www.jusletter.ch

Alexandre Jotterand / Frédéric Erard

Recherche sur l'être humain et données personnelles

Gestion des échanges et répartition des responsabilités

Les échanges de données personnelles sont aujourd'hui omniprésents dans la recherche et posent des questions juridiques complexes. Conçue à la fois dans une optique théorique et pratique, la présente contribution a pour objectif de déterminer les rôles des différents acteurs impliqués dans une recherche et d'identifier leurs obligations en matière de protection des données. Pour y parvenir, les auteurs y examinent le cadre légal applicable et les outils contractuels qui peuvent ou devraient être adoptés par les parties impliquées. Plusieurs cas pratiques inspirés de situations réelles sont également analysés à des fins didactiques.

Catégories d'articles : Articles scientifiques
Domaines juridiques : Droit de la santé

Proposition de citation : Alexandre Jotterand / Frédéric Erard, Recherche sur l'être humain et données personnelles, in : Jusletter 30 août 2021

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Table des matières

1. Introduction

[1] Dire que la conduite d'un projet de recherche nécessite de collecter et traiter des données est une lapalissade. La recherche, particulièrement dans le domaine de la médecine personnalisée, se nourrit de toutes sortes de données, qu'elles soient personnelles ou non, codées ou non, collectées dans le cadre de soins, d'un protocole de recherche, ou observées dans la vie courante (ex. : à l'aide des capteurs d'une montre connectée). Ces données sont collectées, structurées, combinées, partagées et réutilisées par différents acteurs de la recherche, publics ou privés. Si ces activités sont

largement considérées comme des facteurs déterminants du progrès scientifique[1], et donc bénéfiques pour la société dans son ensemble, elles posent des questions juridiquement complexes concernant le respect des règles applicables en matière de protection des données et des droits des participants à la recherche (ceux dont les données sont traitées).

[2] Le présent article se focalise sur la gestion des partages de données dans le cadre de projets de recherche sur l'être humain. Son but est triple : (i) décortiquer les règles applicables aux différentes catégories de données (*section 2*) ; (ii) assigner parmi les acteurs de la recherche (ex. : direction de la recherche/investigateur, centre de recherche, promoteur/sponsor, CRO, commission d'éthique, autorités, etc.) les rôles et responsabilités qui leur incombent lorsqu'ils traitent et partagent des données personnelles (*section 3*) ; et (iii) analyser le régime contractuel qui devrait être mis en place afin d'assurer une gestion adéquate de ces données (et des responsabilités qui en découlent) entre les différents acteurs impliqués (*section 4*).

[3] Enfin, trois exemples pratiques sont analysés (*section 5*). Ces exemples sont tirés de cas concrets provenant de nos expériences professionnelles respectives, et présentent trois situations relativement ordinaires pour des projets de recherche :

- Le cas 1 « *Partage de données entre chercheurs d'hôpitaux universitaires via une infrastructure sécurisée* » (section 5.a) présente la situation « simple » du partage de données entre chercheurs d'hôpitaux universitaires via une infrastructure sécurisée. Dans cet exemple, un chercheur employé dans un hôpital universitaire cantonal souhaite utiliser les données des patients de l'établissement dans lequel il travaille, ainsi que des données d'autres hôpitaux dans le cadre d'un projet de recherche. Les données des patients sont mises à disposition via une infrastructure sécurisée exploitée par un tiers.
- Le cas 2 « *Partage de données dans le cadre d'un consortium de recherche* » (section 5.b) présente la situation dans laquelle des données sont échangées au sein d'un large consortium international de recherche, via une infrastructure développée par les parties.
- Le cas 3« *Réalisation d'un essai clinique* » (section 5.c) présente la situation dans laquelle une entreprise pharmaceutique privée et un hôpital public collaborent en vue de la réalisation d'un essai clinique.

[4] Les exemples pratiques font l'objet d'une analyse et d'explications qui synthétisent le contenu de cet article. Le lecteur pressé pourra se concentrer dans un premier temps sur la lecture de ces exemples.

1 SPHN, Responsible Data Processing in Personalized Health Research, 2e version, 7 mai 2018, p. 11 ; ALLEA, EASAC and FEAM Joint initiative on resolving the barriers of transferring public sector data outside the EU/EEA, International Sharing of Personal Data for Research, avril 2021, disponible sous www.doi.org/10.26356/IHDT (cité : ALLEA/EASAC/FEAM, International Sharing of Personal Data for Research). Tous les liens URL cités dans cet article ont été visités la dernière fois le 20 juin 2021.

2. Cadre légal applicable et catégorisation des données traitées

a. Remarques introductives

[5] La présente contribution se concentre essentiellement sur la gestion des données personnelles relatives aux participants à la recherche[2] et l'échange de ces données dans le cadre des projets de recherche sur l'être humain. En Suisse, la recherche sur l'être humain, et plus précisément la recherche sur les maladies humaines et sur la structure et le fonctionnement du corps humain[3], est régie à titre principal par la loi fédérale relative à la recherche sur l'être humain (LRH). Celle-ci définit de manière générale la « *recherche* » comme « *la recherche méthodologique visant à obtenir des connaissances généralisables* »[4], une notion qui se veut volontairement large. Comme l'expliquait le Conseil fédéral, la recherche sur l'être humain se rapporte non seulement aux activités de recherche pratiquées directement sur les personnes, mais englobe aussi plus largement les recherches sur du matériel biologique d'origine humaine ou des données personnelles par exemple[5].

[6] Tous les échanges de données effectués dans le cadre d'un projet de recherche n'ont pas nécessairement pour objet des données « *personnelles* ». Certains projets se limitent par exemple à analyser des données agrégées qui ne se rapportent à aucune personne physique identifiée ou identifiable. Les projets de recherche multipartites impliquent de surcroît souvent des échanges d'informations sans lien avec l'objet direct de la recherche, à l'instar d'informations financières ou de données purement techniques. Par ailleurs, lorsque des données « *personnelles* » sont effectivement partagées entre plusieurs acteurs dans le contexte d'une recherche, ces données ne se rapportent pas nécessairement à des participants à la recherche. Elles peuvent en effet aussi concerner les chercheurs impliqués dans le projet ou le personnel des institutions impliquées. Ainsi, l'institution qui traite des données relatives aux employés d'une autre institution partenaire est tenue de respecter les règles applicables en matière de protection des données.

[7] Enfin, cet article se focalise sur les problématiques liées à la protection des données dans le cadre de projets de recherche. Bien que certains aspects réglementaires soient présentés, l'article n'a pas vocation à analyser les enjeux réglementaires liés à la conduite d'un projet de recherche. Nous ne traiterons pas non plus de manière spécifique des règles applicables à la gestion du matériel biologique. Ainsi, nous renonçons à présenter dans le détail le régime juridique applicable aux biobanques, même s'il est vrai que leur gestion implique le traitement de données personnelles[6].

[8] Avant de présenter les différents acteurs potentiellement impliqués et d'identifier leurs rôles respectifs, il convient d'abord de se pencher sur la nature des données échangées et l'identification du cadre juridique qui leur est applicable.

---

2 Sur la notion de « participant à la recherche », cf. *infra* section 3.a.i.

3 Art. 2 al. 1 de la loi fédérale du 30 septembre 2011 relative à la recherche sur l'être humain (LRH ; RS 810.30).

4 Art. 3 let. a LRH.

5 Message du Conseil fédéral du 12 septembre 2007 relatif à l'article constitutionnel concernant la recherche sur l'être humain, FF 2007 6345, 6354.

6 Sur la question des biobanques : Yves Donzallaz, Traité de droit médical, vol. II, Berne 2021, N 6153 ss.

b. Droit général de la protection des données

i. Droit suisse

[9] Les traitements de données personnelles effectués par des personnes privées ou des organes fédéraux sont soumis à la loi fédérale sur la protection des données (art. 2 al. 1 LPD). Après un processus long de plusieurs années, le Parlement fédéral a adopté une nouvelle loi fédérale sur la protection des données au cours de l'automne 2020 (nLPD)[7].

[10] Pour des questions liées au fédéralisme helvétique, les traitements de données personnelles effectués par des organes cantonaux sont quant à eux soumis aux législations cantonales sur la protection des données. Aujourd'hui, tous les cantons se sont dotés de lois sur la protection des données[8]. Dans le contexte de la recherche, le rôle des lois cantonales sur la protection des données ne doit pas être sous-estimé. Bon nombre des plus grandes institutions de recherche en Suisse sont en effet des organes cantonaux (ex. : hôpitaux universitaires) et sont donc en principe soumises aux lois cantonales en matière de protection des données[9].

[11] La LPD et les lois cantonales sur la protection des données s'appliquent aux « traitements » de « données personnelles ». Les traitements sont définis de manière large et visent, selon la lettre de la LPD dans sa version actuellement en vigueur, « *toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données* » (art. 3 let. e LPD). Dans la LPD révisée, cette liste sera complétée par les actions d'enregistrement et d'effacement (art. 3 let. d nLPD).

ii. Droit européen

[12] En sus de la législation suisse (fédérale et cantonale) sur la protection des données, il est possible que le Règlement général européen sur la protection des données (RGPD)[10] s'applique (ou soit appliqué) à des activités de recherche réalisées depuis la Suisse, en particulier dans les situations qui suivent.

[13] Premièrement, en application du critère du lieu d'établissement, le RGPD s'applique « *au traitement des données à caractère personnel effectué* ***dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union****, que le traitement ait lieu ou non dans l'Union* » (art. 3 par. 1 RGPD ; nous mettons en évidence). Cette clause est interprétée de manière large et peut s'appliquer à des entités sises en Suisse qui disposent

7 FF 2020 7397, délai référendaire échu sans qu'un référendum n'ait abouti. Cette loi ne devrait toutefois pas entrer en vigueur avant le début de l'année 2023. Le projet de révision total de l'ordonnance relative à la loi sur la protection des données (OLPD) a été mis en consultation le 23 juin 2021 (disponible sous https://www.fedlex.admin.ch/fr/consultation-procedures/ongoing#https://fedlex.data.admin.ch/eli/dl/proj/2021/30/cons_1) et n'est pas encore définitif à l'heure où ces lignes sont écrites.

8 Les cantons du Jura et Neuchâtel ont quant à eux conclu un concordat intercantonal à cet effet RS-NE 150.30.

9 Par exemple pour Genève : cf. art. 3 al. 2 let. c de la loi genevoise du 5 octobre 2001 sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD ; RS GE A 2 08) *cum* art. 3 al. 1 let. d de la loi genevoise du 27 septembre 2017 sur l'organisation des institutions de droit public (LOIDP ; RS GE A 2 24).

10 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).

d'un établissement, voire d'un seul employé ou agent[11], dans l'Union européenne. En se fondant notamment sur la jurisprudence *Google Spain*[12], le Comité européen de la protection des données retient qu'un lien « inextricable » peut exister entre les traitements effectués par une entité sise hors de l'Union européenne et les activités de l'établissement sur le territoire de l'Union européenne (justifiant l'application du RGPD à ces traitements), même si l'établissement dans l'Union européenne ne joue aucun rôle dans ces traitements[13]. Ce cas d'application du RGPD pourrait notamment concerner des entreprises suisses effectuant des activités de prospection commerciale ou du marketing dans l'Union européenne (à travers un représentant local) se rapportant à des activités de recherche réalisées en Suisse.

[14] Deuxièmement, selon l'art. 3 par. 2 RGPD, le RGPD peut s'appliquer aux traitements de données personnelles relatifs à des personnes concernées qui se trouvent sur le territoire de l'Union européenne par un responsable de traitement ou un sous-traitant qui n'est pas établi dans l'Union européenne. Il faut toutefois que les activités de traitement soient liées à l'offre de biens ou de services aux personnes concernées ou, alternativement, au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne.

[15] La question de savoir si les projets de recherche menés en Suisse avec des données relatives à des personnes qui se trouvent dans l'Union européenne remplit ou non les critères d'extraterritorialité définis par l'article 3 par. 2 RGPD n'est pas claire. On peut en effet légitimement se demander si les traitements de données qui interviennent dans le contexte d'une recherche scientifique constituent une offre de « biens » ou de « services » à des personnes qui se situent sur le territoire de l'Union européenne. Tel pourrait éventuellement être le cas si les participants à la recherche qui se trouvent en Europe reçoivent des informations en lien avec les résultats du projet de recherche[14] (ce à quoi ils ont droit en vertu de l'art. 7 LRH).

[16] En ce qui concerne les suivis de comportement, le considérant 24 du RGPD explique que ces suivis doivent intervenir par le biais d'internet. Le Comité européen de la protection des données retient toutefois un champ plus large et estime que le suivi (ou pistage) doit aussi être pris en considération s'il intervient par d'autres types de réseaux ou de technologies impliquant un traitement de données à caractère personnel[15]. Il souligne que le suivi peut englober un large éventail d'activités, à l'instar de la surveillance de l'état de santé d'une personne ou de l'établissement de rapports réguliers connexes[16]. Dans le contexte de la recherche, on peut présumer qu'un suivi en temps réel de participants à la recherche qui se situent sur le territoire de l'Union européenne constitue un suivi de comportement entraînant l'application du RGPD pour le traitement des données concernées[17]. Pour d'autres types de projets, à l'instar d'études longitudinales ou de simples études impliquant la réutilisation de données de recherche concernant des personnes en

11 Comité européen de la protection des données, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), version 2.0, 12 novembre 2019, p. 7.

12 Arrêt de la CJUE du 13 mai 2014, Google Spain,C-131/12, ECLI :EU :C :2014 :317.

13 Comité européen de la protection des données, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), version 2.0, 12 novembre 2019, pp. 8–9.

14 David Peloquin/Michael DiMaio/Barbara Bierer/Mark Barnes, Disruptive and avoidable : GDPR challenges to secondary research uses of data, European Journal of Human Genetics 2020, p. 697 ss, 702.

15 Comité européen de la protection des données, Lignes directrices 3/2018 relatives au champ d'application territorial du RGPD (article 3), version 2.0, 12 novembre 2019, p. 22.

16 *Idem*, p. 23.

17 Peloquin/DiMaio/Bierer/Barnes (nbp 14), p. 697 ss, 702.

Europe, une analyse au cas par cas est préconisée[18]. La Commission européenne a, quant à elle, proposé une interprétation favorisant un champ d'application (trop) large du RGPD. Dans un document à visée informative uniquement, elle a en effet estimé que le RGPD trouvait déjà application dans le cas où le promoteur d'un essai clinique traite des données personnelles relatives à des participants à la recherche situés dans l'Union européenne, y compris dans le cadre de la gestion d'un essai clinique (« *in the context of managing the clinical trial* »)[19].

[17] Troisièmement, indépendamment des critères décrits ci-dessus, l'application du RGPD entre en pratique régulièrement en considération lorsque des recherches menées en Suisse présentent des liens avec l'Union européenne, par exemple lorsqu'une institution suisse participe à un projet de recherche européen ou qui implique des équipes de recherche européennes[20]. Dans un tel contexte, une équipe de recherche suisse peut être amenée à traiter en Suisse des données personnelles collectées par des partenaires européens et/ou qui concernent des participants à la recherche situés sur le territoire de l'Union européenne. Ces partenaires européens doivent s'assurer (pour se conformer à leurs propres obligations) que les données qu'ils transmettent seront traitées conformément aux règles du RGPD et chercheront en conséquence à imposer contractuellement à leurs partenaires étrangers le respect du RGPD. Enfin, le RGPD est fréquemment utilisé en tant que standard en matière de protection des données, en particulier lors de collaborations impliquant des partenaires se trouvant dans des juridictions différentes. Dans ces situations, les équipes de recherche situées en Suisse se trouveront *de facto* contraintes d'accepter contractuellement de se conformer aux règles du RGPD si elles veulent participer au projet de recherche.

c. Réglementation spéciale dans le domaine de la recherche sur l'être humain

i. Droit suisse

[18] La loi fédérale relative à la recherche sur l'être humain (LRH) est une loi spéciale[21] qui contient des règles particulières pour les traitements de données intervenant dans le contexte de la recherche sur l'être humain[22]. Ces dispositions prennent ainsi le pas sur les réglementations générales du droit de la protection des données, sans toutefois évincer complètement celles-ci.

---

18 En faveur de l'application du RGPD aux études longitudinales qui impliquent des personnes en Europe au regard de la nature des données concernées (santé et/ou génétique) : Ana Nordberg, Biobank and Biomedical Research : Responsibilities of Controllers and Processors Under the EU General Data Protection Regulation, in : Santa Slokenberga et al. (édit.), GDPR and Biobanking, Cham 2021, p. 61 ss, p. 67, accessible en libre accès : https://link.springer.com/book/10.1007%2F978-3-030-49388-2.

19 Commission européenne / Direction générale Santé et sécurité alimentaire, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, avril 2019, consultable ici : https://ec.europa.eu/health/sites/default/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

20 Voir par exemple l'*Innovative Medicines Initiative (IMI)*, une initiative soutenue à la fois par l'Union européenne et le secteur privé qui vise à soutenir la recherche dans le domaine de la médecine. Pour plus d'informations : www.imi.europa.eu.

21 La LPD et les législations cantonales sur la protection des données constituent des normes dites « générales ». Elles peuvent être supplantées par des législations dites spéciales (*lex specialis*), qui imposent des règles particulières en matière de protection des données dans certains domaines spécifiques. De telles règles spéciales sont nombreuses en pratiques et sont disséminées dans une multitude de lois. En général, ces lois spéciales se limitent à régler certains aspects des traitements de données seulement. Les lois générales viennent alors compléter les règles spéciales sur les points que ces dernières ne règlent pas.

22 SHK HFG-Brunner, Vorbemerkungen art. 56–61 N 4, in : Bernhard Rütsche (édit.), Humanforschungsgesetz (HFG), Berne 2015 (cité : SHK HFG-Auteur) ; Frédéric Erard, Les données codées dans le contexte de la re-

Ces dernières continuent à s'appliquer là où la LRH reste muette, par exemple pour l'application des principes généraux en matière de protection des données (ex. : principes de proportionnalité ou de légalité).

[19] Les traitements de données personnelles qui interviennent dans le cadre de projets de recherche seront donc soumis aux dispositions de la LRH, en sus de la réglementation générale du droit de la protection des données. La LRH contient notamment des dispositions spécifiques sur le droit à l'information et l'obligation d'obtenir le consentement des participants à la recherche (not. art. 7, 8, et 16 à 18 LRH), ainsi qu'un chapitre spécifique sur les conditions de réutilisation des données personnelles liées à la santé (chapitre 4, art. 32–35 LRH).

[20] La « réutilisation » des données se distingue de l'« utilisation primaire » des données, qui couvre notamment toutes les opérations de traitements de données effectuées dans le contexte des soins ou les opérations relatives à une recherche ou un essai clinique spécifique, depuis le début de la recherche ou de l'essai (en particulier la collecte des données) jusqu'à la fin de la période d'archivage des données[23]. La LRH établit un système relativement complexe de niveaux de consentements de la personne concernée pour la réutilisation de ses données. Les possibilités de réutilisation et les exigences formelles du consentement nécessaires dépendent dans une double mesure de la nature des données (données génétiques ou non génétiques) et de la forme des données (données non codées, codées ou anonymisées). Selon le type de données en jeu, le consentement à la réutilisation des données n'est admissible que pour un projet de recherche en particulier ou « à des fins de recherche » en général. La LRH prévoit par ailleurs des règles allégées pour le recueil du consentement des personnes concernées en vue de la réutilisation de leurs données sous forme « codée ». Par exemple, un participant à la recherche peut consentir de manière générale à ce que ses données génétiques soient réutilisées sous forme codée « à des fins de recherche », alors que son consentement doit être donné spécifiquement pour chaque projet de recherche lorsque ses données génétiques sont traitées sous une forme non codée (art. 32 al. 1 et 2 LRH). Quant aux données non génétiques, elles peuvent être utilisées sous forme codée « à des fins de recherche » si le participant à la recherche ne s'y est pas opposé (art. 33 al. 2 LRH), alors que son consentement est nécessaire pour une utilisation sous forme non codée (art. 33 al. 1 LRH). Dans ce dernier cas, le consentement peut néanmoins aussi être général.

[21] L'examen détaillé du système de consentements mis en place dans le cadre de la LRH dépasse toutefois le cadre de la présente contribution et nous renvoyons à la doctrine spécifique sur cette question[24]. Notons cependant qu'à défaut de consentement, l'article 34 LRH prévoit une règle d'exception (*escape clause*) qui permet de réutiliser, « à titre exceptionnel » seulement, des données personnelles liées à la santé aux conditions strictes posées par l'article 34 LRH[25]. Parmi celles-ci figure l'impossibilité ou les difficultés disproportionnées d'obtenir le consentement de

---

cherche : personnelles ou anonymes, AJP/PJA 2021/5, p. 613 (cité : Erard, Les données codées) ; David Rosenthal, Die rechtlichen und gefühlten Grenzen der Zweitnutzung von Personendaten, sic ! 2021, p. 168, 170.

23 Sous l'angle du droit européen : Commission européenne / Direction générale Santé et sécurité alimentaire, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, avril 2019, consultable ici : https://ec.europa.eu/health/sites/default/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

24 Par exemple : Valérie Junod/Bernice Elger, Données codées, non codées ou anonymes : des choix compliqués dans la recherche médicale rétrospective, in : Jusletter 10 décembre 2018 ; Alexandre Barbey, La recherche sur l'être humain envisagée sous l'angle de la protection des données, Berne 2021, p. 26 ss, disponible en libre accès : https://register.weblaw.ch/bookinfo.php?book_id=2250&pref_lang=fr.

25 Barbey (nbp 24), p. 27.

la personne concernée. La réutilisation de données de santé au sens de l'article 34 LRH doit faire l'objet d'une autorisation délivrée par la commission d'éthique compétente (art. 45 al. 1 let. b LRH).

[22] La LRH est complétée par deux ordonnances d'exécution, qui contiennent toutes deux des dispositions relatives à la protection des données. L'ordonnance fédérale relative à la recherche sur l'être humain à l'exception des essais cliniques (ORH)[26] impose par exemple des règles relatives à la conservation des données personnelles liées à la santé (art. 5 ORH), à l'information qui doit être donnée à la personne concernée lors du recueil du consentement pour la participation à la recherche (art. 8 ORH, voir aussi 28 ss ORH pour le consentement à la réutilisation des données), aux conséquences de la révocation du consentement (art. 10 ORH), à la définition de la réutilisation de données (art. 24 ORH), à l'anonymisation des données (art. 25 ORH) ou encore au codage et au décodage des données (art. 26 et 27 ORH). Pour sa part, l'ordonnance fédérale sur les essais cliniques dans le cadre de la recherche sur l'être humain se concentre, comme son nom l'indique, sur les essais cliniques et contient des dispositions du même type sur la protection des données dans le contexte des essais cliniques.

ii. Droit européen

[23] En vue d'encadrer les activités de recherche sur l'être humain, l'Union européenne a en particulier adopté le Règlement (UE) n° 536/2014 relatif aux essais de médicaments à usage humain (généralement abrégé « CTR » pour « *Clinical Trial Regulation* »)[27]. Bien qu'il soit en vigueur depuis 2014, il n'entrera vraisemblablement pas en force avant janvier 2022 et les essais cliniques restent pour l'heure soumis à l'ancienne directive européenne 2020/20/CE[28]. Les traitements de données de recherche qui ne sont pas liées à des essais cliniques sont quant à eux soumis au RGPD ainsi qu'aux législations nationales pertinentes adoptées par les États membres, dans la mesure de leurs compétences. Cette situation conduit à des disparités juridiques au sein de l'Union européenne. Pour des raisons de simplification et à titre d'illustration, les lignes qui suivent se focalisent toutefois essentiellement sur les traitements de données liées aux essais cliniques, tels qu'ils sont réglés par le nouveau règlement (CTR).

[24] Si le CTR contient certes des dispositions relatives à la manière de traiter des données à caractère personnel dans le contexte d'essais cliniques[29], il renvoie aussi de manière générale aux règles établies par le RGPD (via le renvoi de l'art. 93 CTR notamment[30]). Les interactions entre les activités de recherche et le RGPD sont toutefois complexes.

[25] Alors que la LRH helvétique prône un système essentiellement centré sur le consentement du participant à la recherche pour l'utilisation ou la réutilisation de ses données, le droit européen établit des règles sensiblement différentes. Sous l'angle du RGPD, un traitement de données n'est

26 RS 810.301.

27 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.

28 Directive 2001/20/CE du Parlement européen et du Conseil du 4 avril 2001 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.

29 Ex. : art. 28 par. 2, 57 et 58 CTR pour les règles relatives à la réutilisation des données, la tenue d'un dossier permanent de l'essai clinique et à son archivage.

30 À noter que cette disposition renvoie à l'ancienne directive 95/46/CE, remplacée depuis par le RGPD.

licite que s'il remplit l'une des conditions prévues par l'art. 6 RGPD. De surcroît, l'art. 9 par. 1 RGPD interdit par principe les traitements portant sur des catégories particulières de données à caractère personnel, à l'instar des données génétiques ou des données concernant la santé. De tels traitements peuvent toutefois être justifiés en présence de l'un des motifs énoncés dans la liste de l'art. 9 par. 2 RGPD, étant entendu que États membres gardent la possibilité d'adopter des régimes plus stricts pour encadrer les traitements de données génétiques, de données biométriques ou de données concernant la santé (art. 9 par. 4 RGPD).

[26] Selon l'avis du Comité européen de la protection des données et de la Commission européenne, les opérations de traitements de données sont en premier lieu justifiées lorsqu'elles reposent sur une obligation légale en vue d'assurer la fiabilité et la sécurité des essais cliniques[31]. Quant aux opérations de traitements de données purement liées aux activités de recherche, elles peuvent, selon les circonstances, être justifiées pour trois motifs[32,33] :

- L'opération de traitement est nécessaire à l'exécution d'une mission d'intérêt public, alternativement dans le domaine de la santé publique ou à des fins de recherche scientifique (art. 6 par 1 let. e *cum* art. 9 par. 2 let. i et j RGPD). Le fondement d'un tel traitement doit toutefois être défini par le droit de l'Union européenne ou le droit national des États membres (art. 6 par. 3 RGPD).
- L'opération de traitement relève des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, lorsqu'elle est nécessaire à des fins de recherche scientifique (art. 6 par 1 let. f *cum* art. 9 par. let. j RGPD). Un tel traitement doit lui aussi reposer sur une base légale inscrite dans le droit de l'Union européenne ou d'un État membre, et doit respecter les garanties prévues par l'art. 89 par. 1 RGPD.
- L'opération de traitement repose sur le consentement explicite de la personne concernée (art. 6 par. 1 let. a *cum* art. 9 par. 2 let. a RGPD). Les deux instances opèrent cependant une distinction entre le consentement donné en vue de la recherche de celui qui porte sur le traitement de données. Le consentement pour la participation à la recherche est d'abord un garde-fou qui permet d'assurer la protection des personnes concernées et ne vise pas en lui-même à justifier les traitements de données à la lumière du RGPD. Par ailleurs, aussi bien le Comité européen de la protection des données que la Commission européenne insistent sur la prudence à adopter lorsqu'il faut examiner le caractère libre du consentement dans le contexte particulier de la recherche. En raison des circonstances qui entourent les essais

31 Comité européen de la protection des données, Avis 3/2019 concernant les questions et réponses sur l'interaction entre le règlement relatif aux essais cliniques et le règlement général sur la protection des données (RGPD), 23 janvier 2019, p. 5 ; Commission européenne / Direction générale Santé et sécurité alimentaire, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, avril 2019, p. 4, consultable ici : https://ec.europa.eu/health/sites/default/files/files/documents/qa_clinicaltrials_gdpr_en.pdf.

32 Commission européenne / Direction générale Santé et sécurité alimentaire, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, avril 2019, p. 4 ss, consultable ici : https://ec.europa.eu/health/sites/default/files/files/documents/qa_clinicaltrials_gdpr_en.pdf. Voir aussi : Comité européen de la protection des données, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 février 2021, p. 5, qui évoque aussi la possibilité de recourir à la base légale du traitement nécessaire pour respecter une obligation légale selon l'art. 6 par. 1 let. c RGPD, consultable ici : https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf.

33 Sur cette question débattue, voir aussi par exemple : Magalie Wasem Tréguer, Where Do We Stand on Patients' Informed Consent Forms ?, Life Science Recht 2019, p. 192 ss.

cliniques par exemple, cette liberté pourra rarement être assurée en pratique, de telle sorte qu'il faudra généralement s'appuyer en priorité sur l'un des deux autres motifs mentionnés ci-dessus pour justifier l'opération de traitement de données.

[27] La réutilisation des données collectées dans le cadre de la recherche à des fins différentes de celles prévues dans le protocole de recherche initiale (utilisation secondaire) nécessite, elle aussi, de reposer sur un motif énoncé à l'art. 6 par. 1 RGPD pour être licite, étant entendu que ce motif ne doit pas nécessairement être le même que celui qui justifie le traitement primaire des données[34]. Sans préjudice du RGPD, l'art. 28 par. 2 CTR énonce que le promoteur d'un essai clinique peut demander au participant ou à son représentant d'accepter que ses données soient utilisées en dehors du protocole et exclusivement à des fins scientifiques, et que ce consentement peut être retiré à tout moment. En vertu de la réserve à l'égard du RGPD, d'autres motifs que le consentement (voir ci-dessus) peuvent toutefois justifier l'utilisation secondaire des données de recherche à des fins scientifiques. Plus généralement, une attention particulière devra être portée à la question de la compatibilité entre le traitement primaire et le traitement secondaire. À cet égard, l'art. 5 par. 1 let. b RGPD prévoit, à certaines conditions, une présomption de compatibilité pour les traitements secondaires qui seraient opérés à des fins de recherche scientifique. Les contours de cette présomption suscitent néanmoins des discussions et, selon les circonstances, la recherche d'un nouveau consentement ou la conduite d'un test de compatibilité au sens de l'art. 6 par. 4 RGPD peut se révéler nécessaire.

iii. Autres normes

[28] Lorsqu'un projet de recherche implique des échanges de données entre des parties situées dans des États différents, la licéité des traitements de données va également dépendre du droit national applicable à chacune des parties. Dans l'Union européenne, le RGPD octroie par exemple certaines marges de manœuvre aux États pour régler les traitements de données effectués dans le cadre de la recherche sur l'être humain[35]. Aux États-Unis, les traitements de données de santé sont en bonne partie réglés par le *Health Insurance Portability and Accountability Act 1996* (HIPAA), dont le champ d'application est toutefois limité aux données générées dans le contexte des soins. En dépit de cela, l'HIPAA est souvent utilisé en dehors des États-Unis dans le milieu de la recherche ou de l'informatique médicale en guise de standard pour les questions liées à l'anonymisation des données par exemple (méthodes de dé-identification des données). De telles pratiques doivent toutefois être soigneusement évaluées à la lumière du droit applicable, car le droit suisse ou le RGPD imposent généralement un cadre légal plus strict[36].

---

34 Commission européenne / Direction générale Santé et sécurité alimentaire, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation, avril 2019, p. 7–8, consultable ici : https://ec.europa.eu/health/sites/default/files/files/documents/qa_clinicaltrials_gdpr_en.pdf. Voir aussi : Comité européen de la protection des données, Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research, 2 février 2021, p. 6-7, consultable ici : https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf.

35 Pour des exemples dans le contexte de la recherche, voir : James Scheibner et al., Data protection and ethics requirements for multisite research with health data : a comparative examination of legislative governance frameworks and the role of data protection technologies, Journal of Law and the Biosciences, 6 mai 2020, p. 12, accessible en libre accès : https://academic.oup.com/jlb/article/7/1/lsaa010/5825716.

36 James Scheibner et al., (nbp 35), p. 9.

[29] En résumé, chaque projet impliquant l'échange de données à l'échelon international doit faire l'objet d'une analyse spécifique qui implique l'examen des droits applicables à chacune des parties amenées à traiter les données, de telle sorte à s'assurer que les données personnelles de recherche seront en tout temps traitées de manière licite au regard des obligations légales imposées aux parties qui fournissent les données en particulier. Il faut également souligner ici l'importance de respecter les conditions légales imposées par les législations applicables en matière de transfert de données personnelles à l'étranger, en particulier lorsque l'État destinataire ne bénéficie pas d'un niveau de protection reconnu comme équivalent à celui de l'État expéditeur[37]. Cette question dépasse cependant le cadre de la présente contribution.

[30] En parallèle, les projets de recherche impliquant des échanges de données personnelles doivent être menés dans le respect du cadre réglementaire et éthique plus large applicable à la recherche. De manière non exhaustive, on mentionnera en particulier :

- les règles posées pour la recherche scientifique par la Convention sur les Droits de l'Homme et la Biomédecine du 4 avril 1997 (art. 15 ss). En particulier, ce texte dispose qu'un projet de recherche sur des personnes ne peut être réalisé que si celles-ci ont été dûment informées de leurs droits et des mesures requises par la loi pour leur protection (art. 16 lit. iv), et qu'elles ont (sauf exception) donné leur consentement de manière expresse et spécifique, lequel doit au demeurant être documenté (art 16 lit. v cum 5) ;
- la Déclaration universelle sur la bioéthique et les droits de l'homme de l'UNESCO du 19 octobre 2005, dont l'art. 9 prône le principe de vie privée et de confidentialité. Ce dernier expose que, dans toute la mesure du possible, les informations collectées sur les personnes « *ne devraient pas être utilisées ou diffusées à des fins autres que celles pour lesquelles elles ont été collectées ou pour lesquelles un consentement a été donné, en conformité avec le droit international, et notamment avec le droit international des droits de l'homme* » ;
- les déclarations de l'Association médicale mondiale (AMM). On pense d'abord à la Déclaration d'Helsinki qui énonce les principes éthiques centraux applicables à la recherche médicale impliquant des êtres humains, y compris la recherche sur du matériel biologique humain et sur des données identifiables. L'AMM a aussi adopté plus spécifiquement en 2016 la Déclaration de Taipei sur les considérations éthiques concernant les bases de données de santé et les biobanques ;
- les lignes directrices internationales d'éthique pour la recherche en matière de santé impliquant des participants humains du Conseil des Organisations internationales des Sciences médicales (CIOMS) ;

37 À ce sujet, notons que suite à l'arrêt de la Cour de Justice de l'Union européenne C-311/18 du 16 juillet 2020 (Schrems II), les Etats-Unis ne sont plus reconnus par l'Union européenne et la Suisse comme un Etat offrant un niveau de protection adéquat (art. 45 RGPD ; art. 6 al. 1 LPD). Les communications de données personnelles à destination des Etats-Unis doivent donc nécessairement reposer sur des garanties appropriées au sens des art. 46 RGPD ou 6 al. 2 LPD, à l'exemple de garanties contractuelles suffisantes. La Commission européenne a récemment publié de nouvelles clauses types de protection des données, voir : Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil. Quant au Préposé fédéral à la protection des données et à la transparence, il a publié en juin 2021 un « Guide pour l'examen de la licéité de la communication transfrontière de données (art. 6, al. 2, let. a, LPD) » visant à faciliter l'examen de la licéité du transfert de données à caractère personnel vers l'étranger, consultable ici : https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html.

- l'obligation d'observer le secret professionnel en matière de recherche sur l'être humain instituée par l'art. 321bis CP ;
- pour les essais cliniques, les bonnes pratiques cliniques mentionnées à l'annexe 1 de l'OClin, notamment la directive de la Conférence internationale sur l'harmonisation relative aux bonnes pratiques cliniques[38]. Conformément à l'art. 5 al. 1 OClin, les essais cliniques doivent être réalisés conformément à ces règles[39] ;
- enfin, à l'échelon helvétique, le ELSI Advisory Group du Swiss Peronalized Health Network (SPHN) a adopté un cadre éthique pour des traitements de données responsables dans le contexte de la recherche en santé personnalisée[40]. Les participants à des projets de recherche financés par le SPHN sont tenus de se conformer à ce cadre. Le cadre est basé sur quatre principes généraux, soit (i) le respect des personnes dont les données sont traitées dans le contexte d'un projet de recherche, y compris leur droit à l'autodétermination informationnelle ; (ii) la confidentialité et sécurité des données ; (iii) la loyauté ; et (iv) l'*accountability (*responsabilité/imputabilité). En lien avec le contenu du présent article, le cadre fixe des règles pour la réutilisation des données basées sur les art. 32 à 34 LRH, qui sont toutefois en partie plus restrictives que celles de la LRH, notamment pour la réutilisation de données personnelles non génétiques qui ne sont pas codées[41]. Au demeurant, le cadre impose aux institutions participantes de s'assurer par des mécanismes appropriés d'être en mesure de donner rapidement suite aux révocations de consentement des participants à la recherche, ainsi que de pouvoir effectivement être en mesure de communiquer les résultats de la recherche aux participants (notamment par des procédures de réidentification).

d. Catégorisation des données

i. Régime général du droit de la protection des données

[31] Selon la LPD, les **données personnelles** visent « *toutes les informations qui se rapportent à une personne identifiée ou identifiable* » (art. 3 let. a LPD). Une personne est identifiée par des données lorsque son identité ressort directement des informations détenues[42]. Elle est identifiable

38 Conférence internationale sur l'harmonisation (CIH) [*International Council For Harmonisation Of Technical Requirements For Pharmaceuticals For Human Use (ICH)*], Bonnes Pratiques Cliniques [*Good Clinical Practice*] : Integrated Addendum to ICH E6(R2), 9 novembre 2016, disponible sous : https://database.ich.org/sites/default/files/E6_R2_Addendum.pdf (cité : « CIH, Bonnes Pratiques Cliniques »). Un projet de révision de ce document a été mis en consultation en avril 2021, qui n'est toutefois pas encore entrée en vigueur au moment où cet article est rédigé.

39 Des règles spécifiques s'appliquent aux essais cliniques portant sur des dispositifs médicaux de diagnostics et certains produits thérapeutiques qui contiennent des tissus humains dévitalisés, des cellules humaines dévitalisées ou leurs dérivés, ou qui en sont constitués (cf. OClin, annexe 1).

40 SPHN, Ethical Framework for Responsible Data Processing in Personalized Health Research, 2e version, 7 mai 2018, disponible sous : https://sphn.ch/document/ethical-framework. Ce cadre éthique a également été endossé par la Swiss Biobanking Platform et les ETH.

41 Le cadre impose pour ces données un consentement spécifique (lié à un projet de recherche) alors que l'art. 33 al. 1 LRH autorise leur réutilisation sur la base d'un consentement général (pour des projets de recherche futurs encore indéfinis).

42 Philippe Meier, Protection des données. Fondements, principes généraux et droit privé, Berne 2011, N 431 p. 201 (cité : Meier, Protection des données) ; Barbey (nbp 24), p. 12.

lorsqu'elle peut être indirectement identifiée au moyen d'une corrélation d'informations tirées des circonstances ou du contexte[43].

[32] Aussi bien la LPD que les lois cantonales sur la protection des données prévoient des régimes juridiques renforcés pour différentes catégories de données considérées comme sensibles, qui se caractérisent par leur importante répercussion sur la personnalité des personnes concernées[44]. Ces catégories de données sont définies de manière exhaustive dans chacune des lois applicables. Dans la LPD, sont notamment considérées comme sensibles les **données relatives « *à la santé* »**. La notion de santé n'est pas forcément claire, mais la doctrine recommande généralement d'adopter une interprétation large et flexible. Meier définit, par exemple, les données de santé comme « *toutes les informations qui permettent, directement ou indirectement, de tirer des conclusions sur l'état de santé, physique, mental ou psychique, d'une personne* »[45].

[33] Dans le contexte des soins, les données de santé concernent généralement toutes les données concernant le patient, à l'image de l'anamnèse, du résultat des examens cliniques et des analyses effectuées, de l'évaluation de la situation du patient ou encore des soins proposés et ceux effectivement prodigués[46]. Il ne faut cependant pas perdre de vue qu'en raison des développements technologiques récents, un grand nombre de données de santé sont aujourd'hui également collectées en dehors du contexte des soins, notamment au moyen d'appareils portables connectés. Ces données sont non seulement collectées en nombre sensiblement plus important et par de nouveaux acteurs extérieurs au secteur des soins (ex. : Google, Amazon), mais il devient souvent toujours plus difficile de déterminer si elles se rapportent effectivement à la santé ou plutôt aux simples habitudes de vie[47]. Certaines données sans lien apparent avec la santé peuvent potentiellement présenter des liens avec la santé lorsqu'elles sont recoupées entre elles ou lorsqu'elles sont traitées dans un contexte particulier[48].

[34] De manière générale, les données collectées en dehors d'un protocole de recherche, en particulier celles qui sont collectées dans le contexte des soins, sont parfois qualifiées de « ***real world data*** » ou « RWD »[49]. En raison de leur nombre et de leur potentiel, les RWD suscitent évidemment l'intérêt des milieux de la recherche en vue d'en tirer des « *real world evidence* » (données empiriques), par exemple pour développer de nouveaux modèles de santé personnalisée ou pour combattre de manière plus efficace les épidémies[50].

---

43 Message du Conseil fédéral du 15 septembre 2017 concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois, FF 2017 6565 ss, 6639.

44 Message du Conseil fédéral du 23 mars 1988 concernant la loi fédérale sur la protection des données (LPD), FF 1988 II 421 (Message LPD), 455.

45 Meier, Protection des données (nbp 42), N 486.

46 Cette liste exemplative est tirée de l'art. 16 al. 4 de la loi genevoise sur le réseau communautaire d'informatique médicale (e-Toile) du 14 novembre 2008, RG-GE K 3 07.

47 Kerstin Noëlle Vokinger, Gesundheitsdaten im digitalen Zeitalter, in : Jusletter 27 janvier 2020, N 7 ss.

48 Franziska Sprecher, Datenschutz im Gesundheitsbereich : aktuelle Entwicklungen, in : Kieser/Pärli/Uttinger (édit.), Datenschutztagung 2018. Ein Blick auf aktuelle Rechtsentwicklungen, Zurich/St-Gall 2018, p. 137ss, 147.

49 Voir p. ex. : Alea Garbagnati/Dorien Van Doninck/Barbara Schroeder de Castro Lopes, Unlocking the Potential of Scientific Data-Driven Research, Life Science Recht 2020, p. 58ss, 59. Sur la question plus spécifique de la définition des *real world data*, voir notamment : Amr Makady, What Is Real-World Data ? A Review of Definitions Based on Literature and Stakeholder Interviews, Value in Health 2017, p. 858 ss, disponible en ligne : https://www.valueinhealthjournal.com/action/showPdf?pii=S1098-3015%2817%2930171-7.

50 Voir par exemple : Joseph Menzin/Peter Neumann, How Real-World Data Can Help Us Better Prepare for the Next Pandemic, Scientific American, 22 avril 2021, disponible en ligne : https://bit.ly/3gNj4QM. A noter que le cadre éthique développé pour SPHN vise aussi à s'appliquer aux données qui ne sont pas traditionnellement associées aux activités à la recherche, telles que les données de géolocalisation, de médias sociaux ou celles collectées

[35] Dans la LPD révisée, la liste des catégories de données considérées comme sensibles intégrera explicitement les données génétiques (art. 5 let. c ch. 3 nLPD)[51]. L'examen des débats parlementaires montre cependant qu'il ne s'agit pas de toute donnée génétique, mais seulement des données génétiques qui permettent d'identifier une personne[52].

ii. Régime spécial de la loi relative à la recherche sur l'être humain (LRH)

[36] En Suisse, le champ d'application de la LRH s'étend non seulement aux activités de recherche pratiquées directement sur les humains, mais aussi aux recherches menées sur les « **données personnelles liées à la santé** » (art. 2 al. 1 let. e LRH).

[37] Les « données personnelles » liées à la santé sont définies par la LRH comme les « informations concernant une personne déterminée ou déterminable qui ont un lien avec son état de santé ou sa maladie, données génétiques comprises ». À l'exception du fait que la LRH vise spécifiquement les *données relatives à la santé* (cf. *supra* section 2.d.i), la notion de données personnelles est similaire à celle employée par la LPD (art. 3 let. b LPD), et vise aussi bien les données qui se rapportent à des personnes identifiées qu'à des personnes identifiables[53].

[38] En principe, la LRH ne s'applique cependant pas aux recherches pratiquées sur les données qui ont été collectées anonymement ou qui ont été anonymisées (art. 2 al. 2 let. c LRH). Lorsque plusieurs chercheurs ou équipes de recherche s'échangent des données anonymes, ceux-ci peuvent très bien convenir contractuellement de modalités particulières pour l'utilisation des données anonymes (ex. : droits de propriété intellectuelle sur les résultats, citations en cas de publication). La LRH offre cependant à tout le moins une protection limitée aux participants à la recherche qui se trouveraient à l'origine de certaines données anonymes. Lorsque du matériel biologique ou des données génétiques sont en jeu (et uniquement dans ces cas-là), le matériel biologique ou les données génétiques ne peuvent être anonymisés à des fins de recherche que si la personne concernée ne s'y est pas opposée après avoir reçu une information adéquate (art. 32 al. 3 LRH).

[39] Les données anonymisées sont définies par l'art. 3 let. i LRH comme les données « qui ne peuvent être mises en relation avec une personne déterminée ou ne peuvent l'être sans engager des efforts démesurés ». L'art. 25 ORH apporte quelques précisions sur le processus d'anonymisation (ou dé-identification) : toutes les informations qui, combinées, permettent de rétablir l'identité de la personne sans efforts disproportionnés doivent être rendues définitivement méconnaissables ou être détruites. Parmi ces informations figurent en particulier (liste exemplative), le nom, l'adresse, la date de naissance et les numéros d'identification caractéristiques[54].

[40] Les données de recherche sont fréquemment traitées sous une forme codée, parfois aussi désignées comme **données pseudonymisées**. Les **données codées** sont définies par la LRH comme « *les données qui ne peuvent être mises en relation avec une personne déterminée qu'au moyen d'une*

---

au moyen de capteurs portables commerciaux par exemple : SPHN, Ethical Framework for Responsible Data Processing in Personalized Health Research, 2e version, 7 mai 2018, p. 2, disponible sous https://sphn.ch/document/ethical-framework.

51 Sur les difficultés à reconnaitre que des données génétiques puissent encore être anonymes : Barbey (nbp 24), p. 15.

52 Voir en particulier l'intervention de la Conseillère fédérale Keller-Sutter, BO (CN) 2019, p. 1787.

53 Barbey (nbp 24), p. 14.

54 Le droit suisse ne préconise donc pas de méthode spécifique pour anonymiser des données, à l'instar d'une liste exhaustive d'identifiants à rendre méconnaissables (méthode dite du « *safe harbor* »).

clé » (art. 3 let. h LRH). En d'autres termes, le codage vise à remplacer certaines caractéristiques identifiantes de telle manière à ce que seul celui qui est en possession du code puisse réidentifier les données[55]. Il est donc par définition réversible. Selon l'art. 26 al. 1 ORH, les données personnelles de recherche sont réputées correctement codées lorsqu'elles peuvent être qualifiées d'anonymes dans l'optique d'une personne qui n'a pas accès au code. Le code doit par ailleurs être conservé séparément des données de recherche, par une personne qui est désignée dans le projet de recherche soumis à la commission d'éthique, sans toutefois être impliquée dans le projet.

[41] Par rapport à l'anonymisation, le codage des données présente certainement l'avantage d'être plus facile à mettre en œuvre (éviter les incertitudes liées à la question de savoir si les données sont « suffisamment anonymisées ») et permet surtout de réidentifier, si cela est nécessaire, la personne concernée par les données[56]. Un tel procédé peut se révéler particulièrement utile, par exemple pour approfondir des recherches en lien avec certains participants à la recherche. Le codage des données répond par ailleurs aux exigences liées au principe général de proportionnalité (art. 4 al. 2 LPD) puisqu'il équivaut à une mesure de « minimisation » du traitement de données. À ce titre, les technologies de codage sont parfois qualifiées de « *privacy enhancing technology* »[57]. En raison des risques moins importants liés aux traitements de données personnelles codées par rapport aux données personnelles non codées, la LRH prévoit par ailleurs des règles plus permissives pour le recueil du consentement des personnes concernées en vue de la réutilisation de leurs données sous forme codée (cf. *supra* section 2.b.i). Notons encore que dans le contexte des essais cliniques par exemple, le recours à un code d'identification pour chaque participant à la recherche est préconisé par les Bonnes Pratiques Cliniques[58].

[42] Dans le secteur de la recherche sur l'être humain, les données codées doivent être considérées comme des données personnelles, même à l'égard des personnes qui ne disposent pas de la clé permettant la réidentification. En dépit des discussions doctrinales à ce sujet sous l'angle du droit général de la protection des données, cette solution s'impose dans le domaine de la recherche au regard du régime spécial imposé par la LRH et des règles particulières imposées par cette loi pour le traitement des données codées (ex. : les données codées ne peuvent en principe pas être utilisées autrement qu'à des fins de recherche)[59].

3. Identité et rôles des acteurs impliqués

a. Présentation des acteurs potentiels

[43] La réalisation d'un projet de recherche impliquant l'utilisation ou la réutilisation de données personnelles fait nécessairement intervenir plusieurs acteurs. Avant d'examiner leur fonction à la lumière du droit de la protection des données et des responsabilités qui s'y rattachent, il est nécessaire de les identifier et de les présenter brièvement.

55 Meier, Protection des données (nbp 42), N 446 p. 206.

56 Barbey (nbp 24), p. 39.

57 Sur le sujet, cf. section 4.b.

58 § 5.5.5 CIH, Bonnes Pratiques Cliniques (nbp 38).

59 Sur cette question particulière, voir : Erard, Les données codées (nbp 22), p. 606 ss.

i. Participants à la recherche

[44] Bien qu'il se trouve au centre de tout projet de recherche, le « **participant à la recherche** » ou « **sujet de la recherche** » n'est pas défini par le droit suisse. La LRH évoque parfois les « participants à un projet de recherche » (ex. : art. 12 al. 1 LRH) ou la « personne concernée » (ex. : 7 et 8 LRH). Pour des raisons liées au contexte particulier qu'elle régit, l'ordonnance sur les essais cliniques emploie quant à elle plus spécifiquement la notion de « participant à l'essai clinique ».

[45] Dans des lignes directrices à l'attention des comités d'éthique, l'Organisation mondiale de la santé (OMS) propose la définition suivante du participant à la recherche : « *Personne qui participe à une recherche biomédicale, soit comme sujet direct de l'intervention (ex. : administration d'un médicament / exécution d'un acte invasif expérimental), soit comme témoin ou sujet d'observation. La personne peut être, soit un sujet sain acceptant volontairement de participer à la recherche, soit une personne ayant un état non directement lié au sujet de recherche et qui accepte volontairement de participer à l'étude, voire un sujet (généralement un patient) dont la condition justifie l'utilisation du produit étudié ou l'examen des questions qui sont à la base de la recherche* »[60].

[46] La notion de participant à la recherche doit dans tous les cas être interprétée de manière large et vise aussi les personnes dont on utilise (ou réutilise) les données en vue de mener un projet de recherche au sens de la LRH, que ces personnes aient ou non consenti à cette utilisation (ou réutilisation).

ii. Direction du projet et investigateurs

[47] La personne qui mène un projet de recherche est désignée comme la **« direction » du projet** (*project leader/Projektleitung*) ou l'**« investigateur »** (*investigator/Prüfperson*). La direction du projet est responsable de la réalisation pratique du projet de recherche en Suisse et de la protection des personnes participant au projet de recherche au lieu de réalisation (art. 3 al. 1 ORH). Selon la terminologie de la loi, l'investigateur assume quant à lui des responsabilités similaires dans le contexte spécifique des essais cliniques (art. 2 let. d OClin). Ces deux acteurs sont nécessairement des personnes physiques, qui doivent répondre à des exigences légales particulières en matière de qualifications professionnelles (art. 4 ORH ; art. 6 OClin). Il s'agit donc en règle générale du ou des médecins ou chercheurs qui sont responsables de la réalisation pratique du projet de recherche.

[48] La direction du projet et l'investigateur doivent ainsi mener la recherche conformément au plan de recherche (art. 15 let. c ORH) ou au protocole de recherche pour les essais cliniques (art. 25 let. d OClin), tels que validés par la commission d'éthique compétente. Cette fonction implique de nombreuses tâches, parmi lesquelles figurent notamment, selon le type de projet, le recrutement des participants, le recueil du consentement à la participation au projet et/ou à la réutilisation des données, l'application concrète de la méthode ou du traitement à tester, la surveillance de l'essai, la consignation des résultats ou encore la responsabilité d'assumer le point de contact pour les participants à la recherche[61].

---

60 OMS, Lignes Directrices Opérationnelles pour les Comités d'Ethique chargés de l'évaluation de la Recherche Biomédicale, TDR/PRD/ETHICS/2000.1, Genève 2000, p. 16.

61 Shirin Grünig, Die Haftung nach Humanforschungsgesetz. Zugleich eine Untersuchung zum Recht der Gefährdungshaftung, thèse, Zurich 2020, N 137.

[49] Il va sans dire que l'activité même de la direction de la recherche et de l'investigateur implique nécessairement le traitement de données personnelles relatives aux participants à la recherche. Ces activités de traitement peuvent non seulement couvrir la collecte de données, mais aussi leur analyse, leur conservation, leur codage/anonymisation, voire leur destruction.

[50] Un projet de recherche, même monocentrique[62], est rarement mené par un chercheur unique, mais implique généralement l'intervention d'une équipe de recherche composée par exemple de médecins, d'assistants de recherche, de coordinateurs, etc. Ces personnes agissent sous la responsabilité de la direction de recherche ou de l'investigateur, qui est dans ce cadre qualifié d'« **investigateur principal** » (*principal investigator*)[63]. Les personnes qui, sous la supervision du *principal investigator*, ont la responsabilité de prendre des décisions médicales relatives à l'essai clinique, ou d'autres décisions importantes relatives à celui-ci, sont qualifiées de « **sous-investigateurs** » (*subinvestigators*)[64].

[51] Les projets de recherche multicentriques impliquent nécessairement plusieurs chercheurs, actifs dans différents centres de recherche. Dans le contexte des essais cliniques, cette configuration implique de désigner un « **investigateur coordinateur** » (*coordinating investigator*) et des « **investigateurs locaux** » (*local investigators*)[65]. L'investigateur coordinateur est notamment responsable en Suisse de la coordination des investigateurs locaux compétents pour les différents lieux de réalisation des essais cliniques et du dépôt de la demande auprès de la commission d'éthique compétente[66]. Pour les autres projets de recherche, on emploie parfois en pratique les qualifications de « coordinateur du projet »[67] ou de « *project leader of the main center* » et de « *investigators at the local site* » même si, comme on l'a vu, la loi réserve plutôt le terme d'investigateur pour le contexte particulier des essais cliniques.

iii. Centre de recherche/centre investigateur (medical institution)

[52] Le « **centre de recherche** » ou « **centre investigateur** » (*study site* ou *medical institution*/*Prüfzentrum*), parfois également nommé « **institution (médicale)** » (*(medical) institution*), est l'établissement au sein duquel un projet de recherche ou des essais cliniques sont menés, soit en règle générale l'institution au sein de laquelle la direction du projet/l'investigateur principal est actif (en qualité d'employé ou à un autre titre). Plusieurs centres de recherche peuvent collaborer à un même projet de recherche (réalisé sur la base du même protocole de recherche), auquel cas le projet de recherche sera qualifié de « *multicentriques* »[68], par opposition aux projets « monocentrique » menés par un seul centre de recherche.

[53] Le centre de recherche/centre investigateur n'est pas directement mentionné dans la LRH ou ses ordonnances d'exécution, son rôle étant le plus souvent « éclipsé » derrière celui individuel de la direction de projet ou de l'investigateur. Toutefois, dans le cadre d'essais cliniques, les

62 Sur la notion, voir *infra* section 3.a.iii.

63 Grünig (nbp 61), N 143 ; CIH, Bonnes Pratiques Cliniques (nbp 38), N 1.34.

64 CIH, Bonnes Pratiques Cliniques (nbp 38), N 4.31.

65 Art. 27 OClin ; CIH, Bonnes Pratiques Cliniques (nbp 38), N 1.19.

66 Art. 27 OClin.

67 Art. 47 al. 2 LRH.

68 Art. 47 al. 2 LRH et 17 ORH ; CIH, Bonnes Pratiques Cliniques (nbp 38), N 1.40 ; voir également *supra* section 3.a.iii.

bonnes pratiques cliniques du CIH (applicables par le renvoi de l'art. 5 al. 1 OClin à l'annexe 1 de l'OClin) font supporter de manière indifférenciée la responsabilité de certaines tâches liées à la conduite d'essais cliniques à l'investigateur et/ou au centre de recherche[69]. Au demeurant, c'est en principe directement avec le centre de recherche que la relation contractuelle avec les participants à la recherche est nouée, et non pas avec l'investigateur et/ou la direction du projet. Il en va de même de la relation avec le promoteur (cf. section suivante), qui en pratique est conclue entre le promoteur et le ou les centres de recherche concernés, l'accord entre ces parties nommant alors les investigateurs en charge de la recherche[70]. Il n'est toutefois pas impossible qu'un chercheur agisse de manière indépendante (sans dépendre d'un centre de recherche), auquel cas il sera directement partie au contrat.

iv. Promoteur de la recherche/sponsor

[54] Le « **promoteur** » ou « **sponsor** » est la personne ou entité qui est responsable de l'initiative du projet de recherche, soit en particulier son lancement, sa gestion et son financement en Suisse, si aucune autre institution en Suisse n'en assume la responsabilité (voir art. 3 al. 2 ORH et art. 2 let. c OClin pour les essais cliniques)[71]. Il peut notamment s'agir d'une entreprise pharmaceutique souhaitant mettre sur le marché un nouveau médicament, ou d'une société innovante développant des prothèses médicales, qui doivent conduire un essai clinique en vue de la mise sur le marché de leur produit.

[55] La reconnaissance du statut de promoteur n'est pas anodine dans la mesure où elle a une incidence directe sur la responsabilité. Celui qui initie un projet de recherche sur des personnes répond en effet des dommages que ces personnes subissent en relation avec le projet (art. 19 al. 1 LRH). Le promoteur peut déposer un projet de recherche à la place de la direction de la recherche ou de l'investigateur ; il reprend alors en lieu et place de ces derniers les obligations correspondantes dans le cadre de la procédure d'autorisation de la recherche (art. 14 al. 2 ORH *cum* art. 17 à 23 ORH ; art. 24 al. 3 OClin *cum* art. 28 et 29 OClin). Le promoteur assume au demeurant toute une série d'obligations qui lui sont propres, découlant du cadre réglementaire applicable. Dans le cadre d'essais cliniques, il est notamment responsable du choix de l'investigateur et du centre de recherche[72]. Il doit de surcroît mettre en place un système de gestion qualité et de contrôle, notamment afin de s'assurer que l'essai est réalisé (et les données collectées et traitées) conformément au protocole de recherche et à la réglementation applicable, et de s'assurer contractuellement qu'il dispose des droits d'accès nécessaires pour le monitoring de l'essai clinique[73]. Il est également primairement responsable de la mise en place des mesures de sécurité des données collectées dans le cadre de l'essai.

[56] En l'absence de promoteur distinct pour un projet, c'est la direction du projet/l'investigateur qui assumera le rôle de promoteur (art. 2 let. e OClin *in fine*). Les fonctions de promoteur et de

69 CIH, Bonnes Pratiques Cliniques (nbp 38), qui en général assigne la responsabilité de la conformité à l'investigateur et/ou au centre de recherche.

70 Voir par exemple le modèle de *Clinical Trial Agreement* de Swissethics (disponible sous https://swissethics.ch/fr/templates/vertraege) ; Michael Isler, Die Rollenverteilung in Klinischen Versuchen, digma 2020, p. 68 (cité : Isler, Rollenverteilung in Klinischen Versuchen).

71 Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 68.

72 CIH, Bonnes Pratiques Cliniques (nbp 38), N 5.6.1.

73 CIH, Bonnes Pratiques Cliniques (nbp 38), N 5.1.

direction du projet/investigateur peuvent donc être unies en une seule et même personne (pour rappel, la direction du projet ou l'investigateur est nécessairement une personne physique), qui assume alors l'ensemble des obligations imposées par la loi à ces deux fonctions. Toutefois, la réalisation d'un projet de recherche est fréquemment déléguée. Les entreprises pharmaceutiques ou autres promoteurs de la recherche procèdent souvent ainsi pour mener à bien des essais cliniques, par exemple. Le partenaire peut être une institution publique de recherche (ex. : hôpital universitaire) ou une organisation de recherche privée (agissant alors comme centre de recherche) ou encore un médecin privé (agissant alors comme direction du projet/investigateur)[74]. Les liens entre le promoteur (ex. : entreprise pharmaceutique) et l'entité ou le chercheur qui va mener la recherche sont alors réglés par un contrat qui prend généralement la forme d'un *Clinical Study Agreement*[75].

[57] Le promoteur d'une recherche peut être amené à traiter des données personnelles relatives aux participants à une recherche. C'est évidemment le cas lorsqu'une seule et même personne assume le double rôle d'investigateur/direction de la recherche et promoteur. Mais la loi impose également au promoteur au sens étroit de conserver certaines données. Dans le cadre d'essais cliniques par exemple, le promoteur est notamment tenu de conserver toutes les données relatives à l'essai clinique jusqu'à la date de péremption du dernier lot livré du médicament testé ou du dernier dispositif médical fabriqué, mais au moins pendant dix ans à compter de la fin ou de l'arrêt de l'essai clinique. Le délai est de quinze ans au moins pour les dispositifs médicaux (art. 45 al. 1 OClin).

v. Sociétés de recherche contractuelle (CRO)

[58] Les **CRO**, pour *Contract Research Organizations* (sociétés de recherche contractuelles ; *Auftragsforschungsinstitut*) sont des personnes morales ou physiques qui se chargent contractuellement pour le compte du promoteur de réaliser certaines tâches liées à des essais cliniques[76]. Le rôle du CRO n'est pas directement défini dans la loi. Il est toutefois décrit dans les bonnes pratiques cliniques du CIH, qui prévoient que le promoteur peut déléguer au CRO tout ou partie des tâches qui lui incombent légalement, mais que le promoteur demeure toutefois responsable de la qualité et de l'intégrité de l'essai clinique[77]. Sous cette réserve, c'est le contenu du contrat qui définit les obligations assumées par le CRO. Les tâches déléguées au CRO peuvent notamment inclure la préparation du protocole de recherche et des demandes d'autorisation, le recrutement de centres de recherche et de participants à la recherche, ainsi que le *monitoring* de la recherche[78].

vi. Fournisseur d'infrastructure

[59] Aujourd'hui, la recherche biomédicale implique le traitement d'un nombre de données (personnelles ou non) toujours plus important. Il en va notamment ainsi pour les recherches qui recourent aux technologies liées au *big data*. Le traitement de ces données personnelles implique

74 Grünig (nbp 61), N 138 ss.

75 Cf. par exemple le modèle de Swissethics (nbp 70).

76 CIH, Bonnes Pratiques Cliniques (nbp 38), N 1.20. Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 68.

77 CIH, Bonnes Pratiques Cliniques (nbp 38), N 5.2.1.

78 Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 68.

non seulement des capacités de stockage plus importantes, mais aussi une augmentation sensible de la puissance de calcul nécessaire. Les données personnelles liées à la santé qui sont traitées dans le cadre d'un projet de recherche doivent de plus être conservées par le biais de mesures opérationnelles et appropriées (art. 5 al. 1 ORH ; art. 18 al.1 OClin). Dans les faits, ces exigences ne font que rappeler les grands principes prônés par les réglementations sur le droit de la protection des données, à l'exemple de l'art. 7 LPD (sécurité des données). Les acteurs de la recherche sont ainsi soumis à un devoir permanent de mettre à jour les mesures de protection des données qu'ils traitent afin d'assurer un niveau de protection adapté à la sensibilité des données traitées. Aux différents éléments précités s'ajoute encore le développement progressif des projets de recherche collaboratifs ou multicentriques qui impliquent une mise à disposition à distance des données de recherche, en général par le biais d'un service *cloud*.

[60] Les exigences en matière d'espace de stockage, de puissance de calcul, de sécurité des données et de disponibilité des données conduisent aujourd'hui les chercheurs à se tourner vers des prestataires externes susceptibles de fournir une infrastructure offrant toutes ces caractéristiques lorsque l'institution à laquelle ils sont rattachés ne possède pas une telle infrastructure à l'interne (pour des questions de coûts et/ou d'opportunité)[79].

[61] Le réseau *BioMedIT* est un exemple d'infrastructure développée pour répondre aux besoins de la recherche biomédicale sur des données en Suisse[80]. Lancé en 2017, ce projet s'intègre dans le programme de l'initiative nationale *Swiss Personalized Health Network* (SPHN), financée par la Confédération. Le projet *BioMedIT* fonctionne selon un modèle décentralisé qui met en réseau plusieurs nœuds informatiques régionaux, chaque nœud offrant une infrastructure de calcul et de stockage sécurisée pour le traitement de données de recherche sensibles. Les différents nœuds sont connectés entre eux et chaque institution de recherche participante est elle-même connectée à un nœud, de telle manière à assurer des transferts de données sécurisés. Les données de recherche pour un projet particulier sont dirigées vers un nœud « principal » (*main node*) désigné en fonction de chaque projet de recherche. Le projet bénéficie ensuite d'un espace virtuel spécifique sur le nœud principal pour l'hébergement des données de recherche ainsi que d'une puissance de calcul attribuée selon les besoins. Les données de recherche peuvent ainsi être « traitées » en vue de la recherche directement dans l'espace dédié, sans qu'elles ne sortent de cet espace.

vii. Commission d'éthique

[62] La réalisation d'un projet de recherche ainsi que la réutilisation de données personnelles ou de matériel à des fins de recherche en l'absence de consentement des personnes concernées doivent faire l'objet d'une autorisation de la commission d'éthique compétente (art. 45 al. 1 LRH).

[63] Dans le cadre de la procédure d'autorisation, le promoteur ou la direction du projet/investigateur ne communiquent en principe pas à la commission d'éthique compétente des données personnelles relatives aux participants à la recherche. De telles communications ne sont toutefois pas exclues une fois que le projet de recherche a été initié. Dans le cadre des essais cliniques,

79 Le recours à des tiers, ou à des structures gérées par plusieurs acteurs, permet une mutualisation des coûts.

80 Pour plus de détails sur le projet *BioMedIT*, voir Diana Coman Schmid et al., SPHN – The BioMedIT Network : A Secure IT Platform for Research with Sensitive Human Data, in : Pape-Haugaard et al. (édit.), Digital Personalized Health and Medicine, Amsterdam/Berlin/Wahsington D.C. 2020, pp. 1170 ss. Voir également les informations continues sur le site web de l'initiative SPHN : https://sphn.ch/network/projects/biomedit.

l'investigateur doit par exemple annoncer à la commission d'éthique compétente certains effets indésirables graves (cf. art. 40 à 42 OClin). Selon les modèles fournis par Swissethics, l'annonce implique alors au moins la communication du code assigné au participant à la recherche ainsi que son année de naissance et son genre.

[64] De surcroît, au cours d'un projet de recherche, la commission d'éthique compétente peut exiger du titulaire de l'autorisation qu'il lui remette tous renseignements et documents utiles (art. 48 al. 2 LRH). Au nombre des titulaires d'une autorisation figurent la direction du projet ou l'investigateur, voire possiblement le promoteur de la recherche lorsqu'il dépose la demande en lieu et place de ces derniers (art. 24 al. 3 OClin ; art. 14 al. 3 ORH)[81]. Les informations exigées par la commission d'éthique en vertu de l'art. 48 al. 2 LRH pourraient contenir des données personnelles en lien avec les participants à la recherche.

[65] Dans la mesure où les commissions d'éthique revêtent la qualité d'autorité, les traitements de données personnelles qu'elles effectuent doivent en principe reposer sur une base légale. Les bases légales en question figurent aux art. 58 ss LRH, qui autorisent les commissions d'éthique à traiter des données personnelles, potentiellement sensibles, ainsi qu'à communiquer des données personnelles à certaines autorités ou à des tiers sous certaines conditions.

viii. Autres acteurs

[66] En parallèle des commissions d'éthique de la recherche, d'autres autorités peuvent être amenées à intervenir dans le contexte d'une recherche, en fonction du type de recherche menée. Ainsi, les essais cliniques de produits thérapeutiques doivent en principe également être autorisés par l'Institut suisse des produits thérapeutiques (Swissmedic), conformément à l'art. 54 de la loi sur les produits thérapeutiques (LPTh) et aux art. 30ss OClin. Dans ce contexte, Swissmedic se voit par ailleurs confier une mission de surveillance qui lui permet de procéder à tout moment à des inspections pour contrôler le déroulement des essais cliniques en question (art. 54*b* LPTh). De telles inspections peuvent conduire Swissmedic à prendre connaissance de données personnelles en lien avec les participants d'une recherche. Les essais cliniques ayant pour objet des transplantations d'organes, de tissus ou de cellules d'origine humaine doivent quant à eux en principe obtenir l'autorisation de l'OFSP (art. 36 loi sur la transplantation)[82]. L'OFSP bénéfice également de la compétence de contrôler l'exécution d'un tel essai clinique en tout temps (art. 36 al. 2 loi sur la transplantation).

[67] Les bailleurs de fonds (ex. : Fonds national suisse de la recherche, FNS) ne deviennent pas promoteurs d'une recherche du seul fait qu'ils octroient les fonds qui financeront une recherche[83]. Contrairement à ce que prévoit la définition légale du « promoteur » qui expose que le promoteur assume entre autres la responsabilité du financement d'une recherche[84], le bailleur de fonds n'est pas à proprement parler « responsable » du financement. Il intervient en principe seulement sur requête du promoteur, même si l'octroi des fonds est soumis à des condi-

81 SHK HFG-Jenni (nbp 22), art. 48 N 38.

82 L'autorisation de l'OFSP n'est toutefois pas nécessaire pour les essais cliniques de la catégorie A (art. 52 OClin).

83 Par exemple, le FNS considère, à notre avis à juste titre, qu'il ne répond pas à la définition de promoteur lorsqu'il contribue au financement d'un essai clinique. Voir par exemple le document FNS, Mise au concours 2021 des « *Investigator Initiated Clinical Trials (IICT)* », p. 6, consultable à l'adresse suivante : https://www.fedlex.admin.ch/eli/cc/2013/643/fr. *Contra* Barbey (nbp 24), p. 21.

84 Art. 3 ORH ; art. 2 let. d OClin.

tions contraignantes. Les bailleurs de fonds peuvent cependant avoir une incidence sur la gestion des données traitées dans le cadre d'une recherche sur l'être humain qu'ils financent. À titre d'exemple, les chercheurs bénéficiaires de subsides du FNS doivent en principe mettre à disposition d'autres chercheurs les données recueillies durant les travaux de recherche et déposer ces dernières dans des bases de données scientifiques reconnues, conformément aux principes prônés par l'*open research data*[85]. Le FNS peut néanmoins dispenser les chercheurs de cette obligation, notamment en présence d'une obligation de garder le secret reposant sur des clauses juridiques, éthiques, de confidentialité ou concernant les droits d'auteur[86].

[68] Les essais cliniques impliquent un travail considérable, notamment lors de la phase III où l'efficacité et la plus-value d'une nouvelle substance peuvent être étudiées sur des groupes comprenant plusieurs milliers de patients. Lors de la phase IV, des études sont par ailleurs menées à long terme sur un produit thérapeutique après sa mise sur le marché, en « conditions réelles », pour évaluer de manière approfondie d'éventuels effets secondaires rares ou tardifs, les interactions avec d'autres médicaments ou plus généralement les bénéfices et risques sur de grands groupes de patients (*postmarketing clinical trials*). De telles études peuvent aussi parfois conduire à la découverte de nouvelles indications possibles pour un médicament[87]. Pour assumer au mieux la gestion des nombreuses données recueillies au cours de ces différentes phases, le promoteur de la recherche recourt parfois à des entreprises privées. Ces dernières proposent différents services en lien avec la réalisation des essais cliniques, à l'image de services de pharmacovigilance. Dans ce cas, l'entreprise privée collecte directement des données liées aux participants à la recherche pour le compte du promoteur.

[69] Enfin, dans le cadre d'une recherche biomédicale, il est possible que les chercheurs communiquent un certain nombre de données à des registres externes ou des dépôts de données. En présence d'un essai clinique, le promoteur a même l'obligation d'enregistrer son essai clinique dans des registres internationaux[88] en y listant un set d'informations minimales avec l'essai (art. 64 ss *cum* annexe 5 ch. 1 OClin) ainsi que dans la banque de données complémentaire de la Confédération (art. 64 al. 2 OClin)[89]. L'enregistrement imposé par la loi pour les essais cliniques vise non seulement à informer le public sur l'état des recherches qui sont menées, mais aussi à permettre aux autres chercheurs de s'informer sur la réalisation d'autres projets et d'éviter des doublons en impliquant de manière inutile des participants à la recherche.

[70] Les chercheurs peuvent aussi être amenés à partager différents types de données avec des registres ou dépôts de données établis afin de favoriser le partage des connaissances et d'accélérer l'état de la recherche. À titre d'exemple, l'initiative GISAID[90] a permis d'établir une base de

85 Art. 47 al. 1 Règlement des subsides du FNS du 27 février 2015. Sur cette question, voir aussi plus généralement le *Concordat on Open Research Data* du 28 juillet 2016.

86 Art. 47 al. 3 Règlement des subsides du FNS du 27 février 2015 ; FNS, § 2.1 Data Management Plan (DMP) – Directives pour les chercheuses et chercheurs, consultable à l'adresse suivante : http ://www.snf.ch/fr/leFNS/points-de-vue-politique-de-recherche/open_research_data/Pages/data-management-plan-dmp-directives-pour-les-chercheuses-et-chercheurs.aspx.

87 CIH, bonnes pratiques cliniques (nbd 38), N 3.1.3.4–5. Pour plus de détails sur les études menées en phase IV, voir par exemple : Viraj Suvarna, Phase IV of Drug Development, Perspectives in Clinical Research, 2010 1(2), p. 57, consultable ici : https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3148611/.

88 Ex. : International Clinical Trials Registry Platform (ICTRP) opérée par l'OMS.

89 Cette banque de données est tenue par la Koordinationsstelle Forschung am Menschen (kofam), gérée par l'OFSP, et est accessible à l'adresse suivante : https://www.kofam.ch/fr/portail-snctp/rechercher-des-essais-cliniques.

90 https://www.gisaid.org/.

données internationale en lien avec la grippe et/ou le COVID-19 qui comprend des séquences génétiques ainsi que des données cliniques et épidémiologiques associées aux virus.

[71] En principe, les communications de données aux registres ou autres dépôts de données du type de ceux mentionnés ci-dessus n'ont pas pour objet des données personnelles et sortent donc du champ des dispositions relatives à la protection des données personnelles. Il faut cependant évidemment veiller à limiter l'étendue des données communiquées de telle manière à éviter la réidentification des participants à la recherche.

b. Rôles, fonctions et responsabilités en matière de protection des données

i. Introduction

[72] Il ressort des explications ci-avant qu'un projet de recherche peut impliquer de nombreux acteurs, appelés à s'échanger et traiter des données qualifiées de données personnelles afin de mener à bien le projet. En droit de la protection des données, les acteurs liés aux traitements de données personnelles sont classifiés selon les catégories suivantes :

- la personne concernée (*data subject*) ;
- le responsable du traitement (*data controller*), respectivement maître du fichier ;
- les responsables du traitement conjoints (*joint controllers*) ; et
- le sous-traitant (*data processor*).

[73] Cette classification n'a pas simplement un rôle académique – ou taxinomique. Le droit de la protection des données impose des droits et obligations différents à chacun des acteurs, en fonction de la catégorie qui lui est assignée. D'apparence simple, cette classification n'est pas toujours aisée. Comme nous le verrons ci-après, un même acteur peut, pour le même set de données, assumer des rôles différents en fonction des finalités pour lesquelles il les traite.

ii. Personne concernée/participants à la recherche

[74] La personne concernée (*data subject*) est la personne physique[91] identifiée ou identifiable dont des données personnelles sont traitées. En lien avec le sujet de cet article, il s'agit des participants à la recherche[92] dont les données personnelles sont traitées dans le cadre de la recherche.

[75] En cette qualité, les participants à la recherche bénéficient d'une série de droits que leur reconnait non seulement la LRH et ses ordonnances, mais aussi plus largement les législations en matière de protection des données personnelles (LPD, lois cantonales sur la protection des données, RGPD, etc.). Les participants à la recherche doivent en règle générale recevoir une information suffisante préalablement à tout traitement (art. 16 al. 2 LRH ; 8 et 28–32 ORH ; art. 7 OClin), puis concernant le résultat de la recherche (art. 8 LRH) et peuvent faire valoir des droits

91 La LPD actuelle englobe également dans son champ les données personnelles des entreprises (voir art. 3 let. b LPD), particularité suisse qui sera supprimée avec l'entrée en vigueur de la nLPD. Cet article se focalise sur les données personnelles des personnes physiques.

92 Sur cette notion *supra* section 3.a.i.

se rapportant au traitement de leurs données personnelles, notamment d'y accéder, d'exiger leur suppression sous certaines conditions, ainsi que de retirer leur consentement (ou de s'opposer au traitement), à tout moment et sans devoir motiver leur demande (art. 7 al. 2 LRH et 8 al. 1 let c ORH).

iii. Responsable(s) du traitement/maître du fichier

[76] Le responsable du traitement (*data controller*) est la personne (physique, morale, ou l'autorité publique), qui, **seule ou conjointement avec d'autres**, **détermine les finalités et les modalités du traitement**de données personnelles[93].

[77] Pour mémoire, la LPD actuelle ne connaît pas la notion de *responsable du traitement*, mais celle de *maître du fichier*. Bien que les notions soient très proches, la notion de maître du fichier se rapporte à la capacité de décider des finalités d'un objet statique (le « fichier », soit un ensemble de données structuré, p. ex. une base de données de patients)[94], alors que le RGPD, et à l'avenir la nLPD, traitent cet aspect de manière dynamique pour chaque activité de traitement (ex. : l'utilisation de cette base de données dans le cadre de soins ou à des fins de recherche), pour l'ensemble du cycle de vie de la donnée (de la collecte à l'effacement). Cet alignement du droit suisse sur le droit européen doit à notre avis être salué, puisqu'il permet de décrire de manière plus nuancée – et appropriée – les rôles effectivement assumés par les intervenants, comme cela sera exposé ci-après[95].

[78] La capacité de déterminer les finalités du traitement – le « pourquoi » du traitement – est l'élément décisif de la notion[96]. La notion de « finalité du traitement » inclut le but de la recherche, mais également les spécificités et le nombre de participants à la recherche, le type de données devant être collectées, les types de traitements devant être effectués sur celles-ci, etc. La capacité de déterminer ces finalités peut premièrement découler de la loi ou d'un contrat. Dans le cadre d'un projet de recherche, les finalités du traitement sont en principe décrites de manière détaillée dans le plan de recherche (art. 15 let. c ORH) ou le protocole de recherche (art. 25 let. d OClin). Il est au demeurant courant de décrire plus spécifiquement les règles relatives à la gestion des données dans un document séparé nommé *data management plan*[97]. La participation à la rédaction de ces documents sera donc un indice souvent déterminant pour la qualification des intervenants en tant que responsable du traitement ou non[98]. La capacité de déterminer les fina-

93 Art. 4 par. 7 RGPD et 5 let. j nLPD.

94 Cf. art. 3 let. g LPD. Le maître du fichier est donc celui qui dispose du pouvoir général de fixer les principes essentiels relatifs à un fichier donné, notamment son « paramétrage ». Voir David Rosenthal, Handkommentar zum Datenschutzgesetz, Schulthess 2008, N 106 ad art. 3 (cité : Handkommentar DSG).

95 Cette modification n'est donc pas que terminologique et a un impact plus important que ce qui est indiqué dans le message du Conseil fédéral concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (FF 2017 6565), p. 6643 (cité : Message nLPD). Pour le surplus, cf. Groupe de travail « article 29 » sur la protection des données, Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant », 16 février 2010, pp. 3–4, qui précise que « *Même si le résultat aurait sans doute été le même dans de nombreux cas, la notion a de ce fait acquis un sens et une portée bien plus larges et plus dynamiques* ».

96 Meier, Protection des données (nbp 42), N 583 p. 247 ; David Rosenthal, Controller oder Processor : Die datenschutzrechtiliche Gretchenfrage, in : Jusletter 17 juin 2019, p. 9 (cité : Rosenthal, Controller oder Processor).

97 Un tel document est notamment requis pour les projets financés par le Fonds national suisse de la recherche scientifique. Voir p. ex. le modèle fourni par les HUG disponible sous https://crc.hug.ch/data-management/procedures-et-manuels-pour-investigateurs.

98 Voir l'exemple n° 3 ci-après à la section 5.c.

lités du traitement peut toutefois également découler d'une influence de fait ; la responsabilité pour un traitement de données résulte dans ce cas essentiellement du fait qu'une entité a choisi de traiter des données personnelles pour des finalités qui lui sont propres[99].

[79] Dans le cadre d'opérations effectuées par une personne morale (publique ou privée) c'est en principe la personne morale directement qui agit en tant que responsable du traitement et non ses employés, dirigeant ou personnel externe intégré dans l'organisation de manière analogue à la position d'un employé[100]. Les activités du personnel pour le compte de l'organisation entrent en effet dans leur cahier des charges, le personnel agissant pour le compte et sous le contrôle et la responsabilité de l'organisation[101]. Ainsi, lorsqu'une recherche est menée par un chercheur (la direction du projet ou l'investigateur) agissant dans le cadre de ses activités pour son employeur (un hôpital universitaire ou autre centre de recherche), c'est l'hôpital, et non le chercheur, qui assume le rôle de responsable du traitement. Il faut néanmoins réserver le cas de l'employé qui traite des données pour un motif qui s'écarte de ce qui est requis pour l'exercice de ses fonctions (p. ex. en consultant une base de données de son entreprise à des fins privées), lequel agit dans ce cadre en tant que responsable du traitement indépendant[102].

[80] Le responsable du traitement n'a pas forcément accès aux données personnelles. Le responsable peut par exemple instruire un tiers de collecter et traiter les données à sa place, sans y avoir accès lui-même[103]. Il est également possible que deux entités soient considérées comme responsables conjoints du traitement, alors qu'une seule a accès aux données, comme exposé ci-après.

iv. Responsables conjoints du traitement (joint-controllers)

[81] La responsabilité de déterminer les finalités et les modalités du traitement peut être assumée conjointement par deux ou plusieurs parties distinctes (désignées « **responsables conjoints du traitement** » ou « **co-responsables du traitement** » (*joint controllers*))[104]. La participation de ces

---

99 Pour la LPD actuelle, cf. Meier, Protection des données (nbp 42), N 591 p. 249 « *à partir du moment où le mandant intègre les données recueillies par un tiers (par ex. le rapport de surveillance du détective privé mandaté par une assurance) dans un fichier qui lui est propre, il devient à son tour maître de fichier. On peut alors très bien avoir deux fichiers distincts, avec deux maîtres de fichiers différents, chacun étant tenu pour son compte des devoirs liés à cette qualité* » ; selon le RGPD, voir l'art. 28 par. 10 RGPD, qui précise que le sous-traitant qui, en violation du RGPD, détermine les finalités et les moyens du traitement, « (…) *est considéré comme un responsable du traitement* ***pour ce qui concerne ce traitement*** » ; Rosenthal, Controller oder Processor (nbp 96), p. 9.

100 Apparemment du même avis : Rosenthal, Controller oder Processor (nbp 96), p. 43 ; Sylvain Métille, Le traitement de données personnelles sous l'angle de la (nouvelle) loi fédérale sur la protection des données du 25 septembre 2020, SJ 2021 II p.1ss, p. 19. Pour le droit européen, cf. article 29 RGPD et Comité européen de la protection des données, Lignes directrices 07/2020 sur les concepts de responsable du traitement et de sous-traitant selon le RGPD, version 2.0, 7 juillet 2021, N 17 (cité : CEDP, Lignes Directrices responsable du traitement/sous-traitant).

101 En droit suisse, conformément à l'art. 55 al. 2 CC et l'art. 55 al. 1 CO. Rosenthal, Handkommentar DSG (nbp 94), N 109 ad art. 3.

102 En vertu d'une responsabilité « de fait », comme évoqué ci-avant. Pour le droit européen, voir CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), N 88.

103 CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), N 45 ; Rosenthal, Controller oder Processor (nbp 96), p. 17 ; Rosenthal, Schulthess Handkommentar DSG (nbp 94) N 107 ad art. 3 ; Beat Rudin, in : Bruno Baeriswyl/Kurt Pärli (édit.), Handkommentar Datenschutzgesetz, Stämpfli Bern 2015, N 50 ad. art. 3 (cité : Rudin (DSG)) ; Meier, Protection des données (nbp 42), N 589 p. 248.

104 Article 5 let. j et 33 nLPD ; art. 26 RGPD. En droit actuel, art. 1 al. 5 de l'ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11) ; cette disposition est reprise à l'art. 21 du projet de révision total de l'OLPD du 23 juin 2021 (nbp 7).

parties à la détermination conjointe peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale.

[82] Dans les faits, les responsables conjoints peuvent entretenir une relation très proche (partager l'ensemble des finalités et des moyens d'une opération de traitement) ou plus distante (en partageant uniquement une partie des finalités et/ou des moyens)[105]. L'analyse doit être effectuée pour chaque activité de traitement : deux acteurs peuvent être responsables conjoints du traitement pour certaines activités et agir en tant que responsables indépendants pour d'autres. Il n'est pas nécessaire que chacun des deux acteurs ait accès aux données personnelles (qu'elles soient codées ou non)[106]. Ainsi, le fait qu'un promoteur ne reçoive aucune donnée personnelle, ou ne les reçoive que sous une forme codée (anonymisée de son point de vue au sens de l'art 26 al. 1 ORH), ne joue aucun rôle sur sa responsabilité en matière de protection des données. Il en va de même si plusieurs centres de recherche décident ensemble de procéder à une recherche et qu'ils participent conjointement à la détermination des finalités du traitement des données personnelles dans ce cadre, même si certains centres de recherche n'ont accès à aucune donnée personnelle.

v. Sous-traitant (subprocessor)

[83] Par opposition à la notion de responsable du traitement, le sous-traitant des données (*data processor*) est celui qui traite des données personnelles *pour le compte du responsable du traitement* (respectivement du maître du fichier)[107], c'est-à-dire sans être lui-même un responsable du traitement. Cette position présuppose donc la réalisation de trois conditions[108] :

i. Être une entité juridique distincte du responsable du traitement : tel ne sera par exemple pas le cas de l'employé (notamment du chercheur) qui traite les données dans le cadre de ses activités professionnelles pour le compte d'un centre de recherche[109], ni le département d'une entreprise/institution qui traite des données pour le compte d'un autre département. Dans ces deux cas, il n'y a pas de sous-traitance (*sub-processing*), les traitements étant réputés être effectués directement pour la personne morale[110].

105 Pour des développements sur ce sujet en droit européen, voir notamment Comité européen de la protection des données, Guidelines 8/2020 on the targeting of social media users, version 2, 13 avril 2020, N 34.

106 Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 70 ; voir également les arrêts de la Cour de justice de l'Union européenne « Wirtschaftsakademie » (C-201/16, ECLI :EU :C :2018 :388, paragraphe 38) et « Fashion ID » (C-40/17 du 29 septembre 2019 ; résumé par Célian Hirsch, Fashion ID, Facebook, le bouton « j'aime » et la notion de coresponsable du traitement, in : www.lawinside.ch/805/). Dans ce second arrêt, la CJUE a considéré que l'exploitant d'un site web qui place un plug-in de Facebook (le bouton « j'aime ») sur son site web, agit comme responsable conjoint du traitement avec Facebook concernant la collecte des données des visiteurs du site web effectuées par Facebook au moyen de ce plug-in, alors même que l'exploitant du site web n'a accès à aucune donnée personnelle. La co-responsabilité est toutefois limitée « *à l'opération ou à l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens, à savoir la collecte et la communication par transmission des données en cause* ». CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), N 45.

107 Art. 5 let. k nLPD et art. 4 par. 7 RGPD.

108 CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), Nos 76 ss. Cette position est à notre avis entièrement transposable en droit suisse.

109 Comme exposé *supra* section 3.b.iii, le chercheur n'intervient en principe pas non plus comme responsable de traitement, mais agit pour le compte de son organisation, qui elle assume le rôle de responsable du traitement.

110 Meier, Protection des données (nbp 42), N 592 p. 249 ; CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), Nos 18–19 et 77–78.

ii. Traiter des données personnelles : bien que la terminologie française soit quelque peu malheureuse, la sous-traitance n'implique pas (nécessairement) la délégation d'un service (*sub-contracting*) mais la réalisation d'une activité de traitement ([*sub-*]*processing*)[111], laquelle nécessite un accès aux données personnelles[112]. Cette activité peut couvrir tout le spectre des activités de traitement envisageables[113]. C'est donc bien la sous-traitance d'une activité de traitement, et non pas d'un service, qui constitue l'élément déterminant. À titre d'exemple : si un CRO[114] est engagé par un promoteur uniquement pour l'assister dans le cadre du dépôt de la demande d'autorisation auprès de la commission d'éthique, ou pour fournir d'autres services qui n'impliquent pas l'accès à des données personnelles liées à la recherche, le CRO n'agit pas (en matière de protection des données) comme sous-traitant[115]. Par opposition, une entreprise qui fournit des prestations de maintenance informatique pour un hôpital impliqué dans un projet de recherche sera en principe considérée comme un sous-traitant (*sub-processor*) si elle peut accéder aux données de recherche (aussi sous forme codée) dans le cadre de ses opérations, même si ses prestations ne se rapportent pas directement au projet de recherche en question.

iii. Agir pour le compte du responsable du traitement : le sous-traitant doit encore effectuer l'activité de traitement pour le compte – c'est-à-dire selon les instructions – du responsable du traitement (ce qui implique qu'il ne détermine pas lui-même les finalités du traitement, mais contribue à la réalisation de ces finalités pour le responsable du traitement). La qualité de sous-traitant ne découle ni du libellé du contrat ni de la nature de l'entité traitant des données, mais de son degré d'indépendance concret. Plusieurs critères peuvent être pris en compte dans ce cadre, notamment : (i) la marge de manœuvrede l'entité (qui dépend du nombre et de la précision des instructions préalables données par le responsable du traitement) ; (ii) le contrôle/la surveillance exercés par le responsable du traitement ; (iii) la visibilité/l'apparence données aux personnes concernées, et les attentes que cette visibilité suscite chez elles ; (iv) l'expertise des parties(le rôle et l'expertise professionnelle du prestataire de services jouent un rôle prépondérant, pouvant entraîner sa qualification

111 La terminologie anglaise permet plus aisément de distinguer le *subcontractror* (sous-traitant d'un service) du *sub-processor* (sous-traitant d'une activité de traitement).

112 Rosenthal, Controller oder Processor (nbp 96), p. 40–43. Cet auteur estime au demeurant qu'il n'y a pas d'accès aux données personnelles, et donc pas de sous-traitance, si le récipiendaire (i) n'a accès qu'à des données chiffrées/pseudonymisées, ou (ii) a certes accès aux données personnelles « en clair », mais que le traitement de ces données ne fait pas partie des prestations du récipiendaire (même s'il en prend connaissance). Ces deux positions ne peuvent à notre pas être suivies. Concernant le premier cas de figure, les données codées demeurent des données personnelles (dans le contexte de la recherche en tout cas ; cf. *supra* section 2.d.ii). Au demeurant, l'auteur reconnait que les personnes concernées continuent de pouvoir exercer leurs droits relatifs à ces données (p. ex. le droit d'accès ou d'effacement), ce qui implique qu'il s'agisse encore de données personnelles (ils ne pourraient pas le faire si les données étaient anonymisées, et donc hors champ de la LPD). S'agissant du second cas de figure, il faut à notre avis déterminer s'il est envisagé que le récipiendaire effectue un traitement de données personnelles au sens des art. 3 let. e LPD/ 5 let. d nLPD, ce qui inclut notamment l'enregistrement ou l'effacement des données. Le fait que ces activités ne constituent pas l'objet (principal) de la prestation fournie, mais simplement une conséquence de sa fourniture, n'est à notre avis pas déterminant. En droit européen, la consultation des données est au demeurant expressément mentionnée à l'art. 4 par. 2 RGPD comme une forme de traitement.

113 Meier, Protection des données (nbp 42), N 1196 p. 421. Ceci inclut notamment la collecte, l'enregistrement, la conservation, l'utilisation la modification, la communication l'archivage, l'effacement ou la destruction (cf. art. 5 let. d nLPD).

114 Sur la notion, cf. *supra* section 3.a.v.

115 Même si le contrat entre le promoteur et le centre investigateur prévoit que cette tâche incombe au promoteur, qui est donc contractuellement sous-traitée au CRO (*sub-contracting*), sans constituer une délégation du traitement (*sub-processing*).

de responsable du traitement) ; et (v) les moyens mis en place pour parvenir aux finalités escomptées[116].

[84] Dans la mesure où la détermination des finalités est une tâche réservée uniquement à un responsable du traitement, toute personne qui prend cette décision devient donc un responsable du traitement (de fait)[117]. Ainsi, celui qui d'ordinaire traite des données en tant que sous-traitant (*sub-processor*), mais décide d'utiliser ces données également pour une finalité qui lui est propre, devient de ce fait responsable du traitement pour ce traitement spécifique (car il n'agit plus dans ce cadre pour le compte du responsable du traitement principal).

[85] Par opposition, les moyens techniques et d'organisation du traitement (les modalités) peuvent être déterminés (quasi-)exclusivement par le sous-traitant, à la condition toutefois que les questions sensibles qui sont fondamentales pour la licéité du traitement soient réservées au responsable du traitement[118]. Le sous-traitant doit aussi se conformer aux instructions du responsable du traitement et aux exigences convenues contractuellement avec ce dernier.

[86] Dans une même relation et pour les mêmes données, **une entité peut agir à la fois en qualité de responsable du traitement pour certaines activités de traitement et en tant que sous-traitante pour d'autres activités**. C'est en réalité dans les faits régulièrement le cas, en particulier quand les mêmes données sont traitées à la fois pour fournir le service demandé (en qualité de sous-traitant) et à la fois pour des finalités propres au prestataire (par exemple pour se conformer à ses propres obligations légales ou pour mener des activités de recherche et développement internes)[119]. La relation avec un fournisseur de services ne peut donc pas être traitée de manière schématique (en considérant que le fournisseur de services agit systématiquement comme sous-traitant), mais doit faire l'objet d'une analyse au cas par cas.

vi. Essai de classification

[87] En dépit du fait qu'il faille renoncer à tout schématisme, certaines règles générales peuvent néanmoins être avancées pour déterminer le rôle assumé par les différentes parties impliquées dans un projet de recherche, dans le but de fournir des informations pratiques au lecture. Ces règles doivent toutefois être nuancées par certains cas particuliers dans le cadre desquels ces règles ne s'appliquent pas, comme exposé dans le tableau suivant :

116 Ces critères sont tirés des Lignes Directrices responsable du traitement/sous-traitant du CEDP (nbp 100).

117 Cf. nbp 99.

118 CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), N 40.

119 Voir par exemple le *Microsoft Online Services Data Processing Agreement* de la société Microsoft, version du 9 décembre 2021 (accessible sous https://www.microsoft.com/en-us/licensing/product-licensing/products qui prévoit d'une part que « *Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except* [as stated otherwise herein.] » et d'autre part que « *To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for Microsoft's legitimate business operations incident to delivery of the Online Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use.* » (p. 7).

	La règle	Les cas particuliers
Direction du projet et investigateur :	• n'intervient ni comme responsable du traitement, ni comme sous-traitant, mais agit comme employé/membre de son employeur[120].	• peut intervenir comme responsable du traitement (voire comme sous-traitant) si elle/il agit de manière indépendante d'un centre de recherche (ex. : médecin indépendant ; ou chercheur qui agit hors du cadre de son mandat par son employeur).
Centre de recherche/ centre investigateur (*medical institution*) :	• agit en principe comme responsable conjoint du traitement avec le promoteur ou les autres centres de recherche pour les activités de traitement liées à la recherche[121] (respectivement comme responsable du traitement indépendant en l'absence de ces autres parties). • agit comme responsable de traitement indépendant pour les activités liées à la fourniture de soins à ses patients.	• agit comme sous-traitant du promoteur s'il ne participe pas à la rédaction du protocole de recherche et se limite à appliquer celui-ci, sauf pour ses opérations dictées par le respect des obligations légales qui lui sont propres (pour lesquelles il demeure responsable du traitement).
Promoteur/ sponsor :	• agit comme responsable conjoint du traitement avec le centre de recherche[122].	• agit comme responsable de traitement indépendant lorsque le centre de recherche est sous-traitant.
CRO (Sociétés de recherche contractuelle) :	• agit comme sous-traitant du promoteur.	• agit comme responsable du traitement pour les traitements dictés par le respect des obligations légales qui lui sont propres.

	La règle	Les cas particuliers
Fournisseur d'infrastructure :	• agit comme sous-traitant du responsable du traitement (ou comme sous-traitant ultérieur d'un autre sous-traitant).	• agit comme responsable du traitement pour les activités qui s'écartent de la fourniture du service, en particulier pour les traitements dictés par le respect des obligations légales qui lui sont propres.
Commission d'éthique et autre autorité :	• ne traite pas de données personnelles et n'agit ni comme responsable du traitement, ni comme sous-traitant.	• agit comme responsable de traitement indépendante lorsqu'elle a accès à des données personnelles.
Bailleur de fonds :	• ne traite pas de données personnelles et n'agit ni comme responsable du traitement, ni comme sous-traitant.	• n/a (si ses activités dépassent la l'octroi de fonds, il pourrait selon les cas être qualifié de promoteur et assumer les responsabilités qui en découlent).
Entreprise de pharmacovigilance fournissant des services en vue de la réalisation d'une recherche :	• agit comme sous-traitant du promoteur pour les données personnelles qu'elle traite.	• agit comme responsable du traitement pour les traitements dictés par le respect des obligations légales qui lui sont propres.

c. Impact des distinctions

[88] Le rôle assumé par une entité (responsable du traitement indépendant ou conjoint, ou sous-traitant) a un impact sur ses droits et obligations en matière de protection des données. De manière générale, le responsable du traitement assume plus d'obligations et une responsabilité plus étendue que le sous-traitant. Le responsable du traitement aura toutefois une marge de manœuvre plus large, le sous-traitant étant limité par les instructions du responsable du traitement. Au demeurant, pour autant que les conditions légales soient réunies, la sous-traitance permet de bénéficier de certains allégements. Ainsi, la mise à disposition de données personnelles à un sous-traitant ne constitue pas (sous l'angle du droit général de la protection des

données[123]) une communication de données personnelles ; elle ne nécessite donc pas un motif justificatif pour pouvoir être effectuée et les personnes concernées ne peuvent pas s'y opposer[124]. L'existence d'une sous-traitance impose toutefois certaines conditions supplémentaires, notamment de s'assurer que le sous-traitant est en mesure de garantir la sécurité des données[125]. Le RGPD impose au demeurant que la relation soit régie par un contrat écrit (également électronique), dont le contenu minimum est défini par le règlement (cf. art. 28 RGPD)[126]. Le tableau ci-après liste les principales différences entre les différents rôles :

	Droits / obligations	Responsable du traitement (RdT)	Responsable conjoint du traitement Co-RdT)	Sous-traitant (ST)
Droit de…	**…décider des finalités et modalités du traitement** ?	Oui	Oui	Uniquement des modalités non essentielles (selon accord avec responsable RdT)
	… **communiquer des données à des sous-traitants/des tiers** ?	Oui[127]	Selon accord avec autre(s) Co-RdT(s)	Uniquement avec l'accord du RdT[128]
	… **communiquer des données à l'étranger** ?	Oui	Selon accord avec autre(s) Co-RdT(s)	Uniquement avec l'accord du RdT

123 Nous réservons ici les règles relatives au secret médical. Sur ce sujet, cf. Frédéric Erard, Le secret médical. Étude des obligations de confidentialité des soignants, thèse, Zurich 2021, p. 509 ss (cité : Erard, Le secret médical).

124 En droit suisse, la communication de données personnelles sensibles est présumée de manière irréfragable constituer une atteinte à la personnalité nécessitant un motif justificatif (loi, consentent ou intérêt prépondérant) pour être licite (art. 12 al. 2 let. c LPD ; art. 30 al. 2 let. c nLD). En droit européen, la communication par transmission est une forme de traitement (art. 4 par. 2 RGPD), qui nécessite en principe un motif justificatif pour être licite (art. 5 par. 1 let. a et 6 par. 1 RGPD). Le sous-traitant n'est toutefois pas considéré comme un tiers (art. 4 (10) RGPD) et la réalisation d'une sous-traitance nécessite la conclusion d'un contrat écrit, mais pas l'existence d'un motif justificatif spécifique (art. 28 RGPD *a contrario*).

125 Art. 10*a* al. 2 LPD ; art. 9 al. 3 nLPN ; art. 28 par. 1 RGPD.

126 La nLPD exige l'existence d'un contrat (art. 9 al. 1 nLPD).

127 Comme exposé en introduction de cette section, une communication à un tiers qui n'est pas un sous-traitant nécessitera en principe l'existence d'un motif justificatif.

128 Pour la controverse selon la LPD actuelle, cf. Meier, Protection des données (nbp 42), N 1223 p. 429.

	Droits / obligations	Responsable du traitement (RdT)	Responsable conjoint du traitement Co-RdT)	Sous-traitant (ST)
Obligation …	… de s'assurer de disposer **d'un motif justificatif au traitement** ?	Oui (en droit suisse : uniquement en présence d'une atteinte à la personnalité)[129]	Oui (individuellement par Co-RdT pour les activités dont il est responsable).	Non
	… **d'informer et répondre aux demandes des personnes concernées** ?	Oui	Selon accord avec autre(s) Co-RdT(s)[130]	Non
	… de **notifier les violations de la sécurité des données** ?	Oui à l'autorité et aux personnes concernées (selon les cas)[131]	Selon accord avec autre(s) Co-RdT(s)[131]	Au RdT[132]
	… de réaliser des analyses d'impact sur la protection des données (**DPIA**)[133]	Oui, selon le cas	Oui, selon le cas	Non (mais obligation d'assistance au RdT selon le RGPD)

129 Selon le RGPD, tout traitement doit reposer sur un motif justificatif pour être licite (art. 5 par. 1 let. a et 6 par. 1 RGPD). Selon l'approche du droit suisse, un motif justificatif n'est nécessaire que si le traitement des données porte atteinte à la personnalité (art. 12 al. 1et 13 al. 1LPD ; art 30 al. 1et 31 al. 1 nLPD). La liste des situations considérées (de manière irréfragable) comme entraînant une atteinte à la personnalité est toutefois exemplative et il faut analyser au cas par cas si l'action trouble la personnalité de la personne concernée par une atteinte à son intégrité informationnelle (Meier, Protection des données (nbp 42), N 1528-1531 p. 511). Il est donc à notre avis erroné de considérer qu'un traitement de données ne porte pas atteinte à la personnalité tant qu'il respecte les principes généraux du traitement (sauf opposition explicite de la personne concernée). Voir notamment l'approche « opt–out » défendue par Rosenthal, qui ne tient à notre sens pas suffisamment compte de la multitude de situations (au-delà d'une violation des principes généraux) dans lesquelles une atteinte à la personnalité peut être réalisée ; cf. David Rosenthal/Samira Studer/Alexandre Lombard (pour la traduction), La nouvelle loi sur la protection des données, in : Jusletter 16 novembre 2020, pp. 17–18 et 20.

130 Selon l'art. 21 du projet de révision complète de l'OLPD (nbp 7), la personne concernée peut exercer ses droits contre chaque responsable du traitement conjoint.

131 En droit suisse, une telle obligation n'existera que sous l'égide de la nLPD.

132 Voir art. 33 par. 2 RGPD et 24 al. 3 nLPD. La LPD actuelle n'impose pas une telle obligation au sous-traitant, qui peut toutefois découler d'une autre disposition légale (notamment l'art. 400 CO concernant l'obligation du mandataire de rendre des comptes) ou du contrat entre les parties.

133 La réalisation d'un DPIA n'est actuellement pas requise par le LPD. Cela sera le cas sous l'égide de la nLPD en cas de risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée (art. 22 nLPD), condition qui sera en principe réalisée en cas de recherche impliquant un traitement à grande échelle de données sensibles.

	Droits / obligations	Responsable du traitement (RdT)	Responsable conjoint du traitement Co-RdT)	Sous-traitant (ST)
Obligation …	… de tenir un registre des activités de traitement[134]	Oui, sauf exception	Oui, sauf exception	Oui, sauf exception
	Responsabilité civile et/ou pénale/ administrative ?[135]	Responsabilité pleine	Responsabilité pleine et étendue à l'entier du dommage (solidarité)	Responsabilité en principe limitée à ses propres obligations[136]

4. Gestion contractuelle

a. Introduction

[89] Les intervenants à un projet de recherche seront appelés à régler leur relation dans un ou plusieurs contrats. Ceux-ci pourront prendre des formes variées, en fonction notamment du degré de collaboration recherché (simple prestation de services ou mise en commun de ressources pour atteindre un but commun) et de leur objet (limité au traitement des données ou couvrant d'une manière plus large la collaboration des parties). Les clauses concernant la protection des données sont de manière habituelle contenues dans deux types d'accords distincts (qui ne sont pas propres aux projets de recherche), en fonction du rôle assumé par les parties :

- d'un côté le **contrat de partage de données**[137] (*data transfer agreement* ou *data sharing agreement*) qui est conclu entre deux ou plusieurs responsables du traitement ;
- de l'autre l'**accord de sous-traitance**[138], qui est conclu entre et un responsable du traitement (ou entre un sous-traitant et un sous-traitant ultérieur).

[90] Dans les situations les plus simples, la signature de ce type d'accords (ou d'un mélange des deux, en fonction des rôles assumés par les parties) est suffisante pour régir la relation entre

134 Pour le droit suisse, uniquement à partir de l'entrée en vigueur de la nLPD. Des exceptions seront prévues à certaines conditions pour les responsables du traitement privés employant moins de 250 collaborateurs.

135 Le droit suisse et le droit européen suivent sur cet aspect des approches matériellement différentes. Ainsi, le RGPD prévoit un régime de sanctions administratives (notamment l'amende) imposées aux entités juridiques fautives (cf. art. 58 et 77 RGPD) alors que le droit suisse prévoit un régime de sanctions pénales imposées en général aux personnes physiques au sein de l'entreprise responsables de la violation. Pour le détail, cf. Rosenthal, Controller oder Processor (nbp 96), pp. 3 et 46–48.

136 En vertu de l'art. 28 al. 1 CC, la personne concernée peut néanmoins agir contre toute personne qui contribue à l'atteinte. Une action en dommages-intérêts nécessite toutefois une faute (art. 41 CO *cum* art. 28a al. 2 CO).

137 Voir p. ex le modèle de *Data Transfer And Use Agreement* (DTUA) du SPHN, accessible sous https://sphn.ch/document/template-dtua-dtpa-multiple-nodes/.

138 Voir p. ex le modèle de *Data Transfer And Processing Agreement* (DTPA) du SPHN, accessible sous https://sphn.ch/document/template-dtua-dtpa-multiple-nodes/.

les parties. Lorsque le contrat a vocation à régir une situation plus complexe, les clauses sur la protection des données devront en principe être intégrées/absorbées dans les accords plus larges typiques des projets de recherche, notamment(de manière non exhaustive) :

- contrat de services (ex. pour la réalisation de certaines analyses), qui peut être désigné « *CRO services agreement* » lorsqu'il implique l'intervention d'un CRO ;
- contrat de recherche (*research agreement*), pour la réalisation d'un projet de recherche ;
- contrat pour la réalisation d'essais cliniques (*clinical study agreement*)[139] ;
- contrat de collaboration (*consortium/partnership agreement*)[140] ;
- contrat de transfert de matériel humain (*materials transfer/biological supply agreement*).

[91] Nous traiterons ci-après de manière générale (sans prétendre à l'exhaustivité) des clauses contractuelles se rapportant à la protection des données, qui peuvent (ou devraient) être insérées d'une manière ou d'une autre dans tous les contrats se rapportant à la recherche, quel que soient leur intitulé.

[92] Ces clauses sur la protection des données doivent prendre en considération la possibilité que le même acteur puisse intervenir dans le cadre du projet de recherche dans des rôles et pour des fonctions distincts[141]. Une partie peut en effet intervenir comme responsable du traitement indépendant pour certaines activités de traitement (ex. : des analyses qui ne concernent que ses chercheurs), comme responsable conjoint du traitement pour d'autres (ex. : des analyses sur lesquelles plusieurs centres de recherche travaillent), ainsi que comme sous-traitant pour d'autres activités (ex. : l'hébergement des données d'un consortium). Sauf dans les cas les plus simples, l'on se gardera en conséquence de mettre en place un cadre trop rigide (notamment en imposant de manière générale des obligations de sous-traitant à une entité dont la responsabilité effective est plus nuancée).

[93] Ces clauses devront également prendre en considération le rôle/la fonction effectivement exercé par chaque acteur, en différenciant par exemple ceux intervenant pour la collecte des données (*data collectors*), leur transmission (*data providers*), réception (*data recipients*), contrôle (*data owners*) ou traitement. Compte tenu de la complexité relative à l'assignation des rôles (*controller/processor*), il peut être plus aisé d'assigner des responsabilités selon la fonction exercée, en imposant contractuellement l'obligation à celui qui est naturellement le plus à même de la satisfaire. Ainsi, celui qui collecte les données (*data collector*) sera plus à même d'assurer les tâches liées à l'information des personnes concernées ; celui qui exerce un contrôle des données (*data owner*), et possède potentiellement une vision plus complète de la manière dont elles sont utilisées, pourra quant à lui mieux répondre aux demandes des personnes concernées.

139 Voir p. ex. le modèle proposé par Swissethics (nbp 70).

140 Voir p. ex. le modèle de *consortium agreement* du SPHN, qui inclut à la fois un DTUA et un DTPA, accessible sous https://sphn.ch/services/dtua/.

141 Cf. *supra* section 3.b.v.

b. Les clauses nécessaires

[94] Les parties doivent avant tout définir le **cadre du traitement**. Dans le cas simple d'une sous-traitance, le cadre correspond à l'exécution des prestations convenues, conformément aux instructions du responsable du traitement. En dehors du cas de sous-traitance, les parties doivent convenir des finalités pour lesquelles les données peuvent être traitées (*agreed purposes*). Il est en particulier important pour l'entité qui transmet des données (le *data provider*) de s'assurer que le cadre du traitement soit circonscrit de manière suffisamment précise. En effet, ce dernier assumera souvent à l'interne – par le biais de garanties (*representations and warranties*) – la responsabilité de la licéité des données transmises, notamment concernant la collecte des consentements requis. Or, celui-ci ne pourra s'assurer de sa conformité à son engagement que s'il sait de manière suffisamment précise comment les données vont être traitées une fois partagées. Le *data provider* sera également (en pratique en tout cas) plus exposé aux actions de personnes concernées qui considéreraient que leurs données n'ont pas été traitées conformément au consentement ou à l'information initialement donnée.

[95] Les parties devront également se **répartir les obligations découlant du droit de la protection des données**, notamment concernant *l'obtention des consentements* (des participants à la recherche) et des autorisations (p. ex. des commissions d'éthique ou de Swissmedic) éventuellement nécessaires, l'exercice des droits des personnes concernées, ou encore la réalisation d'analyses d'impact sur la protection des données[142]. En principe, tous les responsables conjoints d'un traitement sont conjointement responsables de l'exécution de ces obligations. Or, dans les faits, certains acteurs peuvent ne pas être en mesure de le faire (ou uniquement imparfaitement)[143]. Il semble en conséquence opportun, comme évoqué ci-avant que les parties au projet de recherche conviennent d'un partage des responsabilités prenant en compte les fonctions/actions qu'ils exercent. Au demeurant, la responsabilité de donner suite aux demandes des personnes concernées, dans les délais courts prévus par la loi, nécessite souvent la mise en place d'un processus impliquant l'intervention des différents acteurs liés au traitement (par exemple une révocation du consentement, ou une demande de suppression des données). Les données étant le plus souvent codées, il sera potentiellement nécessaire de les décoder afin de pouvoir donner suite aux demandes des personnes concernées, ce qui nécessite une collaboration efficace entre les différents intervenants, y compris par le détenteur de la clé de décodage[144]. Les processus nécessaires doivent ainsi être contractuellement prévus.

[96] Lorsque la mise à disposition/le transfert des données hors de la Suisse ou de l'Union européenne est envisagé, les **règles concernant les transferts internationaux** devraient également faire l'objet d'un accord. Les règles limitant les transferts internationaux de données personnelles sont considérées représenter un obstacle majeur à la recherche en Europe, en particulier du fait que les partenaires publics hors de Suisse ou de l'Union européenne (et notamment aux États-Unis) sont réticents à signer les clauses contractuelles types de la Commission européenne[145]. Il

142 Pour le surplus, cf. tableau à la section 3.c.

143 Par exemple un responsable conjoint du traitement qui, certes, participe à la détermination des finalités du traitement, mais qui n'a aucun accès aux données, sera matériellement dans l'impossibilité de répondre à une demande de droit d'accès d'une personne concernée.

144 Le décodage des données personnelles pour donner suite aux demandes des personnes concernées est expressément autorisé (art. 27 let. c ORH). Sur le codage, voir *supra* section 2.d.ii..

145 Sur le sujet, voir le rapport ALLEA/EASAC/FEAM, International Sharing of Personal Data for Research (nbp 1), notamment pp. 28–32 « *It is important to emphasise that while mechanisms such as SCCs work better for private ins-*

est également usuel de limiter **la manière dont les données peuvent être transférées à des tiers**, que ceux-ci agissent comme sous-traitant ou responsable du traitement indépendant.

[97] Les dispositions concernant la **sécurité des données** – et plus généralement la sauvegarde des mesures visant à limiter l'impact des traitements sur les personnes concernées – devront également faire l'objet d'une attention particulière. Le terme « *privacy enhancing technologies* »[146] (PETs) désigne l'ensemble des technologies ayant pour but de minimiser les risques relatifs à la protection des données (tant dans son aspect concernant les droits des personnes concernées (*privacy*) que de la sécurité (*security*))[147]. Au-delà des PETs « innovantes »[148], nous classons dans cette catégorie les mesures de codage/pseudonymisation qui sont couramment utilisées dans le cadre des projets de recherche[149]. Il est dans ce cadre important de s'assurer que les différents acteurs impliqués dans la recherche s'engagent contractuellement à respecter ces mesures, et notamment à ne pas chercher à identifier les personnes concernées[150].

[98] Enfin, les parties devront régler les problématiques plus « classiques » concernant la **responsabilité**, les **garanties** fournies, et les éventuelles obligations d'**indemnisation**. Ces clauses devront prendre en considération le rôle et les responsabilités propres à chaque cocontractant en matière de protection des données. Ainsi, les fournisseurs de données (*data providers*) devront en principe garantir que les données personnelles ont été collectées de manière conforme au droit applicable, et notamment que tous les consentements et toutes les autorisations nécessaires ont été obtenus. Selon les cas, les récipiendaires de ces données (*data recipients*) devront, quant à eux, garantir que les données seront traitées de manière licite, conformément au contrat et de manière sûre. Suivant les circonstances (et le rapport de force entre les parties) des clauses spécifiques d'indemnisations seront prévues, en particulier en cas de co-responsabilité du traitement.

5. Cas pratiques et exemples

[99] Afin d'illustrer les principes présentés dans cet article, nous analysons ci-après trois situations typiques impliquant le partage de données personnelles dans le cadre d'activités de recherche.

---

titutions, they do not work for many public or governmental institutions, such as federal institutions in the USA, which include major research partners (or funders) of many European researchers. ». Cette opinion est antérieure à la publication par la Commission européenne d'une nouvelle version de ses clauses standards le 4 juin 2021, il n'est toutefois pas prévu que ce document résolve les problèmes antérieurement identifiés. Cf. également section 2.c.ii et nbp 37.

146 Traduit en français par « technologies améliorant la confidentialité (TAC) » (voir https://fr.wikipedia.org/wiki/Technologies_am%C3%A9liorant_la_confidentialit%C3%A9).

147 ALLEA/EASAC/FEAM, International Sharing of Personal Data for Research (nbp 1), p. 36.

148 Voir les exemples cités dans le rapport ALLEA/EASAC/FEAM, International Sharing of Personal Data for Research (nbp 1), p. 37 : « *(1) homomorphic encryption allowing data to be encrypted before it is shared ; (2) differential privacy adding noise to an analytical system to render it impossible to trace back individual inputs ; (3) federated analysis allowing parties to share the insights of their analysis without sharing the data ; (4) confidential computing using hardware-based techniques to isolate data, specific functions or the entire applications of an operating system, virtual machines or other processes ; (5) secure multi-party computation spreading data across multiple parties so that no individual party is able to see the complete set of inputs* », ainsi que les pp. 47–50.

149 ALLEA/EASAC/FEAM, International Sharing of Personal Data for Research (nbp1), p. 8 ; cf. *supra* section 2.d.ii.

150 Pour un exemple, voir la clause III.4 du modèle de *Data Transfer And Use Agreement* du SPHN (nbp 137).

a. Cas 1 : Partage de données entre chercheurs d'hôpitaux universitaires via une infrastructure sécurisée

[100] « *Une chercheuse employée dans un hôpital universitaire cantonal effectue une recherche visant à identifier de nouveaux marqueurs tumoraux liés au cancer du sein. Dans ce cadre, elle souhaite utiliser les données des patientes ayant été traitées pour cette maladie dans un autre département de l'hôpital où elle travaille, ainsi que des patientes traitées dans les hôpitaux universitaires de deux autres cantons suisses. Elle soumet une demande et obtient de la commission d'éthique compétente l'autorisation d'effectuer la recherche. Les parties conviennent que les données des patientes utiles à la recherche provenant des autres hôpitaux universitaires seront mises à disposition de la chercheuse via l'infrastructure BioMedIT* [151].»

[101] Dans cet exemple, la chercheuse aura accès à des données de patientes traitées dans plusieurs hôpitaux universitaires suisses en rapport avec leur maladie et les traitements prodigués. Il s'agit de données sensibles (données relatives à la santé) ayant été initialement collectées à des fins thérapeutiques (qui sont donc des *real world data*[152]).

[102] Dans la mesure où la recherche porte sur une maladie humaine et est pratiquée sur des données personnelles liées à la santé qui n'ont pas été anonymisées (mais qui seront en principe codées), la loi sur la recherche sur l'être humain (LRH) s'applique dans cette situation[153]. Les hôpitaux universitaires étant en règle générale des entités de droit public cantonal, les lois cantonales sur la protection des données édictées dans les cantons concernés s'appliquent en principe de manière supplétive (en tant que *lex generalis*)[154].

[103] La chercheuse de cet exemple assume en principe le rôle de direction du projet (art. 3 al. 1 ORH). Elle est soumise à ce titre aux obligations décrites ci-avant dans la section 3.a.ii (notamment la réalisation pratique du projet de recherche, la protection des personnes participant au projet de recherche au lieu de réalisation, ainsi que la réalisation de la recherche conformément au plan de recherche). Ni elle, ni les autres membres du personnel de l'hôpital cantonal dans lequel il exerce, n'assument par contre le rôle de responsable du traitement ; ce rôle est en effet assumé par l'hôpital cantonal directement, ceci pour les traitements se rapportant au projet de recherche[155].

[104] De la même manière, le département de l'hôpital qui transmet des données à la chercheuse rattachée à un autre département n'assume aucun rôle spécifique en matière de protection des données. Cette transmission n'est pas considérée comme une communication/un transfert de données au sens des règles applicables en matière de protection des données, puisque les données restent au sein de la même entité juridique. Il convient toutefois de veiller au respect du secret professionnel, qui trouve quant à lui application au sein d'un même établissement, même entre personnes soumises à la même obligation légale de garder le secret[156].

---

151 Cf. section 3.a.vi.

152 Cf. section 2.b

153 Cf. art. 2 al. 1 let. e et al. 2 let. c (*a contrario*) LRH. Comme exposé à la section 2.d.ii, la LRH s'applique aux données codées, y compris lorsque le récipiendaire des données n'a pas accès à la clé de déchiffrement.

154 Cf. section 2.b.i.

155 Cf. sections 3.b.iii, 3.b.v et 3.b.vi : les collaborateurs d'une entité n'agissent en principe ni comme sous-traitants, ni comme responsables du traitement (tant qu'ils n'outrepassent pas leur fonction).

156 Erard, Le secret médical, p. 508 ss (nbp 123).

[105] Les autres hôpitaux cantonaux agissent en tant que responsables du traitement indépendants pour les activités de traitements qu'ils effectuent sur leur propre base de données. Chaque hôpital est responsable conjoint du traitement avec l'hôpital du chercheur pour le transfert des données de leurs patients au chercheur[157]. Ces entités devront conclure un accord avec l'hôpital de la chercheuse[158] – qui prendra souvent la forme d'un *[controller to controller] data transfer agreement*[159] – définissant notamment les finalités et modalités selon lesquelles les données communiquées peuvent être traitées par la chercheuse, ainsi que la répartition des responsabilités et la collaboration entre les parties.

[106] L'exploitant de l'infrastructure BioMedIT[160] se voit chargé par les hôpitaux d'héberger les données et de les mettre à disposition de la chercheuse via son infrastructure sécurisée. Il agit dans ce cadre en tant que sous-traitant des responsables conjoints du traitement[161]. Un *data processing agreement* ou autre accord de ce type devra être conclu entre les parties concernées[162], définissant notamment les rôles des parties et les engagements du sous-traitant en lien avec les données qu'il traite[163].

[107] Se pose enfin la question du rôle de la commission d'éthique chargée d'approuver et de superviser la recherche. Premièrement, il n'est pas exclu que cette commission ait accès à des données personnelles liées au projet de recherche[164], auquel cas elle les traiterait en qualité de responsable du traitement (indépendante). Au demeurant, même en l'absence d'accès à des données personnelles, la commission d'éthique pourrait se voir reconnaitre une position de responsable du traitement si elle participe à la détermination des finalités et modalités des traitements des données effectués dans le cadre de la recherche[165]. En pratique, ceci devrait à notre avis rester rare (par exemple dans des situations où la commission d'éthique subordonne en vertu de l'art. 48 al. 2 LRH la poursuite d'un projet de recherche à des conditions supplémentaires impactant les finalités et modalités du traitement).

b. Cas 2 : Partage de données dans le cadre d'un consortium de recherche

[108] «*Plusieurs instituts de recherche répartis en Europe et en Suisse décident de participer à un projet de recherche commun et de mettre sur pied une plateforme sécurisée pour l'hébergement et le par-*

157 Cf. sections 3.b.iv et 3.b.vi. La décision concernant le type de données qui sont transférées, leur format, et la finalité du transfert sont décidés en commun par les représentants de chaque hôpital fournisseur de données (*data provider*) et de l'hôpital qui les reçoit (*data recipient*).

158 Un accord entre responsables du traitement est expressément exigé en droit européen par l'art. 26 RGPD. En droit suisse, un tel accord n'est certes pas explicitement requis (que ce soit selon le droit actuel ou la nLPD) ; toutefois, *de facto*, un tel accord apparaît nécessaire pour assurer que chaque responsable puisse se conformer à ses propres obligations (p. ex. pour donner suite à un retrait du consentement d'un participant à la recherche), cf. section 4.b.

159 Pour un exemple, voir le modèle de *Data Transfer and Use Agreement* (DTUA) du SPHN (nbp 137).

160 L'infrastructure BioMedIT est actuellement gérée par trois « nœuds » (à Zurich, Bâle et Lausanne), qui peuvent être mandatés individuellement ou conjointement par des responsables de traitement.

161 Cela même si les données qu'il reçoit sont codées : cf. section 3.b.v et nbp 112.

162 Art. 9 al. 1 nLPD et 28 RGPD. Le RGPD contient une description détaillée du contenu minimum exigé pour ce type d'accord.

163 Pour un exemple, voir le modèle de *Data Transfer and Processing Agreement* (DTPA) du SPHN (nbp 138).

164 Voir les exemples cités à la section 3.a.vii.

165 Cf. sections 3.b.iii et 3.b.vi.

tage des données de la recherche. Les parties élisent un directeur principal du projet (project leader) et définissent dans le cadre de leur accord les contributions de chaque institut. L'un des partenaires est chargé du développement technique de la plateforme sécurisée (build), ainsi que de son opération (run) sur sa propre infrastructure, sans que celui-ci fournisse toutefois lui-même des données. Une fois l'infrastructure fonctionnelle, chaque institut y introduit les données personnelles qu'il détient aux fins de la recherche commune, dans le format convenu, et utilise les données fournies par les autres instituts par le biais de la plateforme pour mener à bien la recherche. »

[109] La présence au sein du consortium de partenaires européens, ainsi que probablement de données personnelles relatives à des résidents européens, pose la question de l'application du RGPD. Comme exposé à la section 2.b, l'application du RGPD à des activités de recherche menées depuis la Suisse en vertu des critères de rattachement territoriaux du RGPD est sujette à débat. Dans les faits, il est toutefois probable que les partenaires européens imposent aux instituts suisses le respect des exigences du RGPD, afin de pouvoir eux-mêmes assurer leur conformité.

[110] Dans cet exemple, tous les instituts sont considérés comme des responsables conjoints du traitement pour les traitements des données personnelles mises à disposition sur la plateforme, puisqu'ils ont décidé ensemble de la finalité et des modalités des traitements (notamment le type de données échangées, la manière de les échanger [via la plateforme], le format, ainsi que les buts du traitement)[166]. Chacun des instituts est cependant un responsable du traitement indépendant pour tout autre traitement effectué en dehors de la plateforme pour ses finalités spécifiques[167]. Il est notamment envisageable que le contrat liant les instituts autorise chacun d'eux à réutiliser les données pour leurs propres activités de recherche, menées de manière indépendante, auquel cas ils agiront chacun dans ce cadre en tant que responsable du traitement indépendant[168].

[111] La relation entre les parties, en ce qu'elle concerne la protection des données, devra donc être couverte par un accord de responsables conjoints (tel que le *[controller to controller] data transfer agreement* mentionné dans l'exemple 1). Il est toutefois courant dans ce type de projet que la relation entre les parties soit régie par un accord à vocation plus large, traitant, en sus des aspects sur la protection des données, notamment de la gouvernance du consortium, des obligations de chaque partie, de la titularité des résultats de la recherche ou des règles applicables en matière de publication[169].

[112] Enfin, le partenaire du projet qui est chargé du développement et de l'exploitation technique de la plateforme sera en règle générale lui aussi qualifié de responsable du traitement conjointement avec les autres membres du consortium. En effet, de par sa position au sein du consortium, il participe à la détermination des finalités et modalités des traitements de données personnelles effectuées au travers de celle-ci. Dans l'hypothèse où cette entité ne faisait pas partie du consortium, mais aurait été mandatée par celui-ci pour exploiter la plateforme, l'entité agirait comme sous-traitant[170].

166 Cf. sections 3.b.iv et 3.b.vi.

167 CEDP, Lignes Directrices responsable du traitement/sous-traitant (nbp 100), p. 23.

168 Il faut naturellement qu'une telle réutilisation soit licite. Chaque institut fournissant des données (*data provider*) aura probablement garanti aux autres que les données personnelles qu'il fournit peuvent être utilisées de manière licite conformément à ce que le contrat prévoit. Cette garantie doit prendre en compte une réutilisation des données pour d'autres projets de recherche si cela est prévu, ce qui implique en principe que les conditions des art. 32 à 35 LRH soient réalisées. Cf. sections 2.c.i et 4.b.

169 Pour un exemple, voir le modèle de *Consortium Agreement* disponible du SPHN (nbp 140).

170 Sous réserve des activités de traitements pour lesquelles elle déciderait elle-même des finalités.

c. Cas 3 : Réalisation d'un essai clinique

[113] « *Un hôpital public et une entreprise pharmaceutique privée décident de réaliser un essai clinique, dans lequel l'hôpital agit comme centre de recherche principal (main site) et l'entreprise pharmaceutique comme promoteur de la recherche (sponsor). Ces parties concluent un Clinical Trial Agreement, qui nomme une chercheuse de l'hôpital en tant qu'investigatrice (main investigator). L'entreprise pharmaceutique et l'hôpital (via son chercheuse) collaborent à la rédaction du protocole de recherche (notamment concernant le but, la méthodologie/la conception de l'étude, les données à collecter, les critères d'inclusion/exclusion des sujets, la réutilisation de la base de données, etc.), qu'ils approuvent tous deux. L'hôpital collecte les données directement auprès de ses patients et les traite tant en sa qualité d'hôpital (fourniture de soin) qu'en tant que centre investigateur (pour la recherche). Les données qui sont utiles à la recherche sont codées par l'hôpital (qui en conserve la clé). L'entreprise pharmaceutique reçoit les données codées pour mener ses activités liées à l'étude et se conformer aux exigences réglementaires pertinentes (par exemple, en ce qui concerne la soumission des résultats aux autorités, pour obtenir l'autorisation de mise sur le marché du médicament et pour se conformer à ses obligations de pharmacovigilance). Conformément à la réglementation sur les essais cliniques (et comme le précise également le contrat qui les lie), l'hôpital et l'investigatrice principale sont uniquement habilités à fournir des données sous forme codée au promoteur de la recherche, mais l'hôpital est tenu de permettre à l'auditeur engagé par le promoteur de la recherche de vérifier dans les locaux de l'hôpital que les consentements nécessaires sont recueillis*[171].»

[114] Dans ce cas, l'hôpital et l'entreprise pharmaceutique sont responsables conjoints du traitement (*joint controllers*) concernant cet essai clinique, car ils déterminent ensemble les finalités communes et les modalités essentielles des traitements[172]. Ceci serait vrai même si l'entreprise pharmaceutique n'avait pas accès aux données personnelles des participants à la recherche (ou seulement sous une forme anonymisée), puisque, par sa participation à la rédaction du protocole de recherche, elle participe à la détermination des finalités des traitements[173].

[115] Dans le cas où l'hôpital ne participe pas à la rédaction du protocole de recherche (il se contente d'accepter le protocole déjà élaboré par l'entreprise pharmaceutique) et où le protocole est uniquement conçu par l'entreprise pharmaceutique, l'hôpital serait – pour les activités de traitement se rapportant spécifiquement à l'essai clinique – considéré comme le sous-traitant (*data processor*) de l'entreprise pharmaceutique, qui agirait quant à elle comme seule responsable du traitement (*data controller*) pour ces activités[174].

[116] Il convient de distinguer les activités de traitements se rapportant spécifiquement à la recherche (pour lesquelles les règles décrites ci-avant s'appliquent), des activités de traitement effectuées par l'hôpital à des fins de soins. Dans ce second cas, l'hôpital agit toujours comme responsable du traitement indépendant (et non comme responsable conjoint ou sous-traitant). Ainsi,

171 CIH, Bonnes Pratiques Cliniques (nbp 38), règles N 5.15 et 5.5.5.

172 Cf. section 3.b.vi et nbp 122.

173 Cf. section 3.b.iv. Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 70.

174 Voir par exemple UK Health Reserach Authority (NHS), *Controller and personal data in health and care research*, in https ://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/what-law-says/data-controllers-and-personal-data-health-and-care-research-context/. Il faut toutefois réserver dans ce cas les activités que l'hôpital doit effectuer pour se conformer à ses propres obligations légales, qu'il effectue en tant que responsable du traitement indépendant : cf. section 3.b.vi.

l'hôpital peut traiter les mêmes données – voire effectuer les mêmes opérations (ex. : inscrire les effets constatés d'un médicament) – tout en assumant des rôles différents[175].

[117] Enfin, si l'entreprise pharmaceutique avait mandaté un CRO pour la réalisation de certaines activités liées à l'essai clinique, par exemple dans le cadre du management des données liées à la recherche (gestion des cahiers d'observation [*Case Report Form* ou CRF], etc.), le CRO aurait en règle générale dû être qualifié de sous-traitant (*subprocessor*) de l'entreprise pharmaceutique[176]. Le CRO traiterait en effet les données personnelles des participants à la recherche sur instruction de l'entreprise pharmaceutique, conformément aux dispositions du contrat de service (*CRO Services Agreement*) ayant été conclu. Cela étant, même dans cette configuration, le CRO pourrait agir comme responsable du traitement indépendant s'il effectuait certaines activités non pas pour le compte de l'entreprise pharmaceutique, mais pour se conformer à ses propres obligations légales ou réglementaires. Ainsi, s'il communiquait des données personnelles à une autorité dans le cadre d'une demande qui concerne le CRO directement, il agirait en principe comme responsable du traitement pour cette activité-là[177].

6. Conclusion

[118] La gestion des données personnelles dans le cadre de la recherche sur l'être humain peut se révéler complexe, non seulement du point de vue de la détermination du cadre réglementaire applicable (ex. : droit suisse ou étranger), mais aussi sous l'angle de l'interprétation des notions juridiques en jeu qui donnent souvent lieu à débat (ex. : notions de responsable du traitement ou sous-traitant, données personnelles ou anonymes).

[119] À l'entame d'un nouveau projet de recherche impliquant des partages de données personnelles, il faut certainement adopter une attitude pragmatique qui consiste à établir clairement les caractéristiques factuelles du projet. Il est ainsi essentiel de commencer par identifier l'ensemble des acteurs concernés par les traitements de données envisagés, puis d'établir un schéma des relations entre ces acteurs. Ces relations impliquent aussi bien les flux de données que les droits d'accès aux données collectées. C'est sur cette base que pourront être appliquées les considérations développées tout au long du présent article, notamment pour identifier le cadre légal applicable et définir les obligations qui incombent à chacun des acteurs du projet de recherche.

[120] Dès l'instant où plusieurs acteurs d'une recherche s'échangent des données personnelles, il est de surcroît primordial qu'ils établissent entre eux une documentation contractuelle pour encadrer ces échanges. Ce cadre contractuel doit en particulier permettre à celui qui partage des données personnelles (*data provider*) de s'assurer que le destinataire des données (*data recipient*) traitera les données en conformité avec ses propres obligations, et réciproquement au *data recipient* de s'assurer qu'il sera en droit de les traiter licitement. Les règles applicables découlent non seulement du droit de la protection des données au sens large (ex. : principe de sécurité), mais

175 *Contra* : Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 71, qui estime que le centre de recherche agit systématiquement comme responsable conjoint du traitement. Le même auteur précise toutefois que le centre de recherche intervient comme sous-traitant du promoteur en ce qui concerne le processus de pseudonymisation des données patients et la transmission ultérieure de ces données pseudonymisées au promoteur.

176 Isler, Rollenverteilung in Klinischen Versuchen (nbp 70), p. 70 ; Rosenthal, Controller oder Processor (nbp 96), annexe.

177 Cf. section 3.b.vi.

aussi et surtout du respect des droits des participants à la recherche garantis par la législation relative à la recherche sur l'être humain (ex. : conséquences du retrait d'un consentement, droit d'être informé des résultats de recherche ou de découvertes incidentes, interdiction de réidentifier les personnes à l'origine des données).

[121] Il va sans dire que les aspects juridiques liés à la gestion des données personnelles dans le contexte de la recherche sont fréquemment vus comme une charge excessive aux yeux des chercheurs et, par conséquent, comme un frein aux avancées de la recherche. Ce sentiment de frustration est compréhensible, d'autant plus que le cadre légal en vigueur en Suisse laisse de nombreuses questions ouvertes ou sans réponse précise. C'est sans compter non plus que le cadre légal doit s'appliquer de manière dynamique à des domaines qui traversent des mutations fulgurantes, à l'image des recherches menées sur des sets de données toujours plus volumineux et voués à être réutilisés, voire fusionnés.

[122] Quoiqu'on puisse en dire, le droit occupe néanmoins un rôle fondamental dans le secteur de la recherche en tant qu'il reflète le contrat social conclu entre la société et les chercheurs. En visant à protéger les participants à la recherche, le droit a pour objectif plus large de préserver la confiance de la population à l'égard du secteur de la recherche. La présente contribution a été rédigée avec la modeste mais sincère ambition de contribuer à éclaircir les concepts juridiques et les règles applicables en la matière, puis de proposer et mettre à disposition des chercheurs des solutions pragmatiques pour leur permettre de faire avancer la recherche.

Alexandre Jotterand, MLaw, avocat, CIPP/E, CIPM, *id est* avocats Sàrl (www.idest.pro).

Frédéric Erard, Dr. iur, avocat, juriste au SIB Swiss Institute of Bioinformatics.

id est avocats Sàrl a contribué à l'établissement des contrats modèles du SPHN cités à titre d'exemple dans cet article. Le SIB Swiss Institute of Bioinformatics est chargé, en collaboration avec l'Académie suisse des sciences médicales (ASSM), de la mise en œuvre de l'initiative SPHN, qui comprend également l'établissement du réseau BioMedIT.

Cet article reflète l'opinion personnelle de ses auteurs et non celle de leurs employeurs respectifs.