RGPD : QUELS ENJEUX POUR LES SOCIÉTÉS DE BIOTECHNOLOGIE ?

François-Maxime Philizot et Agathe Simon, associés chez Mercure Avocats, cabinet d'affaires dédié au secteur de la santé, des biotechnologies et des technologies innovantes, décryptent pour Biotech Finances les enjeux du nouveau RGPD.

Le Règlement européen sur la protection des données personnelles (RGPD) – nouvelle législation qui vise à créer un cadre de protection des données plus solide et cohérent en Europe, tout en répondant aux enjeux soulevés par les récentes évolutions technologiques (objets connectés, big data, intelligence artificielle) – entrera en application le 25 mai 2018. Ce règlement est d'application directe dans notre ordre juridique. Néanmoins, il laisse une certaine marge de manœuvre aux états membres pour adapter la législation en vigueur. C'est ainsi qu'en France, un projet de loi visant à adapter la loi *Informatique et libertés* aux dispositions du RGPD est actuellement en cours de discussion au Parlement.

La plupart des entreprises (près de neuf sur dix en pratique) sont concernées par cette nouvelle législation. Toutefois, si celle-ci est souvent présentée comme une contrainte, l'entrée en application du RGPD peut également être vue comme une opportunité. À titre d'exemple, les formalités administratives seront fortement allégées pour les entreprises traitant des données personnelles.

Certains types de données demeurent soumis à un régime particulier. C'est le cas notamment des données de santé. Selon les traitements et les finalités concernés, les obligations à la charge du responsable de traitement, et les éventuelles formalités à réaliser, peuvent différer. Il est donc d'autant plus important, pour les entreprises du secteur de la santé et des biotechnologies, de bien maîtriser cet environnement.

1. UNE LOGIQUE DE RESPONSABILISATION

Alors que la directive de 1995 et la loi dite *Informatique et libertés* reposaient en grande partie sur la notion de « formalités préalables », le RGPD fonctionne sur une logique de responsabilisation des personnes traitant des données personnelles, qui doivent être en mesure de démontrer à tout moment leur conformité aux règles applicables. Les formalités préalables disparaissent ainsi en grande partie, au profit d'un certain nombre d'obligations à mettre en œuvre, en amont, par les responsables de traitement.

François-Maxime Philizot

Le devoir d'information des personnes a été fortement renforcé.

Notamment, chaque responsable de traitement doit mettre en place une série de mesures lui permettant de cartographier l'ensemble des traitements de données existant dans l'entreprise.

Le RGPD impose à ce titre la création d'un registre recensant l'ensemble des traitements effectués par l'entreprise. Si la tenue de ce registre est obligatoire pour les entreprises de plus de 250 employés, cette obligation s'applique également dans d'autres cas, et en particulier lorsque des données de santé sont collectées et traitées par l'entreprise. Une forte proportion des start-up du secteur de la santé sera donc potentiellement concernée par une telle obligation de tenue d'un registre.

Le RGPD impose par ailleurs la mise en place, au sein de l'entreprise et de façon permanente, d'un délégué à la protection des données (DPO). Différentes situations entraînent l'obligation, pour une entreprise, de désigner un DPO. À titre d'exemple, les entreprises traitant des données de santé « à grande échelle » doivent désigner un DPO. À nouveau, les sociétés en développement du secteur de la santé (biotechs, medtechs) sont potentiellement concernées. Afin de déterminer si une entreprise traite des données à grande échelle selon les termes du RGPD, il faudra s'interroger notamment sur le volume des données traitées, l'étendue géographique du traitement, et le nombre de personnes concernées par les traitements.

Dans le but de renforcer et de garantir la protection des données personnelles, le législateur européen n'a pas hésité à imposer des sanctions élevées en cas de non-conformité : les amendes pourront aller jusqu'à 20 M€ (contre 3 M€ actuellement) ou 4 % du chiffre d'affaires annuel mondial total de l'entreprise responsable du traitement, outre des sanctions pénales, ainsi qu'un risque important en termes d'image.

2. UNE PRÉCISION DU RÉGIME DES DONNÉES DE SANTÉ

Le RGPD donne une définition des *« données concernant la santé »*, qui sont par ailleurs soumises à des règles particulières. Il s'agit de *« données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »*. Il convient de faire attention à la qualification de ces données. En effet, certaines sont des données de santé par nature (comme les maladies, les résultats d'examens, ou encore les traitements médicaux réalisés), alors que d'autres le deviennent du fait de leur croisement avec d'autres données (nombre de pas, en tant que mesure d'effort, croisé avec la mesure de la tension d'une personne, par exemple), ou du fait de leur destination médicale. Le RGPD introduit également la notion de données génétiques, qui sont soumises à des restrictions similaires.

En tout état de cause, le principe reste l'interdiction de traiter des données de santé. Il existe toutefois un certain nombre d'exceptions à ce principe, dont le champ est élargi par le RGPD. Parmi elles figure la notion de traitement

réalisé pour des motifs d'intérêt public dans le domaine de la santé. Cette notion qui, sous réserve des débats au Parlement, devrait clairement inclure les activités du secteur privé (par ex. : start-up du monde de la santé – en effet, la notion d'intérêt public devrait comprendre les traitements de données visant à *« garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux »)*, permet d'offrir aux entreprises de nouvelles possibilités pour traiter des données de santé.

3. UN ALLÉGEMENT DES FORMALITÉS, Y COMPRIS POUR LE TRAITEMENT DES DONNÉES DE SANTÉ

Comme indiqué, la grande majorité des formalités disparaît, conformément à la logique de responsabilisation qui prévaut désormais avec le RGPD. Dans le secteur de la santé, la modification de la loi *Informatique et libertés* vise à poursuivre l'action menée par les autorités dans le sens d'une simplification des formalités préalables.

En ce qui concerne les traitements à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé (par ex. : essais cliniques), le principe préexistant au RGPD demeure :

(i) pour les traitements conformes aux méthodologies de référence adoptées par la CNIL, une déclaration de conformité est suffisante (une autorisation de la CNIL n'est pas nécessaire) : en pratique, ces méthodologies resteront en effet applicables (étant d'ailleurs précisé que certaines d'entre elles, telles que la MR-001 et la MR-003, sont actuellement en cours de mise à jour au regard des dispositions du RGPD) ;

(ii) pour les traitements non conformes, une autorisation de la CNIL restera en principe requise. À noter également qu'une nouvelle méthodologie est en cours de préparation : la MR-004, pour les recherches n'impliquant pas la personne humaine, relevant du CEREES (Comité d'expertise pour les recherches, les études et les évaluations dans le domaine de la santé).

Les autres traitements de données de santé (c'est-à-dire autres que ceux mis en œuvre dans le cadre de recherches) seront soumis à des principes similaires : le projet de loi crée un système de déclaration de conformité à des référentiels ou règlements types édictés par la CNIL ; ce n'est que si le traitement mis en œuvre ne répond pas à ces normes qu'une autorisation préalable devra être demandée à la CNIL (en pratique, cela devra constituer l'exception).

4. LA RÉAFFIRMATION DU CONSENTEMENT ET DE L'INFORMATION

Le consentement (qui n'était pas défini dans la loi *Informatique et libertés)* dispose désormais d'une définition. Il s'agit de *« toute manifestation de volonté, libre, spécifique, éclairée et univoque, par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement »*. Au regard de cette définition précise du consentement figurant dans le RGPD, il est recommandé de considérer que les systèmes de consentement passif ou tacite (*opt-out* ou cases pré-cochées dans des formulaires ou des e-mails) ne peuvent plus être utilisés. Pour les entreprises développant des applications dans le secteur de la santé, il s'agit d'un point essentiel. Par ailleurs, le consentement doit être éclairé, ce qui implique une information claire et précise permettant à la personne de décider en connaissance de cause d'accorder ou non son consentement pour un traitement de données.

Plus généralement, le devoir d'information des personnes concernées par le traitement a été fortement renforcé.

Agathe Simon

Les entreprises traitant des données de santé « à grande échelle » doivent désigner un DPO.

5. L'IMPORTANCE DE LA RELATION AVEC LES SOUS-TRAITANTS

Le RGPD modifie en profondeur la responsabilité des sous-traitants. Le RGPD étend aux sous-traitants des obligations imposées initialement aux seuls responsables de traitement. Dans le secteur de la santé, comme dans les autres secteurs, le recours à des sous-traitants est courant : CRO spécialisées pour la mise en place d'essais cliniques ou la réalisation d'analyses spécifiques, prestataires pour le stockage de données, agences en charge de la réalisation d'études de marchés, etc.

Avec l'entrée en application du RGPD, la formalisation de la relation avec le sous-traitant devient un aspect fondamental. La conclusion d'un contrat (ou autre acte juridique) avec le sous-traitant devient obligatoire, et le RGPD précise les clauses qui, *a minima,* doivent figurer dans ce contrat. Les entreprises doivent donc inclure dans leurs contrats avec les sous-traitants les obligations relatives à la protection des données, et notamment les dispositions listées par le RGPD, étant précisé que des clauses-types sont en cours de préparation par la CNIL.

6. TRANSFERT DE DONNÉES À L'ÉTRANGER

Enfin, le transfert de données hors de l'UE reste soumis à un certain nombre de conditions. En premier lieu, un tel transfert est possible si le pays tiers a été reconnu par la Commission européenne comme assurant un niveau adéquat de protection des données. En deuxième lieu, le transfert peut être fondé sur un mécanisme assurant des garanties appropriées : il s'agit par exemple de la mise en place d'un contrat sur la base de clauses contractuelles types édictées par la Commission européenne. En troisième lieu, sont également prévues des dérogations pour des situations particulières, dans le cas d'absence de décision d'adéquation ou de garanties appropriées. Ces dérogations sont listées dans le RGPD (à titre d'exemple, un consentement circonstancié et explicite permet un tel transfert). Un transfert de données pourra alors être mis en œuvre à condition qu'il réponde à l'une de ces conditions. Dans certains cas, une autorisation demeurera nécessaire.

En ce qui concerne le cas particulier des États-Unis, le Privacy Shield (qui a remplacé en 2016 le Safe Harbor) permet un transfert de données vers des entreprises américaines (alors même que le pays n'est pas considéré comme assurant un niveau adéquat de protection des données), sous réserve que lesdites entreprises soient préalablement inscrites sur le registre tenu par l'administration américaine listant les entreprises certifiées Privacy Shield.

Les discussions au Parlement relatives au projet de loi viendront apporter des éclairages supplémentaires à un certain nombre de points.

François-Maxime Philizot et Agathe Simon, avec Constance Hars, Mercure Avocats