires de ce qui fut appelé la recherche biomédicale. Elle rappelle les bases comme la nécessité d'intérêt thérapeutique aux recherches et introduit des notions comme celles d'investigateur et de promoteur, les obligations du promoteur, le fonctionnement des CPP (Comité de Protections des Personnes), la mise en place d'une autorité de contrôle, les règles d'indemnisation et de participation à une étude, les condamnations potentielles en cas de manquement aux lois, ou les conditions d'obtention du consentement.(10)

Le deuxième texte mis en application est la Loi de Santé publique de 2004 dite loi de Santé Publique (ou loi n°2004-806). Il s'agit de la transposition en loi française d'une directive Européenne mise en place en 2001. Ce texte concerne tout le CSP (Code de Santé Publique), et de ce fait, il a aussi un impact sur les chapitres concernant la recherche biomédicale (Titre V Chapitre II). Ces modifications rendent l'autorisation des CPP obligatoire lors de la mise en place d'une

étude et non plus un simple avis consultatif et donne une place plus importante aux autorités compétentes (AFSSAPS ou « Agence Française de Sécurité Sanitaire des Produit de Santé » à l'époque, devenue l'ANSM ou Agence Nationale de Sécurité du Médicament aujourd'hui) dans l'autorisation et le suivi des études cliniques. Celui-ci apporte également des précisions sur les précédents articles de la loi Huriet-Sérusclat.(11)

Le texte en place actuellement est la Loi Jardé de 2012 ou loi relative aux recherches impliquant la personne humaine (ou Loi n°2012-300). Il redéfinit l'organisation des différents types d'études cliniques en fonction de l'intégration ou non d'une intervention dans les études et si celle-ci comporte des risques conséquents ou minimes.(12)

En Europe, ce sont des directives et des règlements qui sont promulgués. Ces textes permettent d'harmoniser la réglementation des pays de l'Union Européenne. Les directives donnent un objectif à atteindre mais laissent à chaque état la liberté de moyen pour l'atteindre. Par contre, les règlements sont à appliquer directement par les pays, soit dans les 20 jours après leur entrée en vigueur, soit à une date fixée par le règlement en question.

La première directive à avoir été adoptée par l'Europe est la directive concernant le rapprochement des dispositions législatives, réglementaires et administratives des États membres relatives à l'application de bonnes pratiques cliniques dans la conduite d'essais cliniques de médicaments à usage humain de 2001 (2001/20/CE). Elle a pour objectif d'harmoniser la réglementation des différents pays membres en matière de sécurité et de vigilance des études cliniques. Cette directive est également le point de départ de la création d'une base de données européenne listant les évènements indésirables graves : l'EudraVigilance.(13)

Le second texte Européen concernant la recherche clinique est le règlement européen relatif aux essais cliniques de médicaments à usage humain de 2014 (UE n°536/2014) qui abroge la directive 2001/20/CE. Ce règlement a pour objectif d'harmoniser les méthodes d'évaluation des études cliniques au sein de l'Union Européenne car les disparités qui existaient entre les différents pays entraînaient une baisse de l'attractivité de ces pays envers les différents promoteurs. Ce règlement vise également une meilleure transparence des essais cliniques, notamment par la mise en place de documents résumant le cheminement du développement des médicaments

expérimentaux et la mise en place d'une plate-forme permettant de rendre public les résultats des études cliniques conduites dans chaque état membre.(7,14)

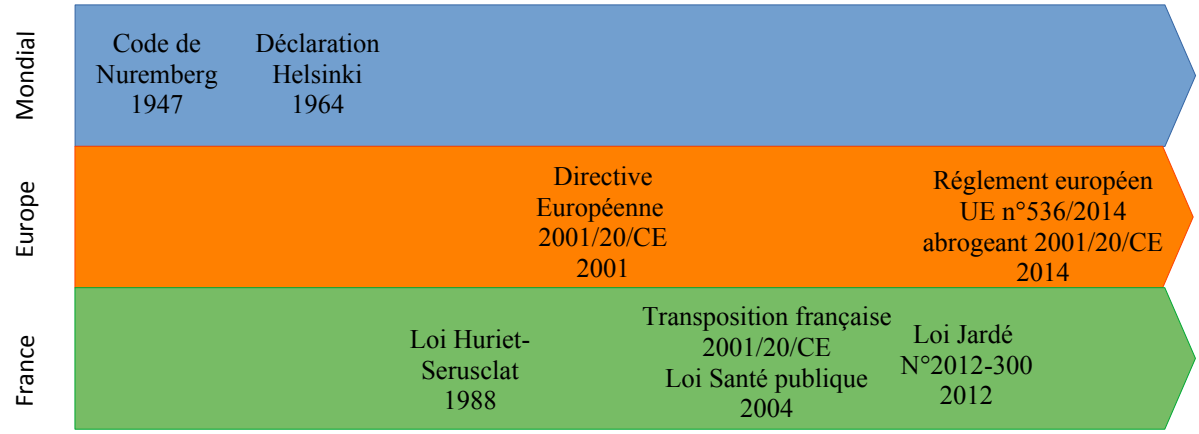

Figure 1: Frise chronologique de l'adoption des textes de loi sur la recherche clinique dans le monde, l'Europe et la France

I.3 Organisation de la recherche clinique en France

A l'heure actuelle, l'organisation de la recherche clinique en France est définie par la Loi Jardé de 2012 qui fut mise en application en 2016, et le règlement Européen de 2014. Les Recherches Impliquant la Personne Humaine (RIPH comme défini dans la Loi Jardé : « Les recherches organisées et pratiquées sur l'être humain en vue du développement des connaissances biologiques ou médicales »(12)) séparent les différentes études cliniques en 3 catégories (Figure 2) :

- Les RIPH interventionnelles (catégorie 1)
- Les RIPH interventionnelles à risque et contraintes minimes (catégorie 2)
- Les RIPH non interventionnelles (catégorie 3)

Selon la catégorie dans laquelle se trouve l'étude clinique à mettre en place, différentes méthodologies de référence (MR) sont utilisables (MR-001, MR-002, MR-003) afin de faciliter la déclaration du traitement des données personnelles.

Afin de permettre une demande d'autorisation dans un des pays de l'Union Européenne, l'essai clinique en question devra être enregistré sur le site EudraCT qui est une plate-forme européenne regroupant toutes les études et dont au moins 1 site se situe dans un pays de l'Union Européenne. Une fois faite, l'étude aura un identifiant EudraCT unique. Cet identifiant est l'élément qui garantit l'enregistrement de l'étude sur EudraCT lors des demandes d'autorisation.

Une fois l'étude enregistrée, celle-ci devra faire l'objet d'un examen par l'autorité réglementaire qui est, pour le cas de la France, l'ANSM dont l'aval sera obligatoire pour les études de catégorie 1 mais n'aura qu'un objectif de consultation pour les catégories 2 et 3.

En parallèle de l'ANSM, un avis favorable devra être obtenu de la part d'un des CPP de France, désigné au hasard.

Une demande d'autorisation adressée à la CNIL (Commission Nationale Informatique et Libertés) sera également nécessaire si les méthodologies de référence n'ont pas été utilisées pour préparer les dossiers de soumission.

Pour les recherches de catégorie 1 et 2, une assurance devra aussi être souscrite par le promoteur.

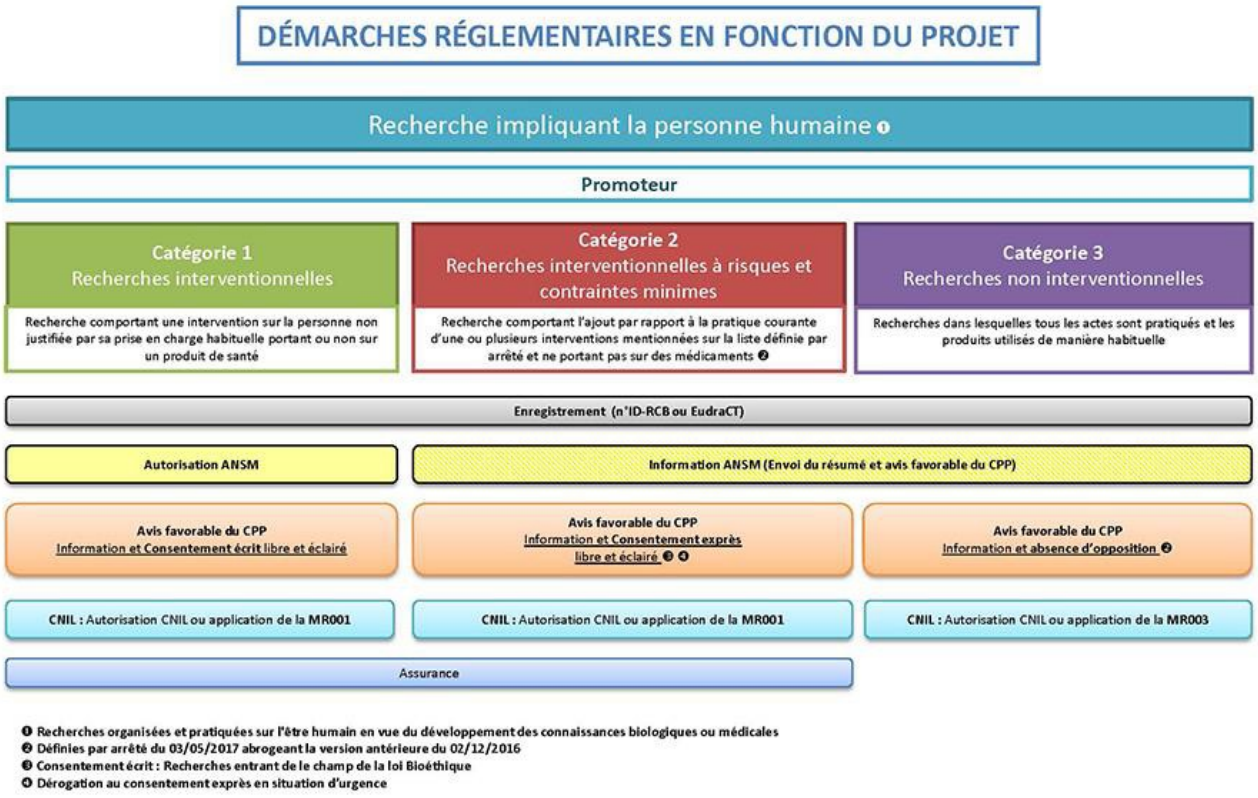

Figure 2: Résumé de la mise en place d'un essai clinique(38)

Une fois l'étude autorisée vient le temps du recrutement des centres. Ceux-ci sont évalués afin de s'assurer qu'ils ont le matériel nécessaire au bon déroulement de l'étude et que le potentiel de recrutement des sujets est suffisant.

Une fois les centres sélectionnés, le recrutement des patients peut débuter. Les différents sujets sont contactés par les médecins investigateurs. Après avoir été informés de l'intérêt de l'étude, de son fonctionnement et des risques/bénéfices attendus, les sujets devront signer un ICF (Informed Consent Form) prouvant leur compréhension de l'étude et leur accord pour une participation. Il peut arriver que dans certains cas (e.g. patient inconscient et en situation d'urgence) la demande de consentement puisse être produite à posteriori, une fois que le patient ou une personne de confiance est en état de le faire. Le principe fondamental à respecter reste la recherche du consentement éclairé du patient dès que possible.

Le patient qui a donné son consentement peut à tout moment décider de quitter l'étude sans avoir à se justifier ou subir de contrepartie. Cette sortie d'étude peut également être du fait du médecin s'il juge que la participation du patient à l'étude peut porter atteinte à sa santé.

Lors de la progression de l'étude, des données personnelles peuvent être collectées auprès du patient telles que son identité et ses données démographiques mais également ses données de santé si celles-ci sont justifiées par l'étude.

Une fois le nombre de sujets nécessaires atteint et l'étude conduite, les centres d'investigation sont clôturés afin de ne plus autoriser de modification ultérieure des données physiques des patients présents dans les documents essentiels.

Quand les centres sont tous clôturés, le promoteur procède à un gel de base pour qu'aucune donnée non physique ne puisse être modifiée. A la suite de ce gel, les données peuvent être analysées pour en obtenir des résultats et conclure sur la problématique de l'étude.

Toutes les études qui ont été enregistrées sur le site EudraCT devront également avoir leurs résultats publiés sur ce site une fois l'étude terminée. Ces résultats sont ainsi publiquement consultables sur le site https://www.clinicaltrialsregister.eu.(15)

Nous allons poursuivre en étudiant comment sont gérées les données personnelles et comment cette gestion est contrôlée en France.

II Traitement des données personnelles

Afin de pouvoir mettre en lumière les problématiques entre l'organisation des essais cliniques en France, l'utilisation des données personnelles et la récente réglementation RGPD, il faut tout d'abord décrire comment est gérée la protection des données, les rapports entre les différents pays concernant le transfert de données et les apports de la RGPD.

II.1 Les organismes qui s'occupent de la mise en place, de l'application, et de la surveillance du traitement des données

Le traitement de données personnelles étant une procédure à caractère sensible, elle doit être contrôlée. Compte tenu des enjeux qui peuvent en découler, il est impératif qu'un groupe indépendant prenne en charge ce contrôle. De tels groupes existent et sont spécifiques à des pays ou régions. Tous les États membres de l'Union Européenne (UE) ont une autorité de contrôle avec des pouvoirs bien définis mais ce n'est pas forcement le cas de tous les pays du monde. En outre, ceux qui en ont mis en place ne suivent pas forcement les mêmes exigences que celles des pays européens et ont leurs propres règles et garanties dans la sécurité du transfert de données.

Nous verrons donc les principaux organismes qui existent dans le monde et les différentes relations entre eux, à l'échelle mondiale, européenne puis française spécifiquement.

II.1.1 Les principaux organismes mondiaux hors Europe

Au niveau mondial, de nombreux pays ont adopté une réglementation et mis en place un organisme de protection pour le respect de leur législation. Néanmoins, tous les pays ne sont pas équivalents à ce niveau là. L'Union Européenne a classé ces différents pays en fonction de leurs niveau d'adéquation avec la réglementation européenne. Ces pays ont pour la plupart un

organisme de protection mais ce n'est pas une généralité, certains ne comptant que sur leur législation, voire n'ont pas de texte législatif assurant la protection des données. (Illustration 1)

Ainsi, les catégories classant les différents pays hors UE sont :

- Les pays conformes à la réglementation de l'UE :

Peu de pays rentrent dans cette catégorie. Seuls le Japon, la Suisse, l'Argentine, L'Uruguay, la Nouvelle-Zélande et Israël y appartiennent. Ces 6 pays possèdent un organisme de protection qui leur est propre et qui sont respectivement :

- la PIPC (Personnal Information Protection Comission),
- le préposé fédéral à la protection des données et à la transparence,
- la DNPDP (Dirección Nacional de Protección de Datos Personales),
- l'URCDP (Unidad Reguladora y de Control de Datos Personales),
- l'OPC (the Office of the Privacy Comissioner),
- l'ILITA (the Israël Law, Information and Technology Authority).

Ces organismes possèdent des moyens de contrôle, d'action et de sanction similaires et conformes à ceux des organismes des pays européens.(16)

- Les pays partiellement conformes à la réglementation de UE :

Le Canada et les États-Unis sont les seuls pays classés dans cette catégorie. Leurs autorités respectives sont le Commissariat à la protection de la vie privée pour le Canada, et la FTC (Federal Trade Commission) pour les Etats-Unis. L'adéquation partielle de ces états au règlement de l'UE tient dans le fait que tous les transferts de données ne respectent pas forcément les exigences de ce règlement.(16)

Au niveau du Canada, seuls les transferts concernant les organisations commerciales sont considérés suffisamment sûrs pour ne pas nécessiter de garanties supplémentaires.(17)

Concernant les États-Unis, seuls les transferts de données aux entreprises qui sont adhérentes au Privacy Shield font l'objet de l'adéquation avec l'UE. Ces entreprises sont celles qui ont décidé de se soumettre au pouvoir d'exécution et de contrôle du FTC ou du DoT (Department of Transports),

ce qui ne concerne donc pas le transfert de données aux organismes à but non lucratifs tels que les banques ou les services de télécommunication.(18)

- Les pays qui ne sont pas adéquats à la réglementation de l'UE mais qui possèdent une législation et une autorité indépendante :

Il y a de nombreux pays qui entrent dans cette catégorie. Ceux-ci possèdent des lois sur la protection des données et une autorité indépendante validée par la conférence internationale des commissaires à la protection de la vie privée et des données personnelles. Cependant ces lois ne sont pas en accord avec celles de l'UE, ce qui ne permet pas l'échange de données sans la mise en place d'un outil de transfert pour encadrer cet échange.(16)

il existe 5 méthodes actuellement pour encadrer les échanges :

- signer une clause contractuelle type tirée des modèles de la Commission Européenne entre l'expéditeur et le destinataire des données,

- adopter des « règles internes d'entreprise » ou BCR (Binding Corporate Rules) pour le transfert de données entre des entités d'un groupe dont une des entités se situe dans l'UE,

- appliquer un code de conduite adopté par une entreprise européenne et approuvé par l'autorité de protection de données concernée,

- adopter une certification pour le possesseur des données avec un engagement contraignant et exécutoire d'appliquer les garanties de protection appropriée,

- appliquer certaines condition particulières prévues dans l'article 49 de la RGPD.(19)

- Les pays qui ne sont pas en adéquation avec la réglementation de l'UE qui possèdent une législation ou non et qui ne possèdent pas d'organisme ou bien un organisme qui n'est pas indépendant :

Cette catégorie regroupe la majorité des pays. Ils sont principalement situés en Asie (centrale et orientale), Afrique et Amérique du Sud. Pour tout transfert de données vers ces pays, une des méthodes vues préalablement doit forcement être respectée afin de garantir la sécurité du processus et du traitement des données.(16)

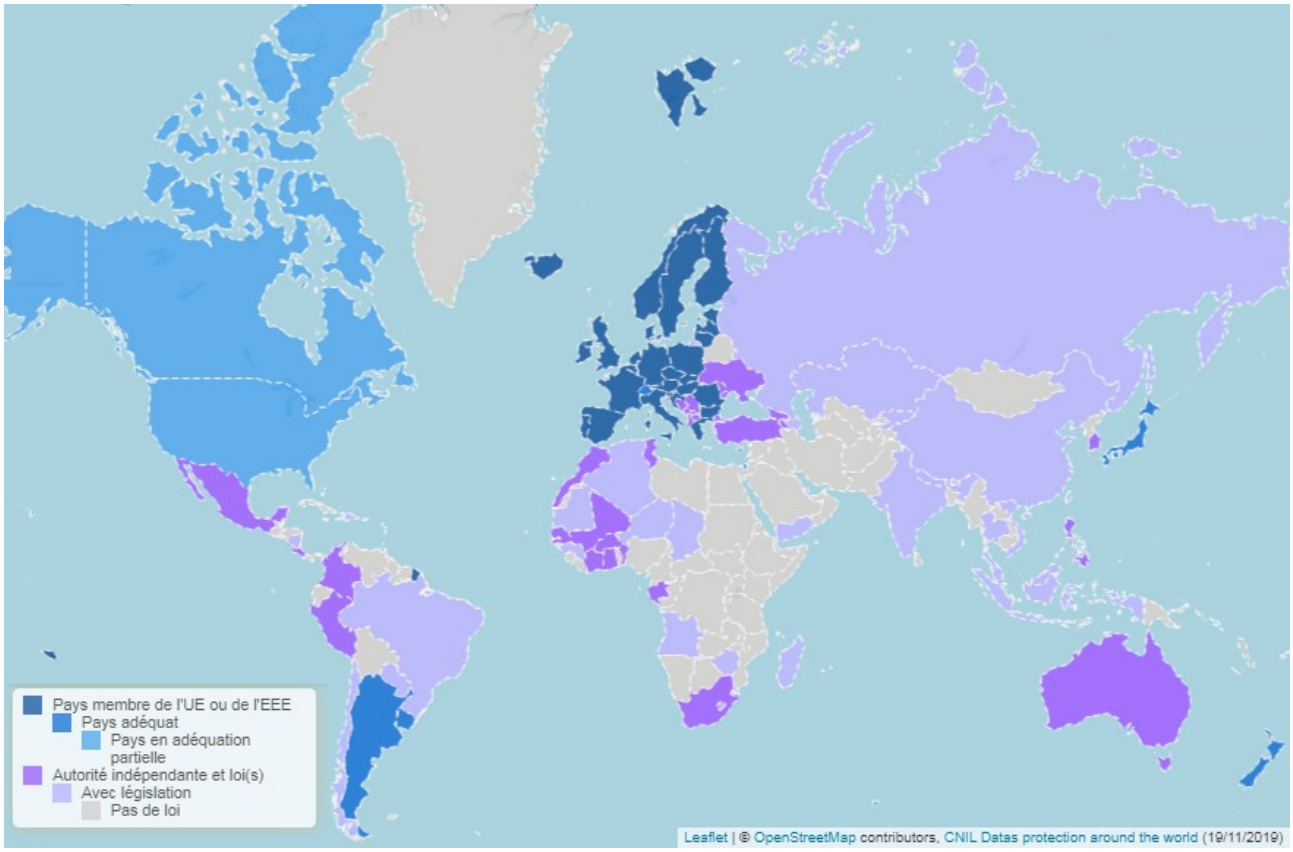

Illustration 1: Carte mondiale des pays en fonction de leur adéquation avec la réglementation de l'UE(16)

II.1.2 Les organismes des pays de l'Union Européenne

L'Union Européenne possède une organisation unique dans le monde. Celle-ci comprend 2 niveaux : une à l'échelle de l'Europe en général, et une à l'échelle de chaque pays. (Schéma 1)

Chacun de ces niveaux possède ses propres institutions et ses propres rôles en matière de protection des données personnelles.

- A l'échelle européenne

La strate européenne est dirigée par le Comité Européen de la Protection des Données (ou European Data Protection Board/EDPB). Ce comité remplace le G29 (l'ancien organisme européen de protection des données dont les missions étaient définies dans l'article 29 de la directive 95/46/CE) depuis la mise en place de la RGPD en mai 2018 mais possède les mêmes rôles et

missions. Cet organisme est indépendant, condition *sine qua none* pour respecter l'article 16 paragraphe 2 du Traité sur le Fonctionnement de l'Union Européenne (TFUE).(20)

Le rôle principal de l'EDPB est de garantir la cohérence dans l'application de la RGPD, ainsi que de la Directive Européenne en matière de Protection des Données concernant les sanctions qui peuvent être appliquées au sein de l'UE .

Son rôle est de publier des orientations générales sur l'interprétation de la RGPD afin que les organismes concernés aient une vision claire de leurs droits et devoirs. L'EDPB a également pour mission de trancher les décisions litigieuses concernant l'application de la RGPD.

Le comité se réunit lors de sessions plénières chaque mois et peut organiser des sessions exceptionnelles. Il publie un rapport annuel qui est rendu public et envoyé eu Parlement Européen, au Conseil Européen et à la Commission Européenne.(21)

L'EDPB n'a pas pour but de contrôler les institutions ou pays. Ce rôle de contrôle est laissé au deuxième organisme de la strate européenne : le Contrôleur Européen de la Protection des Donnnées (CEPD).

Le rôle du CEPD est le contrôle des institutions européennes. Il s'appuie pour cela sur le règlement (UE) 2018/1725 qui est très proche de la RGPD mais s'applique aux sociétés privées et aux administrations publiques des États membres. Il exerce sa mission de contrôle via la possibilité ou nécessité, selon la situation, d'être consulté sur les questions de protection de données lors de la mise en place d'actions par les institutions européennes, et en mettant à disposition des avis et documents sur les lignes directrices de la réglementation. Le Contrôleur peut également réaliser des audits, mener des enquêtes et traiter des réclamations provenant de particuliers. En plus de ce rôle de contrôle, le CEPD peut adopter un rôle de répression en imposant l'interdiction de traitements de données illégaux ou en infligeant des amendes aux institutions. Il peut également saisir la Cour de Justice de l'Union Européenne si nécessaire.(22)

Ainsi, l'EDPB et le CEPD travaillent conjointement pour clarifier et contrôler la réglementation en matière de traitement des données personnelles aux niveaux des institutions européennes mais comme vu auparavant, aucun de ces deux organismes n'a de rôle de contrôle au niveau de chaque État. Ce rôle est réservé aux Autorités de Protection des Données (APD).

- A l'échelle nationale

Les APD constituent la strate nationale de l'organisation européenne. Chaque État de l'UE possède une autorité de contrôle dont le président fait partie des membres de l'EDPB. Certains pays ou régions européens faisant partie de l'Espace Économique Européen (EEE) possèdent également une APD bien qu'ils ne soient pas membres de l'UE (le Liechtenstein, la Norvège et l'Islande). Ils possèdent un droit de présence au sein de l'EDPB mais n'y ont pas de droit de vote. Ils ont pour mission le contrôle, par la possibilité d'enquête et d'adoption de mesures correctrices, de l'application des lois concernant la protection des données. Elles ont également un rôle d'expertise et peuvent traiter les réclamations.(23)

Nous allons voir plus en détail les rôles des APD en prenant l'exemple de l'APD française.

II.1.3 L'organisme de contrôle français

L'APD française est la CNIL. Elle fut fondée en 1978 à la suite du scandale du projet SAFARI et de la loi Informatique et Liberté qui en découla. A cette époque, la CNIL n'avait pas les pouvoirs qu'elle a aujourd'hui et n'avait qu'un rôle consultatif. Ce n'est que depuis l'adoption de la directive 95/46/CE qu'elle possède les missions et possibilités qu'elle a actuellement.(24)

De nos jours, la CNIL possède 4 grands rôles :

1) Informer et protéger les droits des français

La CNIL est chargée d'une mission d'information aussi bien auprès des particuliers que des professionnels. Elle répond aux demandes formulées par ceux-ci mais organise également des campagnes de communication afin de garder les français informés sur leurs droits. La CNIL est également disponible pour conduire des formations ou des campagnes de sensibilisation à la RGPD.

En plus d'informer, la CNIL doit protéger les intérêts des français qui en font la demande. Les particuliers peuvent le faire en adressant des plaintes à la CNIL. Ces plaintes peuvent concerner notamment la réputation en ligne, le commerce, les ressources humaines ou la banque et le crédit.

2) Accompagner la conformité et conseiller

A la suite de la mise en application de la RGPD, la CNIL a mis en place des outils pour aider les organismes privés et publics à rester en conformité. Elle conseille également ces organismes et les autorités. Par exemple, la CNIL doit donner son avis sur les textes de loi gouvernementaux concernant la protection des données personnelles. Elle aide également les organismes publics et privés à mener à bien leurs projets en proposant des solutions qui respectent les réglementations en vigueur.

3) Anticiper et innover

La CNIL a mis en place une veille afin de pouvoir anticiper et analyser l'impact de nouvelles technologies et de leurs nouveaux usages sur la vie privée. Elle contribue également au développement de solutions technologiques qu'elle met à disposition des entreprises pour protéger la vie privée le plus en amont possible pour qu'elles adoptent une logique de « *privacy by design »*. Cet organisme a également mis en place le comité de la prospective pour renforcer sa mission de veille et réfléchir sur les enjeux des futures technologies.

4) Contrôler et sanctionner

La CNIL a également le pouvoir de contrôler n'importe quel organisme qui traite des données à caractère personnel (DCP) et qui possède un établissement en France ou traite de données privées de personnes habitant en France même si les locaux de cet organisme ne sont pas en France Elle peut également agir en association avec l'APD d'un autre pays européen si celui-ci est concerné. Les contrôles sont décidés selon des thématiques d'actualité et en fonction des réclamations et signalements qui lui sont parvenus. La CNIL a tout pouvoir en ce qui concerne la consultation des données auprès des responsables des traitements ou bien de leurs sous-traitants sauf pour quelques cas particuliers qui sont sous couvert du secret professionnel. C'est notamment le cas pour les données qui relèvent de la communication entre un avocat et son client, celles qui sont couvertes par le secret du traitement journalistique et les données couvertes par le secret médical sauf si la consultation se fait sous l'autorité d'un médecin.(25)

En cas de manquement constaté aux lois et règlements, la CNIL a la possibilité de sanctionner les traiteur ou sous-traiteur des données. Les sanctions peuvent être pécuniaires, allant jusqu'à un

maximum de 20 millions d'euros ou dans le cas d'une entreprise, 4 % de son chiffre d'affaire annuel mondial, ou bien non pécuniaires comme un rappel à l'ordre, ou bien l'arrêt définitif d'un traitement. Elles peuvent également être rendues publiques.(26)

La CNIL est l'acteur local qui, à l'échelle du pays, peut contrôler et sanctionner les organismes non conformes aux réglementations en vigueur mais elle possède également un rôle éducatif dans la mise en place de traitements ou de projets, ainsi qu'un objectif d'amélioration en réalisant une veille sur les nouvelles technologies et outils pouvant mettre à mal la sécurité de la vie privée. Ce rôle est également partagé avec toutes les autres APD des états membres qui peuvent ainsi agir ensemble pour faire prévaloir les droits à la protection des données personnelles.

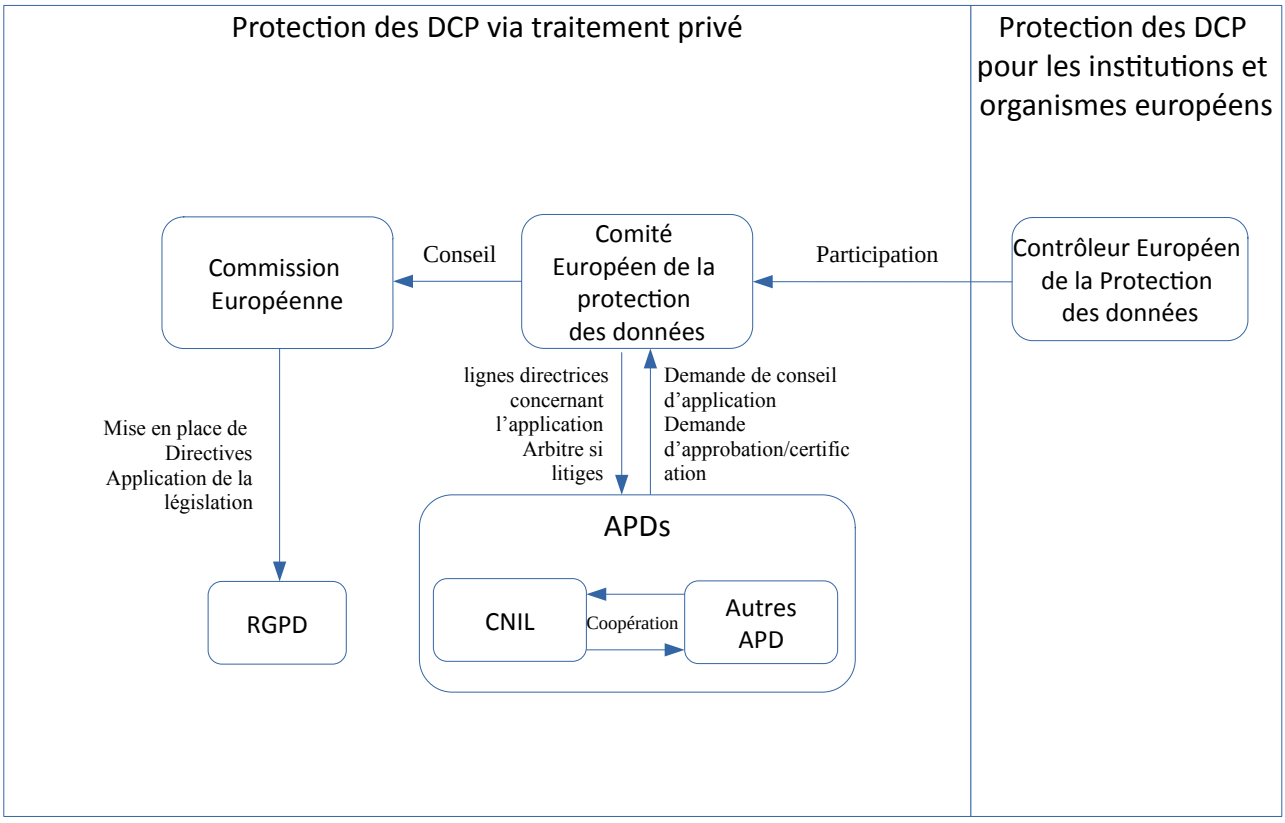

Schéma 1: Relation entre les différents acteur européens de la protection des données

Nous allons voir maintenant plus en détails les différents textes de loi et règlements qui existent et définissent le cadre législatif pour le traitement des données personnelles dans la vie de tous les jours mais aussi dans le cadre de la recherche clinique.

II.2 Les textes de loi sur le traitement des données personnelles

II.2.1 Règlement (UE) 2016/679 (RGPD)

Ce texte, adopté par le Parlement Européen le 27 Avril 2016, est le règlement européen qui est actuellement en application en Europe pour définir les mesures de protection des données personnelles. Sa mise en application s'est faite dans tous les États membres de l'UE à la date du 25 Mai 2018.

Ce texte abroge la directive européenne sur la protection des données personnelles 95/46/CE qui fut mise en place en 1995. Comme vu précédemment, ce règlement ne fera pas l'objet de la mise en place d'une loi de transposition dans chaque pays de l'UE, contrairement à la directive de 1995. Ainsi, l'adoption de ce règlement effacera les disparités des différents pays de l'UE causées par les différentes lois de transition.

Certaines définitions sont à préciser afin de pouvoir comprendre au mieux les points abordés (27) :

- « «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;

- «traitement», toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction;

- «profilage», toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique;

- «responsable du traitement», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;

- «sous-traitant», la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement;

- «consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

- «violation de données à caractère personnel», une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données;

- «règles d'entreprise contraignantes», les règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble

de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe; »

La RGPD établit toutes les règles à respecter concernant la protection des données à caractère personnel (DCP) ainsi que leur circulation et s'applique à tout traitement de ces données sauf s'il n'est pas affecté par les droits de l'UE, s'il correspond à un cas particulier tel que celui porté sur les activités personnelles, la prévention d'infractions pénales ou les enquêtes ou poursuites pour des sanctions pénales ou bien la protection de la sécurité publique. Dans ces cas-là, la RGPD ne peut s'appliquer, laissant le pays organiser sa propre protection des données. Il en va de même avec les institutions européennes qui sont réglementées par un autre règlement similaire à la RGPD.

Le traitement des DCP doit suivre 5 caractéristiques :

- la transparence (aucun traitement ne doit être caché à la personne concernée qui a fourni ses DCP)

- la loyauté (le traitement doit être le même que celui annoncé à la personne concernée qui a fourni ses DCP)

- le traitement doit être explicite

- la traitement doit être légitime

- la finalité du traitement doit être déterminée (sauf pour les recherches scientifiques pour lesquelles il est possible de réaliser un traitement ultérieur). Si une nouvelle finalité doit remplacer la première, celle-ci doit garantir une compatibilité avec la finalité initiale.

En plus de posséder ces 5 caractéristiques, le traitement de DCP ne peut être réalisé que si celui-ci respecte au moins une des conditions suivantes :

- le consentement de la personne qui donne ses DCP a été obtenu. Il doit être démontrable, donné librement et doit pouvoir être retiré à tout moment

- le traitement est nécessaire à l'exécution d'un contrat

- le traitement est nécessaire au respect d'une obligation légale à laquelle est soumis le responsable du traitement

- le traitement est nécessaire à la sauvegarde des intérêts vitaux d'une personne

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public

- le traitement est nécessaire pour les intérêts légitimes du responsable du traitement si ce traitement ne prévaut pas sur les intérêts et libertés de la personne concernée.

Le traitement de certaines DCP reste néanmoins interdit (e.g. origine, religion) sauf dans certains cas particuliers ou l'on peut considérer que le droit de traitement surpasse celui de la personne qui fournit ses DCP (e.g. intérêt public dans la santé publique, sécurité nationale). Il est également nécessaire de justifier la récupération de certaines DCP, notamment celles pouvant identifier la personne, sans quoi il est interdit de les récupérer.

Comme dit précédemment, les informations concernant le traitement des DCP doit être transparent et doit être fourni à la personne si elle en fait la demande. Il y a également nécessité d'information lorsqu'une personne donne ses DCP, notamment de ses droits, et cette personne peut exiger des rectifications concernant les DCP qu'elle a fournies. La personne concernée peut également demander l'effacement de ses DCP comme lors du retrait de son consentement, mais ce droit ne peut pas fonctionner dans certains cas (e.g. missions d'intérêt public ou traitement réalisé à des fins de recherche scientifique). La personne a également le droit à la portabilité de ses données, permettant de transférer une copie des DCP fournis à un responsable de traitement vers un second.

La personne qui fournit ses DCP possède un droit d'opposition qu'elle peut faire valoir si le traitement est basé sur une mission d'intérêt public, si celui-ci est nécessaire aux intérêts légitimes du responsable du traitement ou si le traitement se fait à des fins de prospection.

Tous ces droits et obligations ne sont pas garantis si le traitement est nécessaire pour assurer la sécurité, pour exécuter des sanctions pénales ou si un intérêt économique important pour l'UE est en jeu.

En plus des droits que possèdent les personnes donnant leurs DCP, la RGPD définit des devoirs et mesures que doivent respecter les responsables de traitement.

Ceux-ci peuvent faire appel à des sous-traitants ou d'autres responsables de traitement mais leurs rôles doivent être définis et ceux-ci doivent être liés par contrat. Le code de conduite du sous-traitant doit être compatible avec celui du responsable du traitement. Si un responsable de traitement ou sous-traitant est basé hors de l'UE, celui-ci doit obligatoirement désigner un représentant dans l'UE.

Tout responsable de traitement est également tenu de maintenir un registre des activités de traitement réalisées.

Le responsable du traitement doit également mettre en place un système de protection contre les violations qui correspondra au niveau de risque concernant la liberté des personnes. En cas de violation, celle-ci doit obligatoirement être signalée par le responsable du traitement et les personnes concernées averties.

Il peut être obligatoire pour un responsable de traitement de désigner dans son entreprise un délégué à la protection des données qui sera le lien avec les autorités de contrôle et contrôlera le respect de la RGPD.

Le responsable de traitement peut suivre un code de conduite établi par un organisme ou une association représentant une catégorie de responsable de traitement. Ce code peut également servir a contractualiser le transfert de données hors UE et doit être validé par le Comité Européen si le traitement visé concerne plusieurs pays de l'UE. Le respect des codes peut être contrôlé par l'APD du pays ou par un organisme qui aura eu son approbation. Le manquement à ces codes par le responsable peut entraîner des sanctions comme la suspension du traitement. Le responsable peut demander une certification auprès d'organismes désignés par l'APD afin de démontrer le respect du règlement.

Le transfert de DCP vers un pays tiers ou une organisation internationale est conditionné par un niveau de protection adéquat. Celui-ci doit être validé par la Commission Européenne et doit être réévalué tous les 4 ans. Il reste possible de réaliser un transfert de DCP vers un pays tiers si certaines garanties préalablement approuvées par l'ADP sont mises en place.

La RGDP précise que chaque pays de l'UE doit avoir son autorité de contrôle indépendant dont l'activité des membres doit être compatible avec sa mission de contrôle. Ceux-ci sont nommés par les parlements, gouvernements, chef d'États ou organisations indépendantes de chaque pays.

Les missions de ces ADP et les actions qu'elles peuvent entreprendre sont résumées dans l'Annexe 2.

Chaque ADP fait un rapport annuel qui est ensuite rendu public.

Il y a une nécessité d'entraide entre les APD des différents pays par possibilité d'actions conjointes et de transfert d'information.

Les APD agissent avec la Commission pour définir la cohérence d'application de la RGPD. Néanmoins, pour toute question d'application ou pour toute action qui doit être entreprise par les ADP, c'est l'EDPB qui doit être consulté. Cette consultation n'est pas obligatoire dans le cas ou l'adoption d'une mesure urgente est nécessaire.

L'EDPB est l'organisme central européen. Il ne reçoit pas d'instruction de la part d'autre organismes sauf de la Commission Européenne dans les cas d'interprétation de la RGPD.

Cet organisme possède également de nombreux rôles : de contrôle, de conseil, de publication de lignes directrices, d'agrément des organismes des certification, de définition des niveaux d'exigence en matière de certification, d'avis concernant les décisions des APD et les codes de conduite, de promotion de la coopération entre les APD et la tenue d'un registre des décisions prises par les APD et les juridictions en ce qui concerne la cohérence d'application de la RGPD.

L'EDPB rend également publique un compte-rendu annuel de ses activités sauf pour certains débats que l'EDPB peut juger confidentiels.

Les APD restent les organismes qui peuvent mettre en place des actions localement. Leurs décisions peuvent venir d'une réclamation issue d'une personne physique ou morale. Il est également possible à ces personnes de contester une décision prise par l'APD.

En cas de violation, les APD peuvent infliger, en plus de l'interdiction de traitement, une amende ne pouvant dépasser 4 % du chiffre d'affaire annuel de l'entreprise responsable de la violation, ou 20 millions d'euros (montant le plus élevé).

La liberté d'expression, le traitement des fins journalistiques ou d'expression universitaire, artistique ou littéraire doit rester compatible avec la protection des données. La RGPD précise qu'il est également possible pour les États, dans le cadre des relations de travail, d'adopter des lois ou conventions collectives pour renforcer davantage la protection des données. La RGPD prévoit également que dans le cas des traitements à des fins de recherche scientifique, il est possible de déroger à certains articles tant que les droits des personnes qui fournissent leur DCP sont garanties.

La RGPD sera réévaluée tous les 4 ans par la Commission Européenne. La Commission peut également faire des propositions législatives aux États pour uniformiser la protection des DCP au sein de l'Europe.(27)

II.2.2 Règlement (EU) 2018/1725

Le règlement EU 2018/17/25 vient en complément de la RGPD. Il s'agit du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données. Ce texte abroge le règlement (CE) n°45/2001.

Sur la base de la RGPD mise en place deux ans auparavant, ce texte résume la façon dont peuvent être recueillies les DCP, comment elle peuvent être traitées et comment elles doivent être protégées. Il résume également les droits que les personnes peuvent exercer concernant l'utilisation et le recueil de leurs DCP.

Le règlement (EU) 2018/1725 définit les activités d'une autorité de contrôle qui diffèrent de celles mises en place dans la RGPD. Contrairement à celles qui sont désignées dans la RGPD qui ont un

pouvoir d'action sur les sociétés privées, la législation des États membres ainsi que le transfert des DCP aussi bien au sein de l'Europe que vers des pays hors UE, et qui sont basées dans chaque État membre, l'autorité de contrôle définie par ce texte est le CEPD. Bien qu'existant avant la mise en place de ce règlement, son rôle fut redéfini par ce texte. Le CEPD doit exercer ses missions en toute indépendance et est soumis au secret professionnel. Il exerce de nombreuses missions auprès des institutions et des organismes de l'UE :(28))

- Il est garant de l'application du règlement (EU) 2018/1725 par les institutions

- Il sensibilise et conseille aussi bien le public que les responsables de traitement des droits et devoirs concernant le traitement des données par sa propre initiative, lorsqu'un traitement est susceptible de constituer une violation après être passé par une analyse de risque, ou par les demandes qui lui sont faites.

- Il peut enquêter sur les litiges qui lui sont rapportés par les personnes concernées par le traitement, les possibles organismes mandatés par ces personnes ou bien les organismes eux-même.

- Il peut adopter des clauses contractuelles types utilisables par les organismes ou établir des listes d'opérations de traitement nécessitant une analyse d'impact.

- Il participe aux activités de l'EDPB (clarifier les question d'application de la RGPD) et en assure le secrétariat

- Il répertorie les violations au règlement (EU)2018/1725 et les actions et mesures correctrices entreprises (avertissements, saisie, obligations de mises en conformité, limitation ou interdiction de traitement, ordonner la rectification ou l'effacement de données, l'imposition d'amende ou l'arrêt du transfert de données vers un pays hors-UE).

Bien que participant à la protection des données personnelles, ce texte ne concerne que les institutions et organismes européens et n'intervient donc pas dans la définition des mesures de protection dans le cas des études cliniques.

III RGPD et essais cliniques

Maintenant que nous connaissons en détail la manière dont est gérée la protection des données personnelles et les apports réglementaires issus de la RGPD, nous pouvons voir comment les essais cliniques et la RGPD peuvent s'articuler ensemble. Nous allons d'abord voir dans un premier temps comment la gestion des données personnelle s'effectue lors d'un essai clinique et quelles mesures existent pour garantir une sécurité de traitement des données. Nous verrons pour conclure les points qui restent en suspens entre les règles définies dans la RGPD et l'organisation des essais cliniques.

Pour chacun de ces points d'ombre, il existe des solutions possibles qui peuvent être mises en place mais aucune ne permet d'aboutir à un consensus clair sur la façon d'agir. Ces solutions et leurs limites seront développées dans la dernière partie de cette section.

III.1 La gestion des données dans le cadre d'un essai clinique

Comme vu dans la première partie, la CNIL a mis en place des méthodologies de référence. Ces méthodologies de référence ont été créées lors de la mise en application de la loi Jardé et actualisées après la mise en application de la RGPD.

Elles permettent de créer un cadre assurant une certaine protection des personnes lors d'un processus de recherche. Lorsque la recherche en question est réalisée par un responsable de traitement en accord avec la méthodologie de référence (MR) correspondante, la demande d'avis auprès de la CNIL n'est plus nécessaire. Le respect de cette méthodologie permet donc d'assurer un niveau de protection convenable tout en gagnant du temps. Pour toute recherche impliquant la personne humaine, obtenir un accord préalable du CPP avant de pouvoir entamer toute action de recherche reste une obligation. Lorsque la recherche ne concerne pas la personne humaine, le traitement devra être inscrit sur un répertoire public tenu par l'Institut National des Données de Santé (INDS).(29)

Les méthodologies de références couvrent toutes les catégories de recherche qui constituent les RIPH qui sont celles résumées dans la section I.3. Il s'agit des MR-001 et MR-003.

D’autres méthodologies existent mais couvrent soit des des études non interventionnelles sur la performance de test de diagnostique *in vitro* (MR-002), soit les recherches concernant des données déjà collectées ou les recherches sur les personnes dont les données récupérées pour cette recherche ne correspondent pas la finalité d’une RIPH comme défini dans les articles L.1121-1 et L.1121-2 du CSP (MR-004).(30)

Nous allons maintenant couvrir les différentes caractéristiques de ces méthodologies de références.

III.1.1 MR-001

La dernière modification de cette méthodologie de référence date du 21 Juillet 2016 et est résumée dans la délibération n°2016-262.

La MR-001 encadre le traitement des données des RIPH de catégorie 1 (recherche interventionnelle) et 2 (recherche interventionnelle à risque et contraintes minimes). Ces catégories de recherches concerne l’utilisation de médicament ou de procédé en dehors de leur utilisation courante et nécessite obligatoirement l’accord libre et éclairé des patients. Cette MR est appliquée également pour les recherche nécessitant l’examen de caractéristiques génétiques.

Le responsable du traitement des données doit être le promoteur de la recherche.

Les recherches donnant lieu à un traitement des données appliquant la MR-001 sont :

- Les RIPH de catégorie 1 et 2,

- Les essais cliniques portant sur des médicaments,

- Les recherches nécessitant la réalisation d’un examen de caractéristiques génétiques

Toutes les données ne peuvent pas être récupérées. Seules les données qui sont indirectement identifiantes (codées ou pseudonymisées) peuvent être récoltées, à l’exception des données recueillies dans un tableau de correspondance des données afin que les patients ne puissent pas être directement identifiés. Les données récoltées doivent être nécessaires pour remplir les objectifs de la recherche.

Seules certaines catégories de données sont récupérables et doivent, comme citées précédemment, ne pas permettre directement l'identification du patient et être scientifiquement pertinentes pour le déroulement de la recherche.

Ces catégories sont limitées à, pour les patients :

- l'identification
- les données de santé
- les informations signalétiques
- les images
- la date relative de la recherche
- l'origine ethnique
- les données génétiques
- la situation familiale
- le niveau de formation
- la catégorie socio-professionnelle
- la vie professionnelle
- le régime d'affiliation à la Sécurité Sociale
- la participation à d'autres recherches ou études
- les déplacements
- la consommations de tabac, d'alcool ou de drogue
- les habitudes de vie
- le mode de vie ou habitat
- la vie sexuelle
- le montant annuel des indemnités perçues
- l'échelle de qualité de vie.

Ces données sont limitées à, pour les professionnels de santé participant à la recherche :

- l'identité

- la formation et les diplômes

- la vie professionnelles

- le numéro d'identification du répertoire partagé des professionnels de santé

- les montant des indemnités et rémunérations perçues.

Le temps de conservation de ces données diffèrent selon la personne qui les concerne :

- pour les patients, elles doivent être conservées jusqu'à la mise sur le marché du produit, la publication des résultats ou la rédaction du rapport final de la recherche.

- Pour les professionnels de santé, elles peuvent être conservées jusqu'à 5 ans après la fin de la dernière recherche à laquelle ils ont participé.

A la suite de ces périodes, ces données doivent faire l'objet d'un archivage papier ou informatique (15 ans après la fin de l'essai en général ou 40 ans pour les essais portant sur des médicaments dérivés du sang).

L'accès aux données recueillies doit également être réglementé et seules certaines personnes en ont la possibilité. L'accès est sous la responsabilité du responsable de traitement. Tout personnel ayant accès à ces données sensibles est soumis au secret professionnel.

En ce qui concerne les données des patients, les personnes qui peuvent y avoir accès sont :

- le responsable des traitements et le personnes agissant pour son compte

- l'investigateur coordinateur

- les professionnels de santé intervenant dans la recherche clinique

- les responsables d'assurance qualité au sein des centres

- les personnes chargées des affaires réglementaires

- Les contrôleurs d'autorité sanitaire et d'autorité publique

- Les personnes chargées des analyses statistiques

- les personnes agissant sous responsabilité de l'assurance de responsabilité civile

- le personnel chargé du contrôle qualité des données

- les personnes soumises à contrat auprès du promoteur de la recherche clinique

En ce qui concerne les données de professionnels de santé participant à la recherche, ont accès :

- le responsable des traitements et le personnes agissant pour son compte

- les professionnels de santé intervenant dans la recherche clinique

- les personnes chargées des affaires réglementaires

- Les contrôleurs d'autorité sanitaire et d'autorité publique

Les patients sont tenus d'être informés de leurs droits concernant le traitement de leurs données personnelles. Ce principe s'applique aussi pour les professionnels de santés impliqués dans la recherche.

Le traitement des données à caractère personnel doit être réalisée chez le responsable de traitement ou chez un sous-traitant agissant pour le compte du responsable de traitement.

Le responsable du traitement est le garant de la confidentialité, l'intégrité et la disponibilité des DCP et les mécanismes mis en place pour garantir cette sécurité doivent être issus d'une analyse des risques spécifique au traitement. (Annexe 3)

La MR-001 précise également que seule les données anonymes ou non directement identifiables peuvent être transmise vers un pays situé hors de l'UE.(31)

III.1.2 MR-002

Cette méthodologie de référence fut mise en application le 16 Juillet 2015 et est décrite dans la délibération n°2015-256.

La MR-002 encadre le traitement de données des études non interventionnelles portant sur l'évaluation des dispositif médicaux de diagnostic *in vitro* (DM DIV). Ces études ne nécessitent pas obligatoirement le consentement du patient mais celui-ci doit toujours être informé sur le

traitement de ses information et sur ces droits en matière de protection de données et donc la possibilité de s'opposer au traitement de ses données.

Le responsable du traitement des données doit être le promoteur de la recherche.

Comme pour la méthodologie MR-001, seules certaines données sont récupérable et ne doivent pas être identifiantes tout en étant nécessaire à la réalisation de la recherche.

Ces données sont, pour les patients :

- l'identification
- les données de santé
- les informations signalétiques
- la date d'inclusion sur l'étude
- l'origine ethnique
- les variations génétiques
- la consommation de tabac, alcool ou drogue
- les habitudes de vie
- la vie sexuelle

Ces données sont, pour les investigateurs et professionnels de santé participant à la recherche :

- l'identité
- le sexe
- l'adresse électronique
- le numéro de téléphone
- la formation et les diplômes
- le montant des indemnités et rémunérations
- la participation à d'autres études

Ces données peuvent être conservée jusqu'au rapport final de l'étude ou l'enregistrement du DM DIV pour les données des patients et jusqu'à 5 ans après leur dernière recherche pour les professionnels de santé.

L'accès aux données est réglementée et doit être restreint :

- aux personnes désignées par le responsable de traitement et qui sont chargée du contrôle de la qualité des données

- aux personnes chargée des analyses statistiques

- aux personnes chargée des affaires réglementaires et de l'enregistrement du DM DIV auprès des autorités

- aux inspecteurs des autorités sanitaires et publiques

Les patients doivent être informés de la possibilité d'utilisation de leurs données à des fins de recherche et sur le traitement de leurs DCP. Les patients et les professionnels de santé ont accès à leurs données à tout moment ainsi qu'à la rectification de ces données.

Le responsable du traitement est le garant de la confidentialité, l'intégrité et la disponibilité des DCP et les mécanismes mis en place pour garantir cette sécurité doivent être issus d'une analyse des risques spécifique au traitement. (32)

III.1.3 MR-003

Cette méthodologie de référence fut mise à jour le 21 Juillet 2016 et est décrite dans la délibération n°2016-263.

La MR-003 encadre le traitement des données de santé issus des études non interventionnelles autres que celles portant sur l'évaluation de DM DIV ou RIPH de catégorie 3. Cette catégorie de recherche ne nécessite pas le consentement du patient. Celui-ci doit néanmoins être informé de la finalité du traitement de ses données et peut refuser de participer à la recherche, ce qui constitue la différence majeure avec les études interventionnelles.

Le responsable du traitement est le promoteur de la recherche.

Les recherches donnant lieu à un traitement des données appliquant la MR-003 sont :

- les essais cliniques par grappe (groupes randomisés et non individu randomisé)

- les recherches visant à évaluer les soins courants

- les recherches non interventionnelles autres que pour l'évaluation de DM DIV (e.g. étude d'observance)

Comme pour les méthodologies de référence précédentes, les données qui peuvent être récoltées sont limitées à certaines catégories et leur récolte doit être justifiée. Les DCP qui peuvent être récupérées sont les même que celles listées pour la MR-001, aussi bien pour les patients que pour les professionnels de santé participant à la recherche.

La durée de conservation des données est la même que pour la MR-001, ainsi que les conditions d'archivage. Il en va de même pour les personnes qui ont accès aux données et les informations qui doivent être données aux patients.(33)

III.1.4 MR-004

Cette méthodologie de référence fut mise en place le 3 Mai 2018 et est décrite dans la délibération n°2018-155.

La MR-004 encadre le traitement des données récupérées à des fins d'étude, d'évaluation ou de recherche n'impliquant pas la personne humaine. Cette méthodologie de référence est également celle à utiliser pour la réutilisation de données. La recherche doit avoir un intérêt public pour pouvoir être menée selon cette méthodologie de référence.

Les données récupérées ne doivent pas être identifiantes et le transfert de ces données vers un pays hors UE doit être justifié par la recherche.

Un délégué à la protection des données doit obligatoirement être désigné et le responsable des traitements doit consigner toutes les opérations de traitement dans un registre des activités ainsi que les recherches mises en œuvre.

Chaque projet utilisant cette méthodologie de référence doit être inscrit sur le répertoire tenu par l'INDS.

Il est possible d'utiliser les données du Système National des Données de Santé (SNDS) ou bien d'un de ses système fils (système mettant à disposition des données issus du SNDS) pour les recherches utilisant cette méthodologie de référence mais certaines exigences sont à respecter par le responsable du traitement du système fils et de la recherche utilisant la MR-004 :

- Les données ne peuvent être utilisées pour la promotion de produits a visée cosmétique ou sanitaire destinée à l'homme envers des professionnels de santé ou des établissements de santé.

- le respect du référentiel de sécurité applicable au SNDS

- la transmission du protocole, de la déclaration d'intérêt et des résultats à l'INDS

Les données qui peuvent être récupérées et utilisées sont les mêmes que celles des des méthodologies de référence MR-001 et MR-003.

Les données des patients ne peuvent être conservées que maximum 2 ans après la dernière publication des résultats ou bien à la signature du rapport final d'étude. Concernant celles des professionnels de santé, elles ne peuvent être conservées que 15 ans après la fin de la dernière recherche à laquelle ils ont participé.

Les personnes autorisées à accéder aux données sont les centres participant à la recherche, le responsable du traitement et les structures agissant pour lui. Seuls les professionnels intervenant dans la recherche et les responsable du contrôle et de l'assurance qualité peuvent accéder aux données directement identifiantes. Les sous-traitant peuvent également accéder à ces données mais seulement dans le cadre d'une mission de suivi des personnes, de remboursement de frais ou de livraison de produit. Néanmoins, le traitement de ces données directement identifiantes et des données de santé non directement identifiantes ne peuvent pas être réalisée par le même sous-traitant.

Une information générale et spécifique à chaque patient doit être fournie. Des données et échantillons non spécifiques à la recherche peuvent être réutilisés sans devoir informer le patient si celui-ci à déjà été informé convenablement (article 13 de la RGPD), ou lorsque la réutilisation des données était prévue et que le patient a une référence qu'il peut consulter pour s'informer sur chaque nouveau traitement.(34)

III.2 Conflits et solutions entre la RGPD et les textes réglementaires sur les essais cliniques

Malgré les efforts pour rendre la RGPD la plus complète possible, certains éléments restent conflictuels ou bien nécessitent des clarifications quant à l'interprétation du texte quand ils sont étudiés en parallèle à la réglementation des essais cliniques (EU) n°536/2014. Les principaux éléments qui entrent en conflit sont la base de la licéité du traitement des données et l'utilisation secondaire des données en dehors du protocole d'essais clinique.

III.2.1 Base juridique des traitements primaires

Tous les traitements relatifs à un protocole d'essai clinique spécifique du début de l'essai à la suppression des données à la fin de la période d'archivage doit être considéré comme un usage primaire des données. Néanmoins, tous les traitements ne suivent pas obligatoirement le même objectif. Le CTR ne distingue pas et ne précise pas de contrainte concernant les objectifs et les possibilités quant à la récupération et l'utilisation de DCP lors de la tenue d'un essai clinique. Ces possibilités sont elles contraintes dans la RGPD qui précise que le traitements des données ne peut avoir lieu que si l'étude possède une base de licéité convenable. Ces conditions sont inscrites dans le chapitre II article 6 de la RGPD.

Les enjeux, les méthodologies et les objectifs de tous les essais cliniques ne sont pas les mêmes. La RGPD fait notamment la distinction entre le traitement des données à des fins de recherche scientifique et le traitement des données à des fins de protection de la santé qui met en place des standards de qualité et de sécurité pour les produits de santé. Ces deux catégories diffèrent dans leurs objectifs et ne peuvent, par conséquent, pas utiliser les mêmes bases légales. L'EDPB a proposé une interprétation de la RGPD selon la finalité des traitements lors de son communiqué du 23 Janvier 2019 (Schéma 2).

- Le traitement à des fins de sécurité

Le traitement à des fins de protections de la santé vise à créer des standards de qualité ou évaluer de nouveaux procédés permettant d'améliorer la sécurité des produits de santé en terme de qualité et d'utilisation.

Ce traitement ne peut avoir qu'une seule justification. Le détail de cette justification est défini dans l'article 6.1.c. de la RGPD (le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis). L'obligation en question peut être issus du CTR ou de l'UE ou bien du pays dans lequel se déroule l'étude. C'est notamment le cas pour les rapport de sécurité (articles 41 a 43 de la CTR) et les obligations en matière d'archivage (article 58 du CTR). Dans le contexte de ces obligations, la référence devrait être l'article 9.2.i. (le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée).(35)

- Le traitement à des fins de recherche scientifique

D'après l'EDPB, le traitement des données doit correspondre à l'une de ces trois bases :

- **L'intérêt public** : Cette base est décrite dans l'article 6.1.e. de la RGPD (« le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement; »). Cette base doit être associée aux articles 9.2.i. ou j. : « le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel; » ou « le traitement est

nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. » respectivement.(35)

- **L'intérêt légitime** : Cette base est décrite dans l'article 6.1.f. de la RGPD (« le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »). Cette base doit être associée à l'article 9.2.j. « le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée. »(35)
Cette base peut être utilisée dans les situations ou le contrôleur n'est pas investit d'une mission d'intérêt public et que le traitement des données est nécessaire à ses intérêts ou à celle d'une tierce partie avec pour exception lorsque ses intérêts sont moins importants que les droits fondamentaux des personnes vis-à-vis de leurs données personnelles.(35)

- **Le consentement explicite** : Cette base est décrite dans l'art 6.1.a. de la RGPD (« la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques; »). Cette base doit être associée à l'article 9.2.a. « la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée; »(35)
Le consentement doit être libre, spécifique, éclairé, non ambigu et explicite dans le cas ou ce consentement est utilisé comme justification pour traiter des données à caractère personnel. Le

terme de libre est à surveiller avec attention. Cela implique que le consentement ne peut fonctionner dans les cas ou il y a clairement un déséquilibre entre le contrôleur et le patient (nécessité de soin, besoin d'argent, dépendance hiérarchique…). Ce cas peut arriver fréquemment lors de la tenue d'essais cliniques. Comme expliqué dans le guideline du G29 (ancien EDPB), le consentement ne sera pas, dans la plupart des cas, la base légale appropriée et une autre base doit être utilisée.(35)

Le consentement du CTR et celui utilisé comme base de licéité comme décrit dans l'article 6.1.a. ne servent pas le même objectif.
Le consentement donné pour le CTR sert de base éthique et décrit comment le traitement des données devrait être mis en place. Il ne devrait pas être utilisé comme accord sur le traitement des données. Il s'agit davantage d'une mesure de sécurité plutôt que d'une base de licéité.(36)

En plus de ces bases, d'autres possibilités ont le mérite d'être potentiellement intéressante mais non évoquées pour le moment comme possible base de licéité. Il s'agit notamment du contrat comme précisé dans l'article 6.1.b. de la RGPD. Cette option, bien que faisable, n'est pas évoqué comme une possibilité par l'EDPB dans son dernier avis de Mars 2019. Elle garde malgré tout des contraintes comme le devoir d'informer précisément la personne concernée sur les traitements qui porteront sur ces données, chose qui n'est pas toujours possible dans les essais cliniques.(37)

III.2.2 Points concernant le consentement

L'article 28.3. du CTR précise que le retrait du consentement à la participation à l'essai clinique ne devrait pas affecter les activités déjà entreprises et les données déjà recueillies sur la base du consentement avant son retrait. Mais comme dit précédemment, ce consentement doit être distingué de celui sur le traitement des données personnelles dans le contexte d'un essai clinique. Celui-ci peut continuer tant qu'il y a une base légale à son exécution.
Dans ce cas, les données récoltées jusqu'au retrait du consentement peuvent être conservées pour les objectifs et dans les conditions définies dans le protocole et la législation (ex : les Effets Indésirables Grave (EIG) doivent être reportés aux autorités basées sur les articles 6.1.c. et 9.2.i.de la RGPD).

Si le consentement est utilisé comme base de licéité dans le traitement des données via l'article 6.1.a. de la RGPD, les personnes peuvent retirer leur consentement à tout moment comme précisé dans l'article 7.3. de la RGPD (« La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement. »(27)). Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée est informée de cette possibilité avant de donner son consentement.. Le fait de retirer ou donner son consentement doit rester simple, et ce, sans exception, même pour une recherche à des fins scientifiques.

Si la personne concernée a demandé le retrait de son consentement, le contrôleur peut donc continuer son activité de traitement sauf si il n'y a plus de base légale à sa réalisation. Dans le cas ou il n'y aurait plus de base de traitement, ces données devront être détruite d'après l'article 17.1.b. de la RGPD (« la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement; ») et 17)3) de la RGPD (« Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire:

a) à l'exercice du droit à la liberté d'expression et d'information;

b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;

d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou

e) à la constatation, à l'exercice ou à la défense de droits en justice. »)

Ainsi, d'après le point d), il serait possible de conserver les données récupérées mais leur traitement serait illégal, ce qui rend les possibilités offertes par cette exception caduque.(36)

Une interprétation ce dette incohérence pourrait être que le traitement primaire des données reste faisable mais tout traitement ultérieur serait interdit.(37)
Une autre solution pourrait être, dans les cas ou le traitement est basé sur le consentement, de demander si le patient retire son consentement que pour l'étude clinique ou également pour le traitement de ses données.

Il existe également le cas du consentement dans le contexte d'urgence. L'article 35 du CTR précise bien les conditions permettant l'intégration d'un patient dans un essai cliniques mais les base de licéité décrite dans la RGPD permettant le traitement des données sont donc limitées.
Les seules bases légales utilisables sont l'intérêt public et l'intérêt légitime puisque le consentement ne peut être obtenu. Selon le cas, Le traitement des données issus de la première utilisation dans la situation d'urgence peut utiliser comme base de licéité l'intérêt vital de la personne d'après l'article 6.1.d. de la RGPD (« le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ») associé à l'article 9.2.c. de la RGPD.
Si la personne ou le représentant légal refuse la participation à l'essai clinique ultérieurement, cette personne doit être informée de la possibilité de refuser le traitement des données récupérées.
Dans le cas ou le patient meurt avant de pouvoir donner son accord ou refus à l'utilisation de ses données, le traitement des données n'est plus couvert par la RGPD mais est couvert par la loi nationale.(36)

III.2.3 Utilisation secondaire des données en dehors du protocole d'essais clinique à des fins de recherche scientifique

L'utilisation secondaire des données anonymes n'est pas prise en considération dans la RGPD. Par contre en ce qui concerne les données personnelles, si celles-ci doivent être utilisées dans un but différent de celui précisé dans le protocole d'étude, certains points doivent être pris en compte :
- Posséder une base l'égale issus de l'article 6. de la RGPD, que celle-ci soit la même que celui de l'utilisation primaire ou non.
- Une compatibilité des finalités doit normalement être requis pour les traitements secondaires mais les traitements à des fins de recherche scientifique suppose une compatibilité des fins

d’après l’article 5.b. de la RGPD (le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales) si le traitement secondaire assure un niveau de sécurité suffisant au traitement des données.

- Dans le cas d’une base légale sur le consentement de la personne, certains points doivent être pris en compte

  - Les données doivent être collectées dan un but spécifique, explicite et légitimes,
  - L’accord clair, libre, spécifique et éclairé du consentement de la personne d’après l’article 4.11. de la RGPD,
  - La personne à le droit de retirer on consentement à tout moment et doit être prévenu de cette possibilité avant de participer à l’essai clinique d’après l’article 7.3. de la RGPD.
  - La possibilité de consentir à l’utilisation de ses données pour certains types de traitements, mais fournir malgré tout une description claire et précise des types de traitement lorsque ceux-ci ne sont pas clairement identifié au moment du prélèvement (conseillé dans le récital 33 de la RGPD). Cette possibilité nécessite néanmoins plus de précision.
  - Il est conseillé de demander ce consentement d’utilisation secondaire au début de l’essai clinique et donc avant l’utilisation primaire. Ce consentement doit se distinguer du consentement dans le contexte du CTR comme précisé auparavant.
  - Si l’utilisation secondaire se fait après que l’essai clinique soit terminé, le contrôleur doit rechercher un nouveau consentement auprès des personnes
  - Dans tous les cas, le patient doit être informé de l’utilisation de ses données. (36)

Le Schéma 2 est un résumé des explications apportées par l’EDPB sur la base de licéité possible des différents traitements selon que ces traitements soient primaire ou secondaire et selon leur finalité. (Schéma 2)

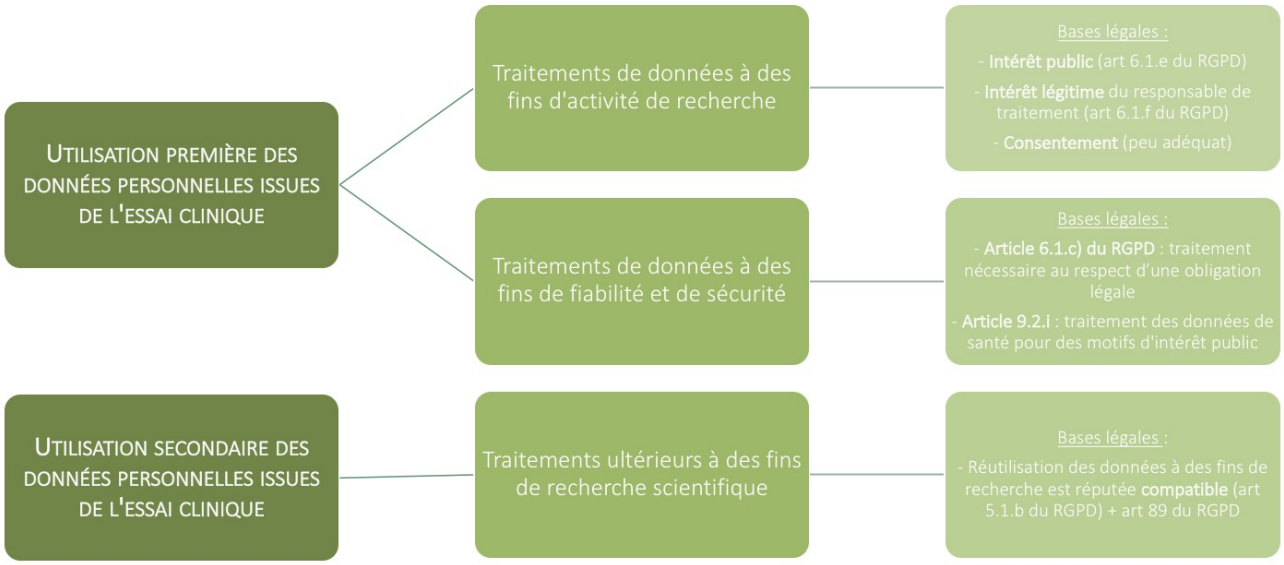

Schéma 2: Solutions proposées par le EDPB concernant les bases de licéité (39)

Conclusion

Les essais cliniques sont un secteur très contrôlé. Les nombreux problèmes éthiques qui sont arrivés par le passé ont obligé la construction d'un environnement juridique complexe afin de répondre aux différents aspects des essais cliniques tels que l'éthique ou la rigueur scientifique. Cette complexité est d'autant plus visible quand celle-ci doit être mise en relation avec d'autres réglementations qui touchent également aux essais cliniques comme le cas du traitement des données. Le développement d'une globalisation des réglementations impacte également cette complexité à l'heure actuelle où la réglementation Européenne prends une part de plus en plus importante, contraignant les lois nationales à s'adapter pour être conforme à ces réglementations.

La récente mise en place de la RGPD ne s'est pas faite sans problème. La compatibilité entre la protection des données personnelles et leur utilisation dans les essais cliniques en est un car la RGPD est avant tout une réglementation générale, ayant pour but de pouvoir être appliquée dans tous les domaines utilisant le traitement de données personnelles et les essais cliniques sont une catégorie particulière car possédant déjà sa réglementation propre et traitant de données de santé qui sont considérées comme particulièrement sensibles. Des organismes on été créés afin de pouvoir articuler la réglementation nationale avec la réglementation européenne et des méthodologies de références ont également été mises en place afin d'atteindre un niveau de conformité convenable avec la RGPD. Malgré cela, plusieurs interrogations subsistent et bien que certains éléments de réponse ont déjà été apportées par l'EDPB lors de son communiqué du 3 Janvier 2019 comme pour les bases de licéité ou la possibilité de traitement secondaire des données, certaines incompatibilités et non-sens demeurent sans réponse et devront faire l'objet d'un avis avant la mise en application de la prochaine réglementation des essais cliniques (EU) n°536/2014 qui devrait avoir lieu en 2020.

Références

1. Press G. A Very Short History Of Big Data [Internet]. Forbes. [cité 27 janv 2020]. Disponible sur: https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/

2. Google Trends [Internet]. Google Trends. [cité 18 déc 2019]. Disponible sur: https://trends.google.fr/trends/explore?date=2008-01-01%202019-12-18&q=Big%20Data

3. Larousse É. Définitions : big data - Dictionnaire de français Larousse [Internet]. [cité 18 déc 2019]. Disponible sur: https://www.larousse.fr/dictionnaires/francais/big_data/10911026

4. le_monde_0.pdf [Internet]. [cité 11 déc 2019]. Disponible sur: https://www.cnil.fr/sites/default/files/atoms/files/le_monde_0.pdf

5. Une enquête s'ouvre sur la collecte massive de données de santé par Google aux Etats-Unis [Internet]. usine-digitale.fr. [cité 27 janv 2020]. Disponible sur: https://www.usine-digitale.fr/article/une-enquete-s-ouvre-sur-la-collecte-massive-de-donnees-de-sante-par-google-aux-etats-unis.N902514

6. La recherche clinique [Internet]. Inserm - La science pour la santé. [cité 6 févr 2020]. Disponible sur: https://www.inserm.fr/recherche-inserm/recherche-clinique

7. 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 Texte présentant de l'intérêt pour l'EEE [Internet]. OJ L, 32014R0536 mai 27, 2014. Disponible sur: http://data.europa.eu/eli/reg/2014/536/oj/fra

8. Inserm_CodeNuremberg_TradAmiel.pdf [Internet]. [cité 9 févr 2020]. Disponible sur: https://www.inserm.fr/sites/default/files/2017-11/Inserm_CodeNuremberg_TradAmiel.pdf

9. WMA - The World Medical Association-Déclaration d'Helsinki de L'AMM – Principes éthiques applicables à la recherche médicale impliquant des êtres humains [Internet]. [cité 9 févr 2020]. Disponible sur: https://www.wma.net/fr/policies-post/declaration-dhelsinki-de-lamm-principes-ethiques-applicables-a-la-recherche-medicale-impliquant-des-etres-humains/

10. Loi n° 88-1138 du 20 décembre 1988 relative à la protection des personnes qui se prêtent à des recherches biomédicales | Legifrance [Internet]. [cité 14 févr 2020]. Disponible sur: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006069027&dateTexte=20101013

11. Loi n° 2004-806 du 9 août 2004 relative à la politique de santé publique | Legifrance [Internet]. [cité 14 févr 2020]. Disponible sur: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005823063&dateTexte=20200214

12. LOI n° 2012-300 du 5 mars 2012 relative aux recherches impliquant la personne humaine. 2012-300 mars 5, 2012.

13. Aspects législatifs des essais cliniques [Internet]. [cité 6 févr 2020]. Disponible sur: https://pharmacomedicale.org/pharmacologie/developpement-et-suivi-des-medicaments/26-aspects-legislatifs-des-essais-cliniques

14. L'impact du règlement (UE) n°536/2014 sur la recherche clinique en Europe [Internet]. [cité 14 févr 2020]. Disponible sur: https://syntheses.univ-rennes1.fr/search-theses/notice.html?id=rennes1-ori-wf-1-8059&printable=true

15. EudraCT Public website - Home page [Internet]. [cité 16 févr 2020]. Disponible sur: https://eudract.ema.europa.eu/index.html

16. La protection des données dans le monde | CNIL [Internet]. [cité 21 févr 2020]. Disponible sur: https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

17. Adequacy decisions [Internet]. European Commission - European Commission. [cité 22 févr 2020]. Disponible sur: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

18. Le Privacy shield | CNIL [Internet]. [cité 22 févr 2020]. Disponible sur: https://www.cnil.fr/fr/le-privacy-shield

19. Transférer des données hors de l'UE | CNIL [Internet]. [cité 21 févr 2020]. Disponible sur: https://www.cnil.fr/fr/transferer-des-donnees-hors-de-lue

20. Traité sur le Fonctionnement de l'Union Européenne.pdf [Internet]. [cité 24 févr 2020]. Disponible sur: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:12012E/TXT

21. Smith J. Concernant le CEPD [Internet]. Comité Européen de la Protection des Données - European Data Protection Board. 2018 [cité 24 févr 2020]. Disponible sur: https://edpb.europa.eu/about-edpb/about-edpb_fr

22. Smith J. Notre rôle en tant que contrôleur [Internet]. Le Contrôleur Européen de la Protection des Données - European Data Protection Supervisor. 2016 [cité 24 févr 2020]. Disponible sur: https://edps.europa.eu/data-protection/our-role-supervisor_fr

23. Que sont les autorités de protection des données (APD)? [Internet]. Commission européenne - European Commission. [cité 24 févr 2020]. Disponible sur: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_fr

24. Fonctionnement de la CNIL | CNIL [Internet]. [cité 24 févr 2020]. Disponible sur: https://www.cnil.fr/fr/fonctionnement-de-la-cnil

25. Comment se passe un contrôle de la CNIL ? | CNIL [Internet]. [cité 24 févr 2020]. Disponible sur: https://www.cnil.fr/fr/comment-se-passe-un-controle-de-la-cnil

26. Les étapes de la procédure de sanction | CNIL [Internet]. [cité 24 févr 2020]. Disponible sur: https://www.cnil.fr/fr/les-etapes-de-la-procedure-de-sanction

27. 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). :88.

28. Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (Texte présentant de l'intérêt pour l'EEE.) [Internet]. OJ L, 32018R1725 nov 21, 2018. Disponible sur: http://data.europa.eu/eli/reg/2018/1725/oj/eng

29. Recherches dans le domaine de la santé : la CNIL adopte de nouvelles mesures de simplification | CNIL [Internet]. [cité 6 avr 2020]. Disponible sur: https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-la-cnil-adopte-de-nouvelles-mesures-de-simplification

30. Recherches dans le domaine de la santé : ce qui change avec les nouvelles méthodologies de référence | CNIL [Internet]. [cité 3 avr 2020]. Disponible sur: https://www.cnil.fr/fr/recherches-dans-le-domaine-de-la-sante-ce-qui-change-avec-les-nouvelles-methodologies-de-reference

31. CNIL. Méthodologie de référence MR-001. :13.

32. Études non interventionnelles de performances concernant les dispositifs médicaux de diagnostic in vitro Méthodologie de référence MR-002 | CNIL [Internet]. [cité 26 mai 2020]. Disponible sur: https://www.cnil.fr/fr/declaration/mr-002-etudes-non-interventionnelles-de-performances-concernant-les-dispositifs-medicaux

33. CNIL. Méthodologie de référence MR-003. :12.

34. Recherches n'impliquant pas la personne humaine, études et évaluations dans le domaine de la santé Méthodologie de référence MR-004 | CNIL [Internet]. [cité 27 mai 2020]. Disponible sur: https://www.cnil.fr/fr/declaration/mr-004-recherches-nimpliquant-pas-la-personne-humaine-etudes-et-evaluations-dans-le

35. qa_clinicaltrials_gdpr_en.pdf [Internet]. [cité 28 mai 2020]. Disponible sur: https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

36. edpb_opinionctrq_a_final_fr.pdf [Internet]. [cité 28 mai 2020]. Disponible sur: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_fr.pdf

37. GDPR et essais cliniques sont-ils (in)compatibles ? [Internet]. Droit & Technologies. 2019 [cité 25 nov 2019]. Disponible sur: https://www.droit-technologie.org/actualites/gdpr-et-essais-cliniques-sont-ils-incompatibles/

38. Ragot S. Cours de méthodologie des essais cliniques. Cours présenté à; 2018; Université de Poitiers.

39. Administrateur. Données de santé à caractère personnel : un traitement précisé par le Conseil de l'Europe et le Comité européen de la protection des données (CEPD) [Internet]. Staub & Associés. 2019 [cité 29 mai 2020]. Disponible sur: http://www.staub-associes.com/donnees-de-sante-a-caractere-personnel-traitement-precise-conseil-de-leurope-comite-europeen-de-protection-donnees-cepd/

ANNEXES

Annexe 1 : Rôle et missions du CEPD [28]

Missions du CEPD tels que précisés dans le règlement (UE)2018/1725

Article 57

Missions

1. Sans préjudice des autres missions prévues par le présent règlement, le Contrôleur européen de la protection des données:

a) contrôle et assure l'application du présent règlement par une institution ou un organe de l'Union, à l'exclusion du traitement de données à caractère personnel par la Cour dans l'exercice de ses fonctions juridictionnelles;

b) favorise la sensibilisation du public et sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement. Les activités destinées spécifiquement aux enfants font l'objet d'une attention particulière;

c) encourage la sensibilisation des responsables du traitement et des sous-traitants en ce qui concerne les obligations qui leur incombent en vertu du présent règlement;

d) fournit, sur demande, à toute personne concernée des informations sur l'exercice des droits que lui confère le présent règlement et, si nécessaire, coopère, à cette fin, avec les autorités de contrôle nationales;

e) traite les réclamations introduites par une personne concernée ou par un organisme, une organisation ou une association, conformément à l'article 67, examine l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire;

f) effectue des enquêtes sur l'application du présent règlement, y compris sur la base d'informations reçues d'une autre autorité de contrôle ou d'une autre autorité publique;

g) conseille, de sa propre initiative ou sur demande, l'ensemble des institutions et organes de l'Union sur les mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel;

h) suit les évolutions pertinentes, dans la mesure où elles ont une incidence sur la protection des données à caractère personnel, notamment dans le domaine des technologies de l'information et des communications;

i) adopte les clauses contractuelles types visées à l'article 29, paragraphe 8, et à l'article 48, paragraphe 2, point c);

j) établit et tient à jour une liste en lien avec l'obligation d'effectuer une analyse d'impact relative à la protection des données en application de l'article 39, paragraphe 4;

k) participe aux activités du comité européen de la protection des données;

l) assure le secrétariat du comité européen de la protection des données, conformément à l'article 75 du règlement (UE) 2016/679;

m) fournit des conseils concernant le traitement visé à l'article 40, paragraphe 2;

n) autorise les clauses contractuelles et les dispositions visées à l'article 48, paragraphe 3;

o) tient des registres internes des violations du présent règlement et des mesures prises conformément à l'article 58, paragraphe 2;

p) s'acquitte de toute autre mission relative à la protection des données à caractère personnel; et

q) établit son règlement intérieur.

2. Le Contrôleur européen de la protection des données facilite l'introduction des réclamations visées au paragraphe 1, point e), par la mise à disposition d'un formulaire de réclamation qui peut aussi être rempli par voie électronique, sans que d'autres moyens de communication ne soient exclus.

3. L'accomplissement des missions du Contrôleur européen de la protection des données est gratuit pour la personne concernée.

4. Lorsque les demandes sont manifestement infondées ou excessives, en raison, notamment, de leur caractère répétitif, le Contrôleur européen de la protection des données peut refuser d'y donner suite. Il incombe au Contrôleur européen de la protection des données de démontrer le caractère manifestement infondé ou excessif de la demande.

Annexe 2 : Résumé de la RGPD [27]

Ce tableau résume le articles écrits dans la RGPD classés par chapitre

Chapitre I – dispositions générales (Art 1 à 4)	
	•Établissement des règles concernant la protection des données à caractères personnelles (DCP) et leur circulation qui est un droit fondamental de l'UE. •S'applique à tout traitement de DCP sauf pour ceux qui ne relèvent pas du droit de l'union, des Activités chapitre 2 titre V du traité de l'UE (politique étrangère et sécurité commune), des activités personnelle ou domestique, des activités de prévention/détection d'infractions pénales, d'enquêtes et de poursuite pour des sanctions pénales ou protection sécurité publique (que par les autorités compétentes). Ne concerne pas le traitement par les institutions (réglementé par le CE 45/2001)
Chapitre II – Principes (Art 5 à 11)	
	•Le traitement doit être transparent, loyal, licite, avoir une finalité déterminée, explicite et légitime (**sauf à fin de recherche scientifique, historique ou statistique** qui ne permet un traitement ultérieur si les garanties de protection sont assurées), adéquat, pertinent et limité à l'objectif. Les DCP doivent être exactes et conservées sur une durée adéquate (**sauf à fin de recherche scientifique, historique ou statistique**). Sécurisation du traitement contre le traitement illicite, la perte de données, la destruction de données ou les dégâts occasionnés. Le responsable du traitement est responsable du respect de ces principes. •Le traitement n'est licite que si une condition est remplie au moins : - **consentement** de la personne pour une ou plusieurs finalités - Si nécessaire a l'**exécution d'un contrat** - Si nécessaire au **respect obligation légale** à laquelle est soumis le responsable du traitement (Peut différer selon l'État membre). - Si nécessaire à **la sauvegarde des intérêts vitaux** d'une personne - Si nécessaire à l'exécution d'une mission d'intérêt publique dont est investi le responsable du traitement (Peut différer selon l'État membre). - Si le traitement est nécessaire pour les intérêts légitimes du responsable, du traitement si ce traitement ne prévaut pas sur les intérêts et libertés de la personne concernée. •Il reste possible de réaliser un traitement à fin différente sans

	consentement, Il faudra alors que le responsable du traitement tienne compte du lien entre finalité initiale et finalités ultérieures, du contexte de collection, de la nature des DCP (voir art 9 et 10), des conséquences possibles du traitement, et de l'existence de garanties appropriées pour déterminer si cette autre fin à une compatibilité avec la fin initiale. •Conditions de traitement sur la base du consentement : - Le consentement donné par la personne doit être démontrable par le responsable du traitement ou sous-traitant, - retrait du consentement faisable a tout moment. Possibilité de traiter les DCP avant le retrait du consentement - Le consentement doit être donné librement et n'empêche pas l'obtention d'un contrat pour lequel le traitement n'est pas nécessaire - Pour les enfant < 16 ans : le consentement doit être donné par le titulaire (selon l'État membre, cela peut aller jusqu'à < 13ans) •Le traitement de certains types de données est interdit (origine raciale, opinion politique, religion, syndic, données génétiques, biométriques, données santé, orientation sexuelle), sauf si une de ces conditions est remplie : - Il y a consentement de la personne (sauf si le droit de l'UE ou de l'État membre refuse la levée d'interdiction), - Si nécessaire à l'exécution des obligations et l'exercice des droits du responsable du traitement en ce qui concerne le droit du travail, la sécurité ou la protection sociale, - Si le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne si elle ne peut pas donner son consentement, - Si le traitement concerne des organismes à but non lucratif et que le traitement se rapporte aux membres ou anciens membres ou personnes tenant contact régulier et que les DCP ne soient pas communiquées hors de l'organisme sans consentement, - Si les DCP ont été rendues publiques par la personne, - Si traitement nécessaire à l'exercice ou défense d'un droit en justice, - Si traitement nécessaire pour des motifs d'intérêt public importants, - Si nécessaire à des fins de médecine préventive ou du travail/ appréciation capacité de travail du travailleur/diagnostic médical/prise en charge/gestion de systèmes et services de soin/protection sociale (le responsable du traitement doit être un professionnel de santé soumis au secret), - Si le traitement est nécessaire pour l'intérêt public dans la santé publique,

	- Si le traitement est réalisé à des fins archivistes dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et que des précautions particulières ont été mises en place pour assurer le principe de minimisation des données. Il y a une possibilité d'introduction de limitation supplémentaire par les États membres en ce qui concerne les données génétiques, biométriques ou de santé. •Pas de nécessité de récupérer les DCP permettant d'identifier une personne si l'identification n'est pas nécessaire au traitement, le responsable doit pouvoir le démontrer à la personne concernée
Chapitre III – droits de la personne concernée (Art 12 à 23)	
Transparence	•Le traitement doit être fourni de façon claire et concise, en toute transparence, par écrit ou bien oralement si la personne en fait la demande (l'identité de la personne doit pouvoir être démontrée par d'autres moyens)
Information et accès au DCP	•Certaines informations sont à donner quand une personne donne ses DCP, idem lorsque ce n'est pas la personne qui fournit directement ses DCP. Il y a possibilité d'obtention d'information quant au traitement de ses DCP ainsi que de rectification de ses données.
Rectification et effacement	•Il y a également un droit à l'effacement si une de ces conditions est remplie : - Si les DCP ne sont plus nécessaires en vue de la finalité du traitement, - Si il y a eu retrait du consentement, - Si les DCP sont traitées avec une finalité de prospection, - Si le traitement est illicite, pour respecter une obligation légale du droit de l'union ou d'un État membre. Cas ou le droit à l'effacement ne s'applique pas : - Liberté d'expression et d'information, mission d'intérêt public, - Santé publique, - Traitement réalisé à des fins archivistes dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques et que des précautions particulières ont été mises en place pour assurer le principe de minimisation des données, - Droit en justice. - Droit à l'oubli si les DCP ont été rendues publiques. •Possibilité de limitation du traitement si l'exactitude des DCP est contestée, si le traitement est illicite, si la conservation des DCP n'est plus

	nécessaire mais pour le traitement mais nécessaire pour la personne pour son droit en justice, ou bien si la personne concernée fournit une raison particulière compte tenu de sa situation. Information de la personne par le responsable du traitement lorsque que la limitation est levée. Une notification de rectification, d'effacement ou de limitation est obligatoire par le responsable du traitement si elle est possible techniquement. •Droit à la portabilité des données. C'est à dire que la personne concernée peut récupérer une copie de ses DCP transmises au responsable du traitement et les fournir à un autre responsable si le traitement est fondé sur certaines justifications.
Droit d'opposition et prise de décisions individuelle automatisée	•Droit d'opposition au traitement des DCP ou profilage si celui-ci est justifié par l'exécution d'une mission d'intérêt publique dont est investi le responsable du traitement, ou si le traitement est nécessaire pour les intérêts légitimes du responsable du traitement si ce traitement ne prévaut pas sur les intérêts et libertés de la personne concernée. Il y a également possibilité d'opposition si le traitement est à des fins de prospection. Ces droits doivent être portés à l'attention de la personne concernée, l'opposition est possible pour les cas de sanction auprès du responsable du traitement. •Il y a possibilité de pouvoir ne pas faire l'objet d'un traitement individuel automatisé, même pour un profilage sauf si : - Nécessaire à la conclusion ou l'exécution d'un contrat - Autorisé par le droit de l'union ou de l'État membre tout en sauvegardant les droits et libertés des intérêts légitimes des personnes - La personne a donné son consentement explicite Le traitement automatisé ne peut concerner les DCP interdites au traitement sauf si le traitement est nécessaire pour des motifs d'intérêt public importants ou si la personne a donné son consentement.
Limitations	•Possibilité d'outrepasser les droits et obligations de transparence, de refus de traitement automatisé, de communication en cas de violation des DCP, ainsi que le respect des principes de base si le traitement est nécessaire pour garantir : - la sécurité nationale, - la défense nationale, - la sécurité publique, - l'exécution de sanctions pénales ou prévention d'infractions pénales, - un intérêt économique ou financier important de l'UE, - la protection de l'indépendance de la justice,

	- la prévention et la détection des manquements à la déontologie de professions réglementées, - des missions de contrôle, - la protection de la personne concernée, - l'exécution de demandes de droit civil.
Chapitre IV – Responsable du traitement et sous-traitant (Art 24 à 43)	
Obligations générales	•Les responsables du traitement sont tenus de respecter le règlement via la mise en place de mesures qui peuvent être réexaminées si besoin. Si ces mesures ont obtenu une certification en matière de protection des données, elles sont considérées comme acceptables. •Il y a la possibilité d'avoir plusieurs responsables de traitement qui doivent dans ce cas définir leur rôle respectif. Si le responsable du traitement se situe hors de l'UE, il y a possibilité de désigner un sous-traitant dans l'UE. Obligation de designer un représentant dans l'UE lorsque les responsables ou sous-traitant ne sont pas établis dans l'UE. •Les sous-traitants sont liés au responsable du traitement par contrat/acte juridique pour un traitement spécifique. Le sous-traitant doit prouver un code de conduite respectant les mesures définies par le responsable du traitement. •Un registre des activités de traitement est à tenir par le responsable du traitement ou son représentant.
Sécurité des données à caractère personnel	•Obligation de mettre en place un système de protection selon les risques pour les libertés des personnes. Le signalement des violations doit être réalisé par le responsable du traitement sauf si celui-ci n'entraîne pas d'incidence. Un rapport doit être rédigé par le sous-traitant si il en est responsable. Toute violation doit être documentée. •Obligation d'information des personnes concernées par la violation sauf cas particuliers
Analyse d'impact relative à la protection des données et consultation préalable	•Si un risque non négligeable existe le responsable du traitement doit réaliser une analyse d'impact relative à la protection des données. Elle est également obligatoire dans certains cas. •Les autorités de contrôle peuvent publier la liste des traitements nécessitant analyse d'impact ou non. •Obligation de consultation de l'autorité de contrôle si il existe un risque élevé pour la protection des données à la suite de l'analyse d'impact.

	•Obligation de consultation de l'autorité de contrôle par les États membres si une proposition de loi doit être adopté par le parlement.
Délégué à la protection des données	•Dans certains cas, il y a obligation de désigner un délégué à la protection des données par le responsable du traitement ou le sous-traitant. Cela reste possible dans les autres cas mais ce n'est pas une obligation. Il est désigné sur les bases de ses qualités professionnelles et ses connaissances, et ses coordonnées sont à délivrer à l'autorité de contrôle. Il intervient pour toute question relative à la protection des DCP et ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou sous traitant. Il est soumis au secret professionnel en ce qui concerne l'exercice de ses missions. •Ses missions sont : - L'information du responsable du traitement ou sous-traitant sur les obligations, - Contrôler le respect du règlement, - Conseiller sur l'analyse d'impact, - Coopérer avec l'autorité de contrôle, - Être de point de contact avec cette autorité.
Codes de conduite et certifications	•Possibilité d'élaboration de codes de conduite par les organismes ou associations représentant des catégories de responsable de traitement ou sous-traitant par la mise en place d'actions citées dans le règlement. Ces codes peuvent servir de référence pour contractualiser le transfert de données vers une zone hors UE si l'autorité de contrôle rend un avis favorable sur le projet de code. Le code est soumis au comité européen dans le cas de traitement entre plusieurs États de l'UE et est soumis à la Commission si avis favorable pour décider si le code peut être d'application générale dans l'UE. Le comité consigne et met à disposition du public les codes et leurs modifications. •Les codes approuvés peuvent être contrôlés par un organisme différent de l'autorité de contrôle mais qui aura obtenu son approbation. Les critères de jugement sont soumis par l'autorité au comité. Cet organisme peut suspendre ou exclure le responsable du traitement ou sous-traitant en cas de manquement au règlement. L'agrément de l'organisme peut être révoqué par l'autorité de contrôle si besoin. •Possibilité d'obtenir une certification concernant les opérations de traitement des données pour démontrer le respect du règlement. Ceci est également faisable pour les organismes non soumis au règlement. Ces certifications peuvent être données par un organisme de certification ou l'autorité de contrôle et sont valables 3 ans. •Les organismes sont désignés par les autorités de contrôle. Ces

	organismes notifient l'autorité compétente des délivrances ou retraits de certifications.
Chapitre V – Transfert de données à caractère personnel vers des pays tiers ou des organisations internationales. (Art 44 à 50)	
	•Le transfert de DCP peut avoir lieu vers un pays ou une organisation internationale si la Commission a constaté qu'il ou elle assure un niveau de protection adéquat. Réévaluation tous les 4 ans, mais suivi permanent de ces pays ou organisations pouvant entraîner l'abrogation de cette autorisation. Publication de l'état de ces pays/organisations sur le journal officiel de l'UE ou le site de la Commission. •Possibilité de transfert sans décision de la Commission si il y a des garanties appropriées, certaines devant être approuvées par une autorité de contrôle. •Possibilité de mise en place de règles d'entreprise contraignantes qui devront être validées par l'autorité de contrôle. •Le transfert ou la divulgation de DCP ne peut être issu d'une décision d'une autorité administrative d'un pays tiers.
Chapitre VI - Autorités de contrôle indépendantes (art 51 à 59)	
Statut d'indépendance	•Il doit y avoir au moins une autorité publique indépendante par État de l'UE. Celle-ci est chargée d'appliquer la RGPD. Les agents sont sélectionnés par l'autorité elle-même et ne peuvent exercer d'activité incompatible avec leurs fonctions. Chaque autorité doit avoir un budget annuel propre et un contrôle financier qui ne menace pas son indépendance. •Les membres de l'autorité sont nommés de façon transparente par le parlement, le gouvernement, le chef d'État ou une organisation indépendante. Les membres et agents sont soumis au secret de leur profession.
Compétence, missions et pouvoirs	•Les autorités de contrôle ne sont pas compétentes pour contrôler les traitements effectués par les juridictions dans l'exercice de leurs fonctions juridictionnelles. •Les autorités ont pour mission : - Appliquer la RGPD, - Sensibiliser le public,

	- Conseiller les institutions sur les mesures législatives, - Sensibiliser les responsables de traitement ou sous-traitant sur leurs obligations, - Informer sur la RGPD, - Traiter les réclamations, - Coopérer avec les autres autorités pour une application cohérente, - Effectuer des enquêtes, - Suivre les évolutions technologiques pertinentes, - Établir et tient a jour une liste en lien avec l'obligation d'effectuer une analyse d'impact, - Fournir des conseils sur les opérations de traitement, - Rendre des avis et approuve les codes de conduite qui fournissent des garanties suffisantes, - Examiner périodiquement les certifications, - Rédiger et publier les critères d'agrément, - Agréer les organismes chargés du suivi des codes de conduite et des certifications, - Autoriser les clauses contractuelles, - Approuver les règles d'entreprise contraignantes, - Tenir un registre interne des violations, - Toute autre mission relative à la protection des DCP, •Les autorités de contrôle possèdent certains pouvoirs d'enquête : - Obtenir toute information auprès des responsables de traitement ou sous-traitant ou leur représentant, - Mener des audits, - Examiner les certifications, - Notifier les violations aux responsables de traitement et sous-traitant, - Obtenir accès à tous les DCP nécessairement, - Obtenir accès à toutes les installations et à tous les moyens de traitement du responsable du traitement ou sous-traitant, - Avertir les responsables de traitement ou sous-traitants qu'un traitement envisagé peut violer la RGPD, - Rappeler à l'ordre après violations, - Obliger les responsables de traitement ou sous-traitants à satisfaire les droits d'une personne concernée , - Ordonner la mise en conformité des traitements , - Ordonner la communication d'une violation aux personnes concernées, - Imposer une limitation ou une interdiction de traitement, - Ordonner la rectification ou l'effacement de DCP et la notification aux personnes concernées, - Retirer une certification ou refuser la délivrance d'une certification, - Imposer une amende,

	- Suspendre l'envoi de données vers un destinataire situé dans un pays tiers ou vers une organisation internationale, •Chaque année, l'autorité de contrôle remet un rapport de ses activités au parlement, au gouvernement et aux autres autorités. Ce rapport est également rendu public.
Chapitre VII – Coopération et cohérence (Art 60 à 76)	
Coopération	•Possibilité de demande de coopération entre une autorité de contrôle chef de file et d'autres autorités de contrôle dans le cadre de la réalisation d'enquêtes ou de contrôle. L'autorité chef de file à le devoir d'informer les autres autorités de contrôle et celles-ci peuvent contester les éventuelles décisions du chef de file. Si désaccord, passage par un mécanisme de cohérence. Si accord partiel, mise en place des décisions convenues et discussion sur les points de désaccord. Il y a possibilité de passer par une procédure d'urgence si nécessaire. •Nécessité d'entraide et d'information entre les différentes autorités via le transfert d'informations ou de conclusions issues de procédures réalisées préalablement. Possibilité d'actions conjointes.
Cohérence	•Action conjointe des autorités de contrôle et de la Commission pour la cohérence d'application du règlement. •Le comité doit être consulté pour avis par les autorités de contrôle lorsque celles-ci veulent mettre en place certaines actions. Toute question d'application générale ou au sein de plusieurs pays membres devra faire l'objet d'un avis du comité. Les questions qui ont déjà fait l'objet d'un avis ne sont pas retraitées. Il y a possibilité de litige et c'est le comité qui adoptera une décision si nécessaire. •Il est possible de se passer du mécanisme de contrôle de la cohérence si une autorité de contrôle estime qu'il est urgent d'adopter certaines mesures pour protéger les droits et libertés des personnes concernées par un traitement. Cette mesure ne peut durer dans le temps. Possibilité de demande d'un avis d'urgence ou de décision contraignante d'urgence par une autorité de contrôle auprès du comité.
Comité Européen de la protection des données	•Le comité possède la personnalité juridique et agit en toute indépendance. Il ne reçoit l'instruction d'aucun organisme mis à par la commission dans certains cas particuliers. Le comité veille à l'application cohérente du règlement. •Le comité possède de nombreux rôles :

	- De surveiller et garantir la bonne application du présent règlement dans les cas prévus aux articles 64 et 65, sans préjudice des missions des autorités de contrôle nationales; - De conseiller la Commission sur toute question relative à la protection des données à caractère personnel dans l'Union, y compris sur tout projet de modification du présent règlement; - De conseiller la Commission, en ce qui concerne les règles d'entreprise contraignantes, sur la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent; - De publier des lignes directrices, des recommandations et des bonnes pratiques sur les procédures de suppression des liens vers des données à caractère personnel, des copies ou des reproductions de celles-ci existant dans les services de communication accessibles au public, ainsi que le prévoit l'article 17, paragraphe 2; - D'examiner, de sa propre initiative, à la demande de l'un de ses membres ou à la demande de la Commission, toute question portant sur l'application du présent règlement, et de publier des lignes directrices, des recommandations et des bonnes pratiques afin de favoriser l'application cohérente du présent règlement; - De publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue de préciser davantage les critères et conditions applicables aux décisions fondées sur le profilage en vertu de l'article 22, paragraphe 2; - De publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue d'établir les violations de données à caractère personnel, de déterminer les meilleurs délais visés à l'article 33, paragraphes 1 et 2, et de préciser les circonstances particulières dans lesquelles un responsable du traitement ou un sous-traitant est tenu de notifier la violation de données à caractère personnel; - De publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe concernant les circonstances dans lesquelles une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques comme le prévoit l'article 34, paragraphe 1; - De publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, aux fins de préciser davantage les critères et exigences applicables aux transferts de données à caractère

	personnel fondés sur des règles d'entreprise contraignantes appliquées par les responsables du traitement et sur des règles d'entreprise contraignantes appliquées par les sous-traitants et concernant les autres exigences nécessaires pour assurer la protection des données à caractère personnel des personnes concernées visées à l'article 47; - De publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue de préciser davantage les critères et exigences applicables aux transferts de données à caractère personnel sur la base de l'article 49, paragraphe 1; - d'élaborer, à l'intention des autorités de contrôle, des lignes directrices concernant l'application des mesures visées à l'article 58, paragraphes 1, 2 et 3, ainsi que la fixation des amendes administratives en vertu de l'article 83; - De faire le bilan de l'application pratique des lignes directrices, recommandations et des bonnes pratiques visées aux points e) et f); m) de publier des lignes directrices, des recommandations et des bonnes pratiques conformément au point e) du présent paragraphe, en vue d'établir des procédures communes pour le signalement par des personnes physiques de violations du présent règlement en vertu de l'article 54, paragraphe 2; - D'encourager l'élaboration de codes de conduite et la mise en place de mécanismes de certification, de labels et de marques en matière de protection des données en vertu des articles 40 et 42; - De procéder à l'agrément des organismes de certification et à l'examen périodique de cet agrément en vertu de l'article 43 et de tenir un registre public des organismes agréés en vertu de l'article 43, paragraphe 6, ainsi que des responsables du traitement ou des sous-traitants agréés établis dans des pays tiers en vertu de l'article 42, paragraphe 7; - de définir les exigences visées à l'article 43, paragraphe 3, aux fins de l'agrément des organismes de certification prévu à l'article 42; - De rendre à la Commission un avis sur les exigences en matière de certification visées à l'article 43, paragraphe 8; - De rendre à la Commission un avis sur les icônes visées à l'article 12, paragraphe 7; - De rendre à la Commission un avis en ce qui concerne l'évaluation du caractère adéquat du niveau de protection assuré par un pays tiers ou une organisation internationale, y compris concernant l'évaluation visant à déterminer si un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou une organisation internationale n'assurent plus un niveau adéquat de protection. À cette fin, la

	Commission fournit au comité tous les documents nécessaires, y compris la correspondance avec le gouvernement du pays tiers, en ce qui concerne ledit pays tiers, territoire ou secteur déterminé ou avec l'organisation internationale; - D'émettre des avis sur les projets de décisions des autorités de contrôle conformément au mécanisme de contrôle de la cohérence visé à l'article 64, paragraphe 1, sur les questions soumises en vertu de l'article 64, paragraphe 2, et d'émettre des décisions contraignantes en vertu de l'article 65, y compris dans les cas visés à l'article 66; - De promouvoir la coopération et l'échange bilatéral et multilatéral effectif d'informations et de bonnes pratiques entre les autorités de contrôle; - De promouvoir l'élaboration de programmes de formation conjoints et de faciliter les échanges de personnel entre autorités de contrôle, ainsi que, le cas échéant, avec les autorités de contrôle de pays tiers ou d'organisations internationales; - De promouvoir l'échange, avec des autorités de contrôle de la protection des données de tous pays, de connaissances et de documentation sur la législation et les pratiques en matière de protection des données; - D'émettre des avis sur les codes de conduite élaborés au niveau de l'Union en application de l'article 40, paragraphe 9; et - De tenir un registre électronique, accessible au public, des décisions prises par les autorités de contrôle et les juridictions sur les questions traitées dans le cadre du mécanisme de contrôle de la cohérence. •Le comité émet un rapport annuel sur ses activités qui est rendu public. Le comité peut néanmoins rendre certains débats confidentiels si elle le juge nécessaire.
Chapitre VIII – voies de recours, responsabilité et sanctions Articles 77 à 84	
	•Possibilité de faire une réclamation auprès d'une autorité de contrôle. Il est également possible pour une personne physique ou morale de former un recours juridique contre une décision d'une autorité de contrôle ou contre l'absence de traitement d'une réclamation. Une personne concernée par un traitement peut également mener un recours juridique contre un responsable de traitement ou un sous-traitant si elle considère le traitement de ses données comme constituant une violation du présent règlement. Possible représentativité des personnes concernées. •Les responsables du traitement et sous-traitants sont responsables des

	dommages causés par le non-respect du règlement et sont chargés de la réparation des préjudices infligés. Possibilité aux autorités de contrôle d'affliger une amende administrative pouvant aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaire annuel mondial pour le cas d'une entreprise selon la gravité de la violation.
Chapitre IX – Dispositions relatives à des conditions particulières de traitement (Art 85 à 91)	
	•Conciliation entre le droit à la protection des données personnelles, la liberté d'expression et d'information, le traitement à des fins journalistiques ou d'expression universitaire, artistique ou littéraire par les états membres via des dérogations qui sont à notifier à la commission. •En ce qui concerne le traitement des données personnelles dans le cadre des relations de travail, les États membres peuvent ajouter des règles plus spécifiques que le présent règlement par le biais de lois ou des conventions collectives. Chaque disposition doit également être notifiée à la Commission. •Les traitements à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques doivent garantir les droits et libertés des personnes concernées. Le États membres peuvent prévoir des dérogations à certains articles pour de tels traitements si nécessaire tant que les droits des personnes concernées sont garantis.
Chapitre X – Actes délégués et actes d'exécution (Art 92 à 93)	
	•La Commission peut adopter des actes délégués selon certains articles du règlement. Ces actes doivent être contrôlés par le Parlement Européen ou le Conseil Européen. Ces 2 structures peuvent également mettre fin à la délégation de pouvoir si nécessaire.
Chapitre XI – Dispositions finales (Art 94 à 99)	
	•Précision de l'abrogation de la directive 95/46/CE. N'apporte pas plus d'élément contraignant par rapport à la directive 2002/58/CE concernant le traitement des DCP et la protection de la vie privée dans le secteur de la communication électronique. Les précédents accords internationaux de transfert de données valides sont toujours valables jusqu'à leur modification, leur révocation ou leur remplacement. •Le présent règlement sera réévalué tous les 4 ans par la Commission qui publiera un rapport accessible au public. La Commission pourra également faire des propositions législatives aux États membres pour uniformiser la

	protection des DCP et de leur traitement. •Ce règlement est en application depuis le 25 Mai 2018

Annexe 3 : Outil d'analyse des risques [31]

Outil mis à disposition lors de l'utilisation de la MR-001 pour évaluer le risque de violation de la protection des DCP lors d'un traitement. Il reprend le flux de données que va généré le traitement, les différents acteurs qui ont accès aux données, les mesures de sécurité prises et les principaux risques prévisibles.

Schéma fonctionnel du traitement détaillant les flux de données personnelles et leurs supports

NB : ce schéma doit s'étendre de la collecte jusqu'à la destruction des données

Mesures de sécurité mises en œuvre	
Catégories de mesures sur les données du traitement[1]	**Description des mesures mises en œuvre**
Catégories de mesures générales sur le système d'information 2	**Description des mesures mises en œuvre**

1 Chiffrement, anonymisation, sécurité des documents papier...

2 Cloisonnement du traitement, moyens d'authentification, profils utilisateurs, journalisation, mises à jour et correctifs, antivirus, équipements mobiles, sauvegarde, maintenance, sécurité réseau, contrôle d'accès physique, sécurité physique...

Mesures de sécurité mises en œuvre	
Catégories de mesures organisationnelles 3	Description des mesures mises en œuvre

Violations potentielles des données du traitement	Impacts potentiels sur la vie privée des personnes concernées	Gravité[4]	Menaces rendant possibles les violations de données	Vraisemblance[5]	Justification
Accès illégitime aux données	■ ■ ■		■ ■ ■		
Modification non désirée des données	■ ■ ■		■ ■ ■		
Disparition des données	■ ■ ■		■ ■ ■		

NB : la gravité des impacts et la vraisemblance des menaces tient compte des mesures de sécurité mises en œuvre

On pourra se référer au Guide de la CNIL : « Étude d'impact sur la vie privée », PIA, l'outillage, chapitres 3.2 et 3.3

UNIVERSITÉ DE NANTES

Année de la soutenance
2020

Trisson Florian

L'utilisation des données personnelles dans le cas des essais cliniques, état des lieux et problématique soulevée par la RGPD

A l'heure du numérique, suite l'intérêt grandissant pour le traitement de données personnelles, l'Europe a mis en application en 2018 la Réglementation Générale pour la Protection des Données (RGPD). Cette réglementation qui se veut être l'aboutissement de plusieurs décennies de législation reste malgré tout un texte généraliste, devant s'appliquer dans de nombreux domaines. Certains domaines traitant de données sensibles comme les essais cliniques, possèdent également une réglementation qui leur est propre, que ce soit au niveau français ou européen, et qui ne s'accorde pas parfaitement avec la RGPD. Nous verrons donc en quoi consistent ces textes de loi et nous traiterons des décalages qui peuvent exister entre eux.

MOTS CLÉS

RGPD, ESSAIS CLINIQUES, EUROPE

JURY

PRÉSIDENT : Mme Véronique SEBILLE-RIVAIN, PU-PH, enseignant chercheur en biostatistiques, modélisation et méthodologie des essais cliniques

ASSESSEURS : Mr Jean-Marie BARD, PU-PH de biochimie générale et clinique
Mme Nadège SPARFEL, Pharmacienne

Adresse de l'auteur : 62 Avenue Antoine de St-Exupéry
69100 VILLEURBANNE