



Benjamin May
Avocat associé
may@aramis-law.com



Cécile Goy
Avocate collaboratrice
goy@aramis-law.com

Avril 2022

Santé connectée : Quelles protections par la propriété intellectuelle?

Les innovations de santé connectée ou *digital therapeutics* connaissent un essor fulgurant porté par l'IA, l'open data et la convergence des technologies. Trouver le bon angle pour protéger et valoriser ces inventions incite à adopter une approche holistique. Cette étude dresse un panorama des outils et des bonnes pratiques.

Des *wearables* permettant de surveiller son diabète aux systèmes d'aide à la décision médicale en passant par les solutions pour l'exploitation des données de santé ou la chirurgie robotique, la e-santé connecte les dispositifs médicaux et les produits pharmaceutiques au monde des données et de l'intelligence artificielle (IA). Les innovations à protéger sont multiples alors que la propriété intellectuelle appréhende difficilement la protection de certains éléments clés tels que les procédés, les données d'entraînement de l'IA, des paramètres, ou encore des algorithmes¹. Des innovations qui de surcroît suivent des cycles de vie courts, de sorte qu'elles peuvent constituer des « cibles mouvantes » pour la propriété intellectuelle. Cette étude dresse un panorama des outils de protection.

1. Droit d'auteur et droit *sui generis* des bases de données : une protection à ne pas surestimer

Le droit d'auteur, mais aussi le droit *sui generis* des bases de données, présentent l'avantage d'être obtenus sans dépôt dès lors que les conditions sont réunies. Ces protections présentent cependant des limites importantes.

A. Le droit d'auteur

L'objet de la protection. - Dans un dispositif de santé connectée, le droit d'auteur peut notamment protéger les interfaces graphiques et éléments multimédias incorporés (son, texte, image). Le *look and feel* d'une application de télésanté pourrait, par exemple, bénéficier de cette protection.

¹ J.-M. Deltorn, Questions de propriété sur les données et modèles d'apprentissage - La protection des applications de l'IA par la propriété intellectuelle : 5e Forum Industriel en Intelligence Artificielle (FIIA), 2020.

S'agissant des logiciels, seule leur expression est protégée par le droit d'auteur, c'est-à-dire le code et le matériel de conception préparatoire (incluant les analyses fonctionnelle et organique, maquettes, organigrammes, spécifications internes et externes et l'architecture fonctionnelle²). Au contraire, « *les idées et principes qui sont à la base de quelque élément que ce soit d'un programme d'ordinateur* » ne sont pas protégés³. Ainsi, le droit d'auteur ne protège pas les algorithmes⁴, les fonctionnalités, le langage de programmation, le format de fichiers de données⁵ ou les méthodes⁶.

Quant aux bases de données, seule leur structure (architecture ou agencement) est protégeable par le droit d'auteur, et non leur contenu. La protection par le droit d'auteur des données elles-mêmes, qui sont au cœur de la valorisation des entreprises de e-santé, est tout sauf évidente. En pratique, on distingue les données brutes des données traitées c'est-à-dire l'« *information organisée, interprétée, contextualisée et parfois enrichie au regard d'une finalité* »⁷. Or, il a été jugé que « *les informations brutes ne peuvent en effet être considérées comme protégeables au titre du droit d'auteur* »⁸. Si elles englobent une œuvre de l'esprit, les données traitées pourraient prétendre à la protection par le droit d'auteur. Ce pourrait par exemple être le cas de données médicales modifiées ou restructurées par des professionnels de santé, mais la condition d'originalité reste un obstacle souvent important à la protection.

Les conditions de protection. - La protection par le droit d'auteur est soumise à une condition d'originalité, définie par la jurisprudence comme l'empreinte de la personnalité de l'auteur. Ce critère développé initialement pour les beaux-arts apparaît mal adapté aux technologies de santé connectée. Il a été aménagé s'agissant des logiciels et des bases de données, mais une certaine insécurité juridique découle des termes abstraits utilisés par la jurisprudence. Pour les logiciels, le célèbre arrêt *Pachot* de 1986 précise qu'un logiciel est original s'il porte la marque de l'apport intellectuel de son auteur et résulte d'un effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante⁹. Il conviendra de vérifier si les choix du développeur témoignent « *d'un apport intellectuel propre et d'un effort personnalisé* »¹⁰. S'agissant des bases de données, la Cour de justice de l'Union européenne (CJUE) estime que « *ce critère de l'originalité est rempli lorsque, à travers le choix ou la disposition des données qu'elle contient, son auteur exprime sa capacité créative de manière originale en effectuant des choix libres et créatifs* »¹¹. Dans le sens de cette jurisprudence, les juridictions françaises ne prennent pas en compte les efforts et savoir-faire consacrés à la création des données elles-mêmes¹².

Les limites liées à l'open data et à l'open source. - L'open data et l'open source sont susceptibles de limiter également la protection par le droit d'auteur.

Dans le but de développer l'open data, une ordonnance de transposition du 24 novembre 2021 a étendu l'exception de fouille de textes et de données (ou *Text and Data Mining*), définie comme la « *mise en œuvre d'une technique d'analyse automatisée de textes et données sous forme numérique afin d'en dégager des informations, notamment des constantes, des tendances et des corrélations* »¹³. C'est l'une des étapes des systèmes de *deep learning*¹⁴.

² Agence pour la protection des programmes, « La protection par le droit d'auteur spécifique des logiciels », 2018.

³ PE et Cons. UE, dir. 2009/24/CE, 23 avr 2009, concernant la protection juridique des programmes d'ordinateur, art. 1, 2°.

⁴ Cass. 1re civ., 14 nov. 2013, n° 12-20.687 : JurisData n° 2013-025752.

⁵ CJUE, 2 mai 2012, aff. C-406/10, *SAS Institute Inc. c/ World Programming Ltd* : JurisData n° 2012-012011.

⁶ TGI Paris, 14 juin 2002 : Comm. com. électr. 2002, comm. 113, note C. Caron. - CA Paris, 5 avr. 1993.

⁷ MEDEF, La stratégie data comme source de valeur pour l'entreprise, sept. 2021.

⁸ TGI Paris, 24 mars 2010, n° 08/12969.

⁹ Ass. Plén. 7 mars 1986, *Pachot*.

¹⁰ Cass. 1re civ., 17 oct. 2012, n° 11-21.641 : JurisData n° 2012-023661.

¹¹ CJUE, 1er mars 2012, aff. C-604/10, *Football Dataco Ltd e.a. c/ Yahoo! UK Ltd e.a.* : Comm. com. électr. 2012, comm. n° 47, obs. C. Caron.

¹² V. notamment CA Paris, 27 oct. 2015, n° 14/14239 : Propr. intell. 2016, p. 69, note J.-M. Bruguière.

¹³ Ord. n° 2021-1518, 24 nov. 2021, transposant la Directive (UE) 2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique, créant les articles L. 122-5-3 et L. 122-6-1, VI du Code de la propriété intellectuelle.

¹⁴ J.-M. Bruguières, Intelligence artificielle et droit d'auteur - Sortir de la science-fiction des "machines/auteurs", entrer dans la réalité du droit des données : Comm. com. électr. 2020, étude 11.

Initialement, cette exception au droit d'auteur était limitée aux fouilles réalisées pour les besoins de la recherche publique, à l'exclusion de toute finalité commerciale. Désormais, toute personne, à toutes fins (donc même commerciales), peut reproduire une œuvre ou un logiciel en vue de la fouille de textes et de données, à condition d'y avoir accédé de manière licite. L'impact pratique de cette exception pour les entreprises de e-santé est encore incertain car la divulgation de l'œuvre semble être une condition de l'exception¹⁵. Dès lors, si l'accès à l'œuvre a été obtenu sous le sceau de la confidentialité, dans le cadre d'un accord de consortium par exemple, l'exception de « fouille » devrait logiquement pouvoir être exclue.

Par ailleurs, les entreprises de santé connectée utilisent des briques *open source* pour développer leurs solutions. De telles « briques » sont des composants logiciels qui peuvent être utilisés, copiés, modifiés, distribués sans autorisation du propriétaire, aux termes d'une licence libre. Or, certaines licences libres, comme la licence GPL v3, sont considérées comme « contaminantes » de sorte que les améliorations ou nouvelles applications réalisées à partir du logiciel *open source* devront être partagées et seront, elles aussi, soumises aux conditions de la licence libre, ce qui implique souvent une perte de valeur de la technologie¹⁶.

B. Le droit *sui generis* des bases de données

L'objet de la protection. - Le droit *sui generis* du producteur de bases de données permet de protéger les bases de données en s'affranchissant des critères du droit d'auteur. Ainsi, le corpus des données d'apprentissage utilisées par une technologie de santé connectée intégrant de l'IA pourrait être protégé. La donnée n'est cependant pas protégée en tant que telle : seule l'extraction ou la réutilisation d'une partie qualitativement ou quantitativement substantielle du contenu de la base peut être interdite.

Les conditions de la protection. - Pour que le contenu de la base de données bénéficie de la protection, sa constitution, sa vérification ou sa présentation doivent attester d'un investissement financier, matériel ou humain substantiel¹⁷. La cour d'appel de Paris a récemment reconnu la protection de la base de données d'annonces immobilières du site leboncoin.fr¹⁸.

Toutefois, selon la jurisprudence européenne, seuls les moyens consacrés à la recherche d'éléments existants et à leur rassemblement sont pris en compte, à l'exclusion des moyens mis en œuvre pour la création du contenu de la base de données¹⁹. Dès lors, la protection apparaît limitée aux bases réunissant des données préexistantes provenant de sources extérieures, les bases réunissant des données créées par celui qui constitue la base ne remplissant, en principe, pas le critère de l'investissement substantiel. Les entreprises de santé connectée doivent donc avoir conscience que ce droit *sui generis* ne leur permettra pas de protéger « *les données produites par des machines, les dispositifs de l'Internet des objets, les mégadonnées ou les données résultants de [l'IA]* »²⁰, ni les modèles utilisés dans l'IA, à savoir le jeu de paramètres issus de l'apprentissage²¹.

Les nouvelles limites de la protection. - Une décision récente de la CJUE a drastiquement réduit la portée du droit *sui generis* en ajoutant une nouvelle condition à la protection : les extractions et réutilisations du contenu d'une base de données ne sont interdites que si elles ont pour effet de priver le titulaire de revenus censés lui permettre d'amortir le coût de l'investissement pour l'obtention, la vérification et la présentation du contenu de la base de données²².

¹⁵ « Lorsque l'œuvre a été divulguée, l'auteur ne peut interdire (...) » (CPI, art. L. 122-5).

¹⁶ A. Dureuil, Les six points de vigilance pour contractualiser autour de l'intelligence artificielle : Mind Health, 9 oct. 2018.

¹⁷ CPI, art. L. 341-1.

¹⁸ CA Paris, 2 févr. 2021, n° 17/17688 : JurisData n° 2021-001481 ; Propr. industr. 2021, comm. 27, J. Larriue ; Propr. industr. 2021, comm. 34, N. Bouche ; Comm. com. électr. 2021, comm. 42, P. Kamina.

¹⁹ CJUE, 9 nov. 2004, aff. C-203/02, *The British Horseracing Board Ltd et a. c/ William Hill Organization Ltd*. - CJUE, 9 nov. 2004, aff. C-46/02, *Fixtures Marketing Ltd c/ Oy Veikkaus Ab* : Comm. com. électr. 2005, comm. 2, Ch. Caron.

²⁰ S. Chatry, Droits des producteurs des bases de données : JCl. Propriété littéraire et artistique, fasc. 1650, citant « Évaluation of Directive 96/9/EC on the legal protection of databases », SWD (2018) 147 final, p. 15 et 24.

²¹ J.-M. Deltom et G. Leménager, La protection de l'intelligence artificielle en France et en Europe : Réalités industrielles, Annales des Mines, nov. 2020.

²² CJUE, 3 juin 2021, aff. C-762/19, *CV-Online Latvia*.

Comme l'a relevé un auteur, cette nouvelle condition risque d'inciter, en pratique, les producteurs de bases de données à se détourner du droit *sui generis* au profit du droit commun, l'action en parasitisme, par exemple, étant plus souple à mettre en œuvre²³.

Par ailleurs, l'ordonnance de transposition du 24 novembre 2021 a également étendu l'exception de *Text and Data mining* aux extractions, copies ou reproductions numériques de bases de données réalisées par toutes personnes, à toutes fins, même commerciales. Ici, encore, l'exception apparaît limitée aux bases de données « mise[s] à la disposition du public »²⁴, à l'exclusion des bases de données dont l'accès a été obtenu sous le sceau de la confidentialité, de sorte que l'impact pour les entreprises de e-santé semble limité.

2. Le brevet : une protection à envisager

Le premier dépôt des start-ups de e-santé est souvent une demande de marque portant sur le nom de l'entreprise, du produit ou du service. Dans le cadre d'une réflexion globale de valorisation des actifs, d'autres dépôts doivent être considérés. Les dessins et modèles peuvent par exemple protéger l'interface graphique d'une application de télésanté ou le design d'une balance connectée. Le dépôt d'un brevet doit également être envisagé : il rassure les investisseurs en conférant une valeur quantifiable à la technologie et représente un obstacle pour les concurrents, qui ne peuvent utiliser la même invention, même développée de manière indépendante. Contrairement à certaines idées reçues, les exclusions de la brevetabilité ne sont pas un obstacle insurmontable à la brevetabilité des innovations de e-santé, même si la protection d'inventions intégrant de l'IA revêt des particularités.

A. Les exclusions de brevetabilité

Les méthodes de diagnostic. - Certaines innovations de santé connectée ont pour objectif de réaliser un diagnostic. Il peut s'agir, par exemple, d'un logiciel qui utilise de l'IA pour interpréter des radiographies. En droit européen, les méthodes de diagnostic appliquées au corps humain ou animal sont exclues de la brevetabilité. L'objectif est d'éviter qu'un praticien ne puisse pas diagnostiquer un patient à raison d'un droit de brevet. Mais les entreprises de e-santé ne doivent pas surestimer la portée de cette exclusion.

Tout d'abord, seules sont exclues de la brevetabilité les méthodes qui présentent toutes les caractéristiques suivantes : une phase d'investigation, une comparaison de ces données avec les valeurs normales, la constatation d'un écart significatif et une phase de décision déductive. « *Seules seront exclues les méthodes dont le résultat permet directement de prendre une décision au sujet du traitement médical à effectuer* »²⁵.

Surtout, seules les revendications de méthode tombent sous le coup de l'exclusion. L'exclusion ne s'applique pas aux substances et appareils pour la mise en œuvre de ces méthodes²⁶. Dès lors, sont potentiellement brevetables les revendications portant sur des dispositifs médicaux, des programmes d'ordinateur ou des supports d'enregistrement²⁷. En conséquence, en matière de santé connectée, peut être protégé le dispositif en lui-même, tel qu'un *wearable* mesurant le flux sanguin et utilisant les données pour diagnostiquer un problème cardiovasculaire. Il est plus difficile de breveter le logiciel et la méthode inclus dans le dispositif, mais cela est possible si la revendication se concentre sur la manière dont les données sont collectées, analysées et traitées, sans référence au diagnostic²⁸.

²³ J. Larrieu, Bases de données : le droit sui generis en péril ? : Propr. industr. 2022, comm. 5.

²⁴ CPI, art. L. 342-3.

²⁵ J.-C. Galloux, J. Azéma, Droit de la propriété industrielle : Dalloz, 8e éd., 2017, p. 193.

²⁶ CPI, art. L. 611-16.

²⁷ OEB, Directives relatives à l'examen pratiqué, Partie G, Chapitre II, 4.2.

²⁸ P. Sadler, Z. Mummery, Innovations in digital healthcare – navigating patent challenges : Med-Tech news, 2 août 2021.

Les programmes d'ordinateur et méthodes mathématiques. - En droit européen, les programmes d'ordinateurs, méthodes mathématiques, plans, principes et méthodes dans l'exercice d'activités intellectuelles en tant que tels sont exclus de la brevetabilité. Pour l'INPI²⁹ comme pour l'OEB³⁰, l'intelligence artificielle est une méthode mathématique mise en œuvre par ordinateur, dans la mesure où elle se fonde sur des modèles de calculs et des algorithmes « utilisés à des fins de classification, de partitionnement, de régression et de réduction de la dimensionnalité ». Toutefois, ces exclusions ne constituent pas des obstacles insurmontables à la brevetabilité des innovations de e-santé, même si celles-ci intègrent de l'IA.

En effet, les programmes d'ordinateur et méthodes mathématiques ne sont exclus de la brevetabilité que pour autant qu'ils soient revendiqués « en tant que tels ». Si les caractéristiques de la revendication sont uniquement abstraites (par exemple, un procédé de classification utilisant l'apprentissage automatique), celle-ci est dépourvue de caractère technique et exclue de la brevetabilité. Au contraire, un programme d'ordinateur est protégeable dès lors qu'il produit un effet technique supplémentaire au-delà des interactions physiques normales entre le programme et l'ordinateur. Un logiciel contrôlant une machine de dialyse ou traitant des données physiologiques issues de capteurs peut, par exemple, être breveté³¹. Surtout, il faut distinguer les « programmes d'ordinateur » des « méthodes mises en œuvre par ordinateur » qui font intervenir des moyens techniques (l'ordinateur) et présentent donc un effet technique³². De même, une revendication portant sur une méthode mathématique faisant intervenir des moyens techniques ou sur un dispositif n'est pas exclue de la brevetabilité³³. La seule référence à un système physique, comme un ordinateur, permet de surmonter l'exclusion³⁴, et c'est au stade de l'appréciation de l'activité inventive qu'une distinction devra être faite entre les caractéristiques techniques et non techniques de la revendication (voir infra).

Il est peu probable qu'un effet technique soit reconnu si le logiciel a une finalité purement organisationnelle, par exemple envoyer automatiquement le diagnostic au médecin³⁵. À l'inverse, l'utilisation d'un réseau neuronal dans un appareil de surveillance cardiaque pour détecter des battements irréguliers, serait brevetable³⁶.

B. Les spécificités des brevets portant sur des inventions intégrant de l'IA

Le développement de l'IA soulève de nouvelles questions pour les offices de propriété intellectuelle. Ce sont autant de spécificités que les entreprises de la santé connectée doivent connaître lorsqu'elles envisagent de breveter des inventions intégrant de l'IA.

La désignation de l'inventeur. - Il est aujourd'hui établi qu'un système d'IA ne peut pas être désigné comme inventeur en Europe. Le 21 décembre 2021, la chambre de recours de l'OEB a confirmé les décisions relatives au rejet des demandes dont l'inventeur désigné était le système d'IA « DABUS »³⁷. Si l'USPTO a statué dans le même sens, des décisions contraires existent notamment en Australie et en Afrique du Sud.

La suffisance de description. - Au sein du brevet, l'invention doit être suffisamment décrite pour que l'homme du métier puisse l'exécuter, ce qui pose de nouvelles questions s'agissant de l'IA. Pour breveter une invention intégrant de l'IA, il convient de décrire les données entrantes, les données sortantes, le type d'IA (réseau de neurones, algorithme génétique, machine à vecteurs de support, etc.), l'architecture interne et son éventuel apprentissage³⁸.

²⁹ INPI, Directives relatives à la délivrance des brevets, 2020.

³⁰ OEB, Directives relatives à l'examen pratiqué, Partie G, Chapitre II, 3.3.1.

³¹ P. Sadler, Z. Mummery, op. cit.

³² OEB, Directives relatives à l'examen pratiqué, Partie G, Chapitre II, 3.6.

³³ OEB, Directives relatives à l'examen pratiqué, Partie G, Chapitre II, 3.3.

³⁴ J.-M. Deltorn, Brevetabilité - La brevetabilité des applications de l'intelligence artificielle et de l'apprentissage automatique : la pratique de l'Office européen des brevets : Propr. industr. 2019, dossier 4.

³⁵ P. Sadler, Z. Mummery, op. cit.

³⁶ OEB, Directives relatives à l'examen pratiqué, Partie G, Chapitre II, 3.3.1.

³⁷ Section de dépôt de l'OEB, 27 janv. 2020, J 8/20 et J 9/20. - Chambre de recours de l'OEB, 21 déc. 2021.

³⁸ O. Rocher, 3 questions - Propriété industrielle et IA : JCP E 2020, 27.

L'algorithme non entraîné pourrait ainsi devoir être divulgué, au même titre que les données d'entraînement qu'il devra utiliser. A par exemple été rejetée, une demande de brevet portant sur une méthode d'évaluation du débit cardiaque à partir de la pression artérielle fondée sur un réseau de neurones artificiels dont les coefficients de pondération sont déterminés par apprentissage car les données d'apprentissage n'étaient pas suffisamment décrites³⁹. Selon un auteur, une description devrait être considérée comme suffisante dès lors que sont fournies « *des informations détaillées sur les méthodologies de sélection des sources et de traitement des données spécifiquement adaptées pour permettre à la personne de métier d'obtenir les données d'apprentissage adéquates en vue de l'objectif visé* »⁴⁰.

L'activité inventive. - Il a été vu que les offices traitent l'IA comme une méthode mathématique, et que la simple mention d'un ordinateur permet de surmonter l'exclusion de la brevetabilité. Toutefois, au stade de l'appréciation de l'activité inventive, l'OEB ne prend en compte que les caractéristiques qui contribuent au caractère technique de l'invention⁴¹. Or, une méthode ne contribue au caractère technique d'une invention que (i) lorsqu'elle répond à une finalité technique ou (ii) lorsqu'elle est adaptée aux fins d'une mise en œuvre technique spécifique. Ainsi, une méthode d'IA présente une finalité technique lorsque l'étape algorithmique participe à la solution d'un problème technique concret⁴². L'OEB considérera que la méthode d'IA est adaptée aux fins d'une mise en œuvre technique spécifique lorsqu'elle est spécifiquement adaptée au fonctionnement interne de l'ordinateur⁴³. Dans ce cas, l'étape algorithmique présente un caractère technique et sera prise en compte pour l'examen de l'activité inventive.

Malgré ces spécificités, les entreprises de e-santé ne doivent pas surestimer la difficulté pour breveter des inventions intégrant de l'IA. À titre d'illustration, un moniteur cardiaque contrôlé par un réseau de neurones spécialement adapté pour limiter les cas de fausses alertes a été considéré brevetable⁴⁴.

3. Le contrat : une protection à construire et entretenir

A. Le contrat pour protéger les secrets d'affaires

Les entreprises de santé connectée collaborent fréquemment avec des tiers : établissements de santé, établissements de recherche, consultants, sociétés tierces, etc. Qu'il s'agisse de partenaires académiques ou partenaires économiques, la confidentialité doit être assurée du début des négociations à la fin du projet, voire au-delà. C'est l'une des conditions pour bénéficier de la protection par le secret des affaires.

L'objet et les limites de la protection. - Les secrets d'affaires peuvent protéger des données, brutes ou traitées, et bases de données. Ainsi, les entreprises de e-santé pourraient bénéficier d'une protection sur le corpus de données d'apprentissage utilisées dans leurs systèmes d'IA. Les secrets d'affaires peuvent également porter sur des algorithmes, du code, des procédés, des paramètres, etc. Toutefois, les secrets d'affaires sont plus difficiles à défendre et valoriser que les formes classiques de propriété intellectuelle puisqu'il s'agit d'un système de responsabilité civile, et non d'un droit de propriété. Ainsi, l'obtention, l'utilisation et la divulgation illicite de secrets des affaires sont sanctionnées, mais la découverte indépendante des mêmes informations reste licite. Il n'est, par exemple, pas possible d'interdire à son concurrent de produire de manière indépendante le même système d'IA.

³⁹ OEB, ch. rec., T 0161/18, 12 mai 2020, *Äquivalenter Aortendruck c/ ARC Seibersdorf*.

⁴⁰ F. Hagel, Les données d'apprentissage, talon d'Achille des inventions utilisant l'IA : Propr. industr. 2021, étude 2.

⁴¹ OEB, Directives relatives à l'examen pratiqué, Partie G, Chapitre II, 3.3.

⁴² J.-M. Deltorn, op. cit.

⁴³ J.-M. Deltorn, op. cit.

⁴⁴ OEB, ch. rec., T 0598/07, 19 mai 2010.

Les conditions de la protection. - Pour espérer bénéficier de la protection du secret des affaires sur une information, quelle que soit sa nature, les entreprises de santé connectée doivent s'assurer qu'elle remplit trois conditions.

L'information doit tout d'abord présenter un caractère *secret*, c'est-à-dire qu'elle n'est pas généralement connue ou aisément accessible pour les personnes familières de ce type d'informations. Les entreprises ne doivent donc pas compter sur cette protection si l'information est susceptible d'être divulguée du seul fait de la mise sur le marché du produit de santé connectée. Il peut aussi être risqué d'inclure des algorithmes ou des secrets de fabrication dans des procédures opérationnelles standard (POS) ou des documents marketing, voire dans une demande de brevet.

L'information doit aussi faire l'objet de *mesures de protection* raisonnables pour conserver son caractère secret. Parmi les bonnes pratiques de protection de la confidentialité, on peut citer la classification des informations selon différents niveaux de confidentialité, le marquage des fichiers et des dossiers et la formation des salariés à la protection de la confidentialité. Au sein de l'entreprise, la mise en place d'une politique d'accès à l'information « *on a need-to-know basis* » (politique de « droits et privilèges ») permet également de limiter l'accès à l'information aux seuls les collaborateurs ayant besoin d'en connaître, avec une procédure d'habilitation et de contrôle des accès aux locaux, aux dossiers sur le réseau informatique, etc. La protection du secret par des mesures raisonnables se construit aussi contractuellement. Il est impératif de signer un *non-disclosure agreement* (NDA) avant toute divulgation dans le cadre de la négociation d'un contrat, que ce soit avec de potentiels fournisseurs, clients, partenaires, ou investisseurs. Les clauses de confidentialité dans les contrats de recherche et développement (R&D) sont indispensables. La durée de la confidentialité à l'issue de la fin du contrat est à adapter en fonction de la sensibilité et de l'obsolescence des informations échangées.

Enfin, l'information doit avoir une *valeur commerciale*. Cette condition pourrait être un obstacle à la protection de la donnée par le secret des affaires. Dans les innovations de e-santé, la valeur résulte le plus souvent de la combinaison des données, en particulier des données d'apprentissage utilisées par les systèmes d'IA, sans qu'il soit toujours possible d'associer une valeur commerciale propre à la donnée isolée. Le contrat apparaît alors comme un outil complémentaire de protection de la donnée.

B. Le contrat pour contrôler l'accès et l'utilisation des données

Les restrictions contractuelles validées par l'arrêt *Ryanair*. - Les données constituent le cœur de la valorisation de bon nombre de sociétés de e-santé, mais, comme il a été vu, les outils de protection de ces données sont imparfaits. Le contrat apparaît alors comme solution pour contrôler l'accès et l'utilisation des données, comme l'illustre l'arrêt *Ryanair*⁴⁵. Dans cette espèce, la compagnie aérienne Ryanair s'opposait à l'utilisation des données présentes sur son site internet par le site de vente en ligne de vols bon marché PR Aviation, non pas sur le fondement du droit d'auteur ou du droit *sui generis* mais sur le fondement de ses conditions générales d'utilisation. La CJUE a retenu que le créateur d'une base de données non protégeable par le droit d'auteur ou le droit *sui generis* peut établir des limitations contractuelles à l'utilisation de celles-ci par des tiers, les dispositions relatives aux droits de l'utilisateur légitime de la base n'étant pas applicables. Comme l'a relevé un auteur, il convient toutefois de veiller à ce que les conditions générales soient acceptées par les utilisateurs, car leur simple mise en ligne ne saurait suffire à les rendre opposables⁴⁶. Le contrat apparaît donc comme un outil essentiel pour contrôler l'accès et l'utilisation des données accessibles au public, comme dans l'affaire *Ryanair*, mais également des données échangées dans le cadre de *data access agreements* ou de contrats de R&D.

⁴⁵ CJUE, 15 janv. 2015, aff. C-30/14, *Ryanair Ltd c/ PR Aviation BV* : JurisData n° 2015-002578.

⁴⁶ J.-M. Bruguères, op. cit.

Les data access agreements. - La signature de *data access agreements* permet aux entreprises de santé connectée de s'assurer un droit d'accès à des données indispensables au fonctionnement et à l'amélioration de leurs technologies, en particulier lorsqu'elles intègrent de l'IA. En pratique, des accords sont conclus entre éditeurs de logiciels et établissements de santé pour que les éditeurs puissent utiliser les données de santé, personnelles ou anonymisées, détenues par les établissements afin d'entraîner leurs systèmes d'IA. Selon le schéma classique prévu dans ces accords, la plateforme et l'algorithme sont mis gratuitement à disposition des établissements de santé par les éditeurs, qui bénéficient en contrepartie d'un droit d'accès aux données⁴⁷. Il convient alors déterminer contractuellement la propriété et les droits d'utilisation des données entrantes, brutes et traitées, mais également des données et modèles issus de l'apprentissage.

Les contrats de R&D. - Il appartient aux entreprises de e-santé d'utiliser la grande marge de manœuvre laissée par la voie contractuelle pour déterminer conventionnellement la propriété et les droits d'utilisation des données apportées et issues des projets de R&D auxquels elles participent. Tout d'abord, les entreprises apportant des données à un projet commun doivent les revendiquer contractuellement en les listant parmi leurs « connaissances propres », dont elles conserveront la propriété à l'issue du projet. Il convient ensuite d'encadrer les droits d'accès et d'utilisation de leurs données par les autres partenaires. En pratique, chaque partenaire bénéficiera d'une licence gratuite sur les « connaissances propres » des autres pour les besoins et la durée du projet, mais il est possible de limiter contractuellement l'accès à certaines données, notamment en interdisant le *reverse engineering* à ses partenaires. Enfin, les entreprises doivent veiller à se réserver la propriété, voire la copropriété des données issues du projet commun. Il convient de négocier, au minimum, un droit d'accès et d'utilisation des données dont elles ont besoin pour faire fonctionner et améliorer leurs technologies, en particulier pour entraîner leurs systèmes d'IA.

Le contrat apparaît donc comme le pilier central d'une protection multifactorielle des innovations de santé connectée, dont la valorisation passe, dans une certaine mesure, par le droit d'auteur et le droit *sui generis* des bases de données, mais également par le brevet, contrairement aux idées reçues.

⁴⁷ A. Dureuil, op cit.