LES RENCONTRES

BMI SYSTEM®

« RÈGLEMENT EUROPÉEN DE PROTECTION DES DONNÉES PERSONNELLES »

JÉRÔME MARTINEZ
Président de BMI SYSTEM

LAURENT CLERC
cofondateur de BMI SYSTEM et expert réglementaire

JEANNE BOSSI MALAFOSSE
Avocate spécialiste de la protection des données, DELSOL Avocats

Retrouvez l'intégralité des interventions dans ce premier numéro des *rencontres BMI*

DU 5 JUILLET 2017
À LA MAISON DE LA RECHERCHE

Jérôme Martinez

Président de BMI SYSTEM

Je suis ravi de vous accueillir à cette première rencontre organisée par BMI SYSTEM, sur une thématique d'actualité et qui nous concerne tous : la protection des données personnelles.

Ayant effectué toute ma carrière dans l'industrie pharmaceutique, si ce n'est que très récemment que j'ai rejoint BMI SYSTEM pour en prendre la présidence, la société ne m'était pas pour autant inconnue. **En 2011, lors de l'adoption de la loi Bertrand** instaurant l'obligation de déclarer les liens d'intérêt avec l'ensemble des acteurs du secteur de la santé, je présidais Santen France et avec mon équipe nous avons choisi BMI SYSTEM pour remplir ces nouvelles exigences réglementaires.

La **transparence** est pour le secteur de la santé plus qu'une obligation réglementaire ; elle s'inscrit dans une démarche d'éthique qui guide celles et ceux dont les activités contribuent à la mission de santé qu'elle soit publique ou privée. Ces dernières années, l'industrie pharmaceutique s'est retrouvée fréquemment sous les feux de l'information, et il nous a fallu travailler avec des décideurs politiques, économiques et médiatiques, pour redresser une image quelque peu ternie y compris pour nos concitoyens.

En 2012, il ressortait des résultats d'une étude menée auprès de 400 décideurs que si l'industrie pharmaceutique était très majoritairement reconnue pour la qualité de sa recherche, son potentiel d'innovation et sa contribution au développement économique, du fait de l'opacité et du manque de transparence qui lui étaient associés, en terme d'image elle se retrouvait classée derrière les industries automobile, pétrolière ou bancaire.

Chacun à votre niveau, vous avez mis en place les ressources nécessaires pour renforcer vos activités de transparence, les valoriser, et, aujourd'hui, alors même que **l'industrie pharmaceutique** n'est toujours pas perçue aussi positivement qu'elle le devrait et que les obligations de transparence s'étendent à l'ensemble du secteur, vous êtes vus comme une **référence** en la matière.

Depuis sa création, BMI SYSTEM a intégralement dédié ses capacités de recherche et d'innovation au développement de solutions permettant de remplir les exigences de transparence et d'éthique de l'industrie pharmaceutique. En 2008, NAYA Promotion est mis en place chez notre premier partenaire, suivi en 2009 de l'application DMOS (Diverses Mesures d'Ordre Social) puis en 2011 du module Transparence, avec toujours le même souci d'efficience et de simplicité pour des opérations complexes mais néanmoins essentielles.

Depuis le lancement de **NAYA**, la réglementation ainsi que vos besoins ont évolué. Notre engagement est de toujours être à la pointe de la technologie et de la réglementation et de travailler avec vous dans une relation de partenaire, pour vous accompagner dans la réflexion et la définition de ces besoins, pour vous apporter les conseils et solutions techniques qui répondent à vos enjeux. La mise en œuvre de la loi Sapin II et celle du **Règlement Européen pour la Protection des Données Personnelles** (GDPR) vont nous permettre d'accroître encore notre exigence de transparence et d'éthique. Une nouvelle page s'ouvre dans le développement de BMI SYSTEM et notre relation commune pour relever ces nouveaux défis.

« Depuis le lancement de NAYA, la réglementation ainsi que vos besoins ont évolué. »

Aujourd'hui, ensemble, nous allons questionner la protection des données personnelles et le tout nouveau Règlement européen. Je remercie Maître Bossi Malafosse, experte de la protection des données personnelles avec plus de 18 ans d'exercice au sein de la CNIL (Commission Nationale de l'Informatique et des Libertés), des questions de santé en qualité de secrétaire générale de l'ASIP Santé (Agence des Systèmes d'Information Partagés de Santé), et depuis peu avocate associée au cabinet Delsol, ainsi qu'experte auprès du Conseil de l'Europe. ■

GDPR Protection des données Personnelles

Laurent Clerc

Cofondateur de BMI SYSTEM et expert réglementaire

Bonjour et bienvenue. BMI SYSTEM, c'est plus de 10 années d'expertise en matière de transparence et d'éthique pour les industries de santé. Le premier logiciel NAYA était destiné à la gestion du DMOS; nous avons ensuite suivi l'évolution de la loi Bertrand puis la mise en place de la loi Touraine.

Aujourd'hui, nous offrons une large plateforme qui inclut la gestion des exigences de transparence, les demandes d'informations médicales et scientifiques ainsi que la mise à disposition des supports promotionnels.

BMI SYSTEM, c'est aussi une cellule dédiée au conseil en transparence et en éthique, tant pour la mise en place des outils, que pour le conseil et le support quotidien de vos équipes, que ce soit sur l'application destinée à la gestion du DMOS ou des exigences en matière de publication.

Enfin, **le troisième pan de notre offre est constitué par la cellule de soutien opérationnelle aux activités DMOS** Transparence qui prend en charge les aspects logistiques, tel que l'envoi de vos documents aux professionnels de santé, et au-delà, l'externalisation d'une partie du DMOS et de la Transparence.

Nos **activités ne se limitent plus** à la transparence et à l'éthique mais vont au-delà pour intégrer la lutte anti-corruption. En effet, afin de renforcer notre offre de services et forts de notre expérience de traçabilité des relations financières entre les industriels, les professionnels et les organisations de santé, nous étendons nos activités aux enjeux de traçabilité définis par la loi Sapin II, et plus particulièrement son article 25, à savoir la déclaration des liens entre les représentants d'intérêt, notamment les responsables d'affaires publiques et les représentants et décideurs publics. Les informations exigées pour garantir cette transparence seront à publier sur le site de la **Haute Autorité pour la Transparence de la Vie Publique** (HATVP).

> « BMI SYSTEM, c'est aussi une cellule dédiée au conseil en transparence et en éthique. »

Un autre grand sujet d'actualité, en relation avec l'éthique, est la protection des données personnelles et le **Règlement européen de protection des données** ou **General Data Protection Regulation** (GDPR) qui entrera en vigueur le 25 mai 2018. En France, rien que pour les entreprises du CAC 40, le montant des investissements nécessaires pour la mise à niveau de leurs systèmes afin de répondre aux exigences du GDPR devrait s'élever à 1,2 milliard d'euros, selon une étude SIA Partners 2017, soit une moyenne de 30 millions par entreprise. Les sanctions pour non-respect du Règlement pourront elles atteindre 20 millions d'euros et jusqu'à 4% du chiffre d'affaires mondial annuel.

Dans une récente étude (2017 Survey of Privacy Professionals, TrustArc / Dimensional Research 2017) menée auprès de professionnels de la protection des données personnelles basés aux USA et travaillant pour des entreprises qui devront se conformer au GDPR, **96%** des personnes interrogées considèrent que la gestion des données personnelles prendra une importance croissante au cours des prochaines années, **95%** que la technologie deviendra indispensable pour répondre à ces obligations et **97%** que le conseil et l'expertise sont indispensables pour permettre aux entreprises de gérer ces données.

96% la gestion des données personnelles prendra une importance croissante au cours des prochaines années

95% la technologie deviendra indispensable pour répondre à ces obligations

97% que le conseil et l'expertise sont indispensables pour permettre aux entreprises de gérer ces données.

De leur côté, les **éditeurs de logiciels sont confrontés à des enjeux** de data privacy by design et devront apporter la preuve que leurs logiciels intègrent les exigences du **GDPR**. Le droit d'accès des personnes à leurs données est renforcé en termes de traçabilité des demandes d'accès, et les entreprises devront apporter les preuves qu'elles ont répondu, comme il se doit, à ces demandes. Le droit à l'oubli est lui aussi renforcé. Les délais de conservation des données (droit à l'oubli) sont définis en fonction de la nécessité de les détenir, et donc de leur finalité, les outils informatiques devront donc gérer les données à caractère personnel en intégrant ce critère. Le détenteur des informations aura alors à prouver que ces données ont bien été supprimées dans les délais définis.

BMI SYSTEM finalise actuellement deux outils destinés à permettre à ses clients partenaires de répondre aux nouvelles exigences en matière de transparence et d'éthique. Le premier, destiné à la mise en oeuvre des exigences du GDPR sera présenté dès la rentrée. Il sera suivi d'un outil adapté à la traçabilité et à la publication des relations telles que définies par la Loi Sapin II.

Dès maintenant nous pouvons annoncer que notre outil de gestion des exigences du **GDPR permettra de tracer tous les traitements des données**, d'éditer un registre informatisé de ces traitements ainsi que toutes les informations qui leurs sont associées: cela concerne aussi bien l'évaluation de l'impact du traitement sur les données personnelles, que les caractéristiques de ce traitement telles que les éléments de sécurité physiques et informatiques, les informations sur les prestataires intervenant dans le traitement (éditeur de logiciel, data centers,...), et les **diverses mesures mises en oeuvre** pour faire respecter les droits concernant leur accès à leurs données à caractère personnel... De fait, notre outil gèrera les éléments qui permettront à une entreprise de démontrer qu'elle est en conformité avec le GDPR et qu'elle en maîtrise la gestion dans l'ensemble de ses filiales. ■

GDPR General Data Protection Regulation

HATVP Haute Autorité pour la Transparence de la Vie Publique

Maître Jeanne Bossi Malafosse

Avocate spécialiste de la protection des données, DELSOL Avocats

Bonsoir à tous. Je vais vous parler du nouveau règlement européen sur la protection des données personnelles. C'est un texte général sur la protection des données : il n'est pas spécifique à la santé.

Le règlement européen a été adopté le 27 avril 2016. Il est déjà entré en vigueur. Les Etats ont un certain temps pour adopter ses principes, et la date du 25 mai 2018 est citée comme celle à partir de laquelle chacun est redevable de son respect. Puisque le règlement est en vigueur, il est très important que vous intégriez déjà ses principes et ses obligations dans les projets que vous développez actuellement.

Ce règlement donne une définition de la donnée de santé, qui n'existe pas en droit français. Il se trouve que cette définition s'accorde avec les nouvelles règles d'échange et de **partage des données de santé** définies par la loi de janvier 2016. Une donnée de santé, c'est tout élément d'information rattaché à un individu de nature à décrire sa prise en charge économique, financière, médicale, biologique, quelle que soit la source de production de cette donnée. Cette définition s'accorde aussi avec la future recommandation du Conseil de l'Europe sur la protection des données de santé, qui s'apprête à fournir davantage de détails que le règlement s'agissant du traitement de ces données. ■

« Ce règlement donne une définition de la donnée de santé, qui n'existe pas en droit français. »

Les caractéristiques du Règlement européen

Un champ d'application étendu

Son champ d'application est défini de façon plus large que celui de la loi Informatique et Libertés. Il concerne tout traitement de données à caractère personnel automatisé en tout ou partie, ou non automatisé dès lors que les données sont classées selon un ordre logique. Il vise également tous les traitements effectués par les organismes et les institutions de l'Union européenne. Il concerne tous les traitements effectués par les responsables de traitement ou les sous-traitants, selon deux critères : celui de l'établissement, et celui du ciblage, alors qu'aujourd'hui, c'est le critère de moyens qui est retenu. **Le règlement va donc concerner tous les établissements établis dans l'Union européenne**, mais également ceux qui sont établis en dehors de l'Union européenne, dès lors que l'activité du responsable de traitement vise les citoyens situés sur le territoire de l'Union européenne. ■

Les principes de protection des données

Ces principes ne sont pas bouleversés par le règlement. On trouve toujours le **principe de licéité,** de loyauté et de transparence pour le traitement des données. On trouve également la notion de limitation de la finalité, mais qui correspond au concept de la finalité déterminée et légitime visé à l'article 7 de la loi Informatique et Libertés. La notion de minimisation des données collectées, qui est une application du principe de la loi française qui pose que les données collectées doivent être pertinentes, adéquates et non-excessives au regard de la finalité du traitement est également présente . La nécessité de définir une durée de conservation des données est rappelée bien sûr (car il n'y a pas de protection sans durée de conservation). Enfin, le règlement **fait état des mesures** de sécurité, qui sont fondamentales et beaucoup plus détaillées que dans l'actuelle loi française. ■

Des droits de la personne renforcés et renouvelés

Les droits des personnes sont renforcés et renouvelés. L'information est enrichie. On retrouve l'obligation d'indiquer l'identité du responsable du traitement, la finalité du traitement, les grandes catégories d'information, la durée de conservation. Le consentement est renforcé quand il est exigé, et il peut être dématérialisé. Les droits d'accès et de rectification sont précisés. Enfin, surtout, **le droit à l'oubli est consacré**. On commence à disposer de beaucoup plus de jurisprudence dans le domaine de la protection des données personnelles. En particulier, celle de la **Cour de Justice de l'Union Européenne** (CJUE) est fondamentale ; il est important de s'y référer. S'agissant du droit à l'oubli, le règlement intègre l'arrêt de mai 2014 de la **CJUE** en consacrant le droit pour tout individu de demander la suppression définitive de ses données. Cependant, ce droit à l'oubli doit se concilier avec une autre liberté fondamentale : la liberté d'information et d'expression. L'équilibre doit être trouvé entre des droits qui s'entrechoquent.

> « On commence à disposer de beaucoup plus de jurisprudence dans le domaine de la protection des données personnelles. »

CJUE Cours de Justice de l'Union Européenne

De nouveaux droits sont aussi consacrés par le règlement. Le droit à la limitation du traitement est par exemple décrit précisément : dans certains cas, la personne peut demander au responsable de traitement qu'elle souhaite qu'une donnée soit supprimée ou que son traitement soit limité. Le droit à la portabilité apparaît également. Ce droit est étendu à tous les traitements : la personne a le droit d'exiger d'un responsable de traitement qu'il transfère ses données dans un format structuré, interopérable et numérisé à un autre responsable de traitement. Le droit de porter une réclamation auprès et contre une autorité de contrôle ainsi que la reconnaissance d'un recours juridictionnel effectif contre un responsable de traitement et/ou un sous-traitant sont enfin détaillés.

Les pouvoirs de contrôle et d'enquête des autorités vont être étendus. Contrepartie de la suppression de la quasi totalité des formalités préalables, les pouvoirs de contrôle, d'enquête et d'autorisations sont élargis.

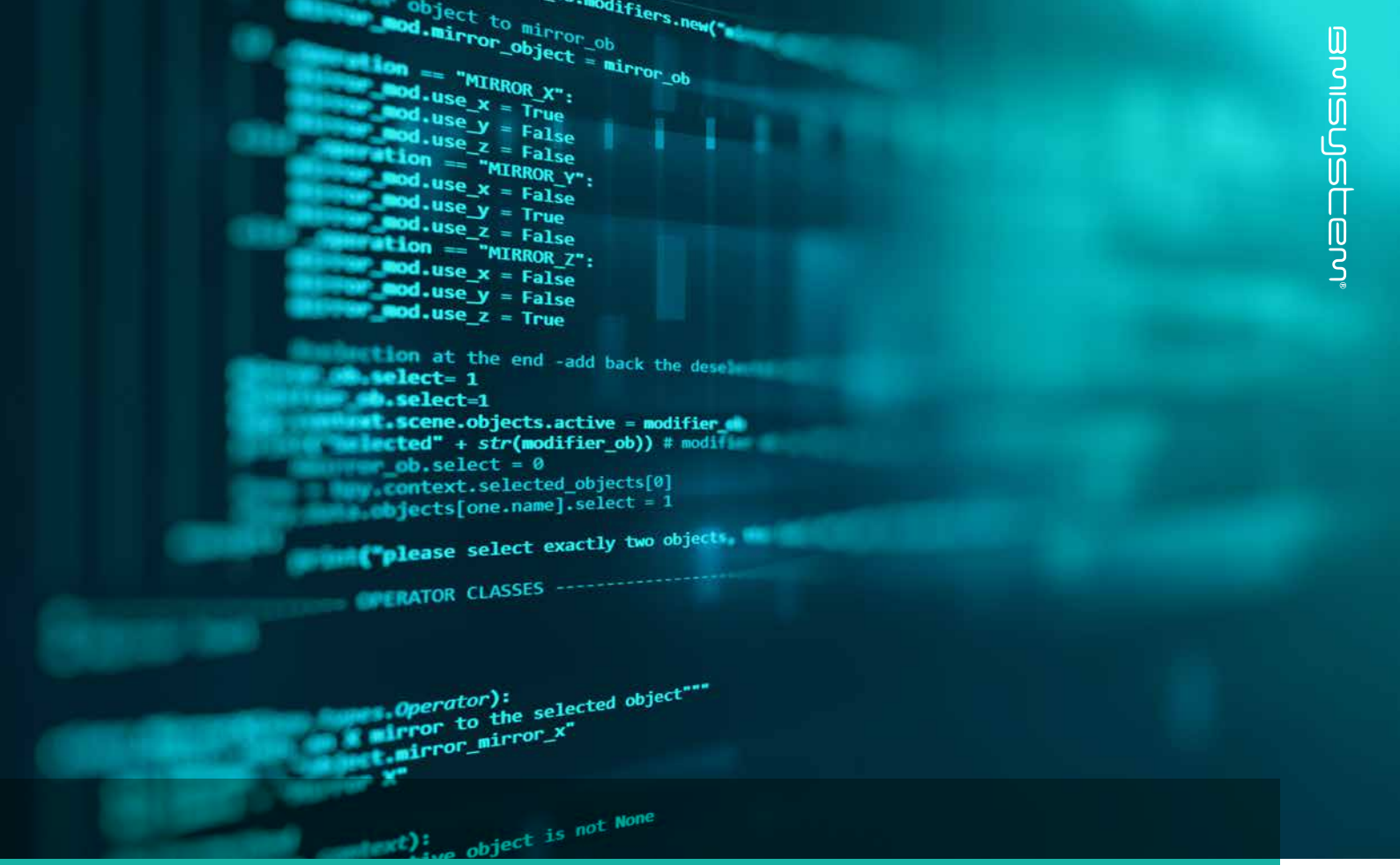
Ce règlement fait surgir des interrogations qui n'existaient pas auparavant. La conformité au règlement est désormais un processus dynamique : il doit conduire les organisations en permanence à s'assurer que les traitements restent conformes aux principes de protection des données. ■

Des sanctions accrues

Les sanctions sont accrues : en cas de non-respect d'un certain nombre de principes, les sanctions pourront atteindre **10 millions d'euros** dans la limite de 2% du chiffre d'affaires, et même **20 millions d'euros** dans la limite de 4% du chiffre d'affaires mondial si l'infraction concerne directement les droits des personnes. La CNIL s'est montrée plus sévère ces derniers temps s'agissant des sanctions qu'elle a prononcées, en particulier en les rendant publiques, ce qui peut porter atteinte à la réputation d'une organisation. La **CNIL** ne se limite cependant pas à constater les manquements au respect des principes de protection des données, elle s'attache aussi, au surplus, à prendre en considération la volonté de coopérer avec les autorités de contrôle. ■

10 MILLIONS D'EUROS
dans la limite de 2% du chiffre d'affaires

20 MILLIONS D'EUROS
dans la limite de 4% du chiffre d'affaires mondial



Le privacy by design et les nouveaux outils

Le principe d'accountability : un changement de paradigme

La conformité au règlement est commandée par le principe du privacy by design. Il s'agit d'intégrer systématiquement la protection des données personnelles à chaque projet mis en place, au même titre que les aspects financiers par exemple, et non plus de l'envisager au terme d'un projet. Cette démarche se traduit par **le principe d'accountability** qui constitue un véritable changement de paradigme : alors que jusqu'à présent, c'était la CNIL qui contrôlait la conformité des traitements à la loi Informatique et Libertés, demain, les entreprises et les laboratoires seront les contrôleurs de leurs **propres applications** et de la conformité de leurs traitements des données personnelles avec le Règlement.

« Le Règlement met à disposition plusieurs outils. »

Pour ce faire, le Règlement met à disposition plusieurs outils : la tenue d'un registre, la possibilité de consulter préalablement la CNIL si les formalités préalables ne sont pas supprimées, ainsi que la nécessité de conduire une analyse de risque et de la compléter si nécessaire d'une privacy impact assessment, une analyse d'impact permettant de définir les mesures techniques et organisationnelles appropriées pour répondre à ces enjeux.

La t**enue du registre** qui incombait jusqu'à maintenant au correspondant informatique sera demain de la responsabilité du responsable de traitement, aidé du Data Privacy Officer (DPO). Cette obligation s'applique autant au responsable du centre de traitement qu'au sous-traitant.

La **suppression** des formalités est un changement majeur. Jusqu'à présent, la protection des données passait beaucoup par l'accomplissement de formalités préalables. Le Règlement envisage la suppression quasi-totale de ces formalités avec comme corollaire l'accountability, c'est-à-dire la **responsabilisation des acteurs.**

Il restera nécessaire de consulter préalablement la **CNIL** dans certains cas, par exemple lorsque l'analyse d'impact ne permettra pas au responsable de traitement de définir lui-même les mesures à mettre en place pour assurer la protection des données. Il est aussi des cas dans lesquels le **Règlement prévoit que les Etats membres auront la possibilité d'organiser eux-mêmes la façon dont vont se déployer ces traitements,** notamment pour les missions d'intérêt public comme la protection sociale, la santé publique ou les ressources humaines qui constituent des secteurs très liés à la culture et à l'histoire du pays dont il est logique qu'ils s'organisent à l'échelle nationale. Il reste donc des domaines sur lesquels chaque Etat membre pourra conserver une mainmise. La loi Informatique et Libertés va être modifiée, le nouveau projet de loi devant être présenté au Parlement à l'automne. Nous verrons alors comment cette loi prévoit de préciser ces espaces laissés par le **Règlement**. ■

« La tenue du registre qui incombait jusqu'à maintenant au correspondant informatique sera demain de la responsabilité du responsable de traitement. »

L'étude de risques et analyse d'impact

Deux autres outils essentiels de mise en conformité sont l'analyse de risque et l'étude d'impact. Le Règlement énumère des cas dans lesquels le responsable de traitement doit conduire une étude d'impact, c'est-à-dire de procéder à une analyse de risques d'un traitement en fonction de sa finalité, de son cadre juridique, et de mettre en place les mesures de sécurité appropriées . **C'est un travail important** que les outils prévus par le règlement chercheront à faciliter.

Depuis la directive de 1995, il existe un groupement, le G29, qui rassemble toutes les autorités de protection des données de l'Union européenne, qui sera remplacé par le European Data Protection Board (EDPB), qui donne d'ores et déjà des pistes sur certaines interprétations à avoir du Règlement. Notamment, il a énuméré plusieurs critères dont la présence de deux d'entre eux qui permettent de conclure à la nécessité d'une étude d'impact, comme par exemple le cas d'un traitement qui fait appel à une nouvelle technique et collecte des données sensibles. ■

EDPB European Data Protection Board

Le principe d'accountability : de nouveaux moyens et de nouvelles mesures

Le Règlement prend aussi en compte les nouvelles capacités d'analyse des données, avec la notion de pseudonymisation et de la finalité ultérieure. **Ce sont des principes théorique**s mais qui restent importants à l'heure du Big data : disposer juridiquement des moyens permettant de faire ces études, d'analyser des données en masse y compris pour une finalité différente de celle pour laquelle les données ont été initialement collectées.

Une nouvelle obligation est la notification de la violation des données à caractère personnel à l'autorité de contrôle et à la personne concernée. Dès lors que le responsable de traitement a constaté une violation, il est tenu de la notifier aux deux parties, et d'indiquer quelles sont les mesures pour pallier cette défaillance.

Enfin, le principe du *one stop shop* ne manquera pas d'être utilisé par les organisations. Un responsable de traitement pourra désigner son autorité de contrôle de référence en fonction du lieu d'implantation de son établissement principal. Par exemple, si un grand laboratoire établit son établissement principal en France, il doit en référer à la CNIL, quelques soient ses autres moyens de traitement situés dans d'autres pays.

Le règlement vient aussi consacrer la *soft law,* qui s'est beaucoup développée dans le domaine des systèmes d'information. Partant du principe qu'il n'est pas toujours adapté d'inscrire dans la loi des mesures de sécurité qui évoluent rapidement, le règlement consacre le recours à des codes de bonne conduite, certifications ou encore labels définis par les acteurs eux-mêmes. ■

Le Data Privacy Officer

Le **Data Privacy Officer** (DPO) prend la succession du **Correspondant Informatique et Libertés** (CIL). Tous les organismes publics auront besoin d'un DPO, ainsi que les organismes privés investis d'une mission de service public. En fait, une très large majorité d'organisations se retrouveront contraintes de désigner un DPO. Le DPO sera désigné pour l'ensemble des traitements mis en œuvre par l'organisme, alors qu'aujourd'hui le CIL peut être désigné que pour une partie des traitements mis en œuvre. Le DPO peut être interne ou externe à l'organisation. Il existe une grande liberté sur la désignation du DPO. Il convient simplement de bien définir ses missions, et de garantir son indépendance vis-à-vis du responsable de traitement, ce qui pourra s'avérer difficile dans certains cas. C'est la raison pour laquelle le Règlement reste exigeant sur son rôle ainsi que ses moyens. Le DPO devra en outre disposer de suffisamment d'autorité, pour être en mesure d'imposer ses orientations.

« Tous les organismes publics auront besoin d'un DPO »

Il aura pour mission d'informer et de conseiller le responsable de traitement ou son sous-traitant, de contrôler le respect des obligations au titre de la législation, et de former le personnel. ■

CIL Correspondant Informatique et Libertés

DPO Data Privacy Officer

Les nouvelles règles de l'échange et du partage des données de santé

La **loi de janvier 2016**, modifie l'article L110-4 du code de la santé publique en élargissant de façon importante le champ du secret **professionnel**. En effet, il rappelle le droit au respect de la vie privée, et le respect du secret des informations qui s'impose à tous les professionnels intervenant dans le domaine de la santé et il définit un nouveau régime de partage des données de santé articulé autour de l'équipe de soin. Cette notion est majeure car on disposait jusqu'à présent d'un régime assez restrictif : d'un côté, un régime pour le secteur sanitaire au sein de l'hôpital, et de l'autre, le secteur médico-social qui n'avait pas de régime équivalent, ce qui empêchait dans beaucoup de cas la communication entre ces deux secteurs. Les nouvelles dispositions sur l'équipe de soin mettent fin à cette distinction et élargissent le secret professionnel médical à l'ensemble de ces acteurs. On retrouve alors la logique du parcours de soin : pour qu'il soit efficace, il faut que les acteurs se parlent et que les systèmes **d'information communiquent de manière interopérable** pour prendre le patient en charge le mieux possible.

A **côté de ce cadre juridique élargi** et qui permet d'échanger et de partager des données de santé, des référentiels de sécurité et d'interopérabilité sont définis et mis à jour par l'ASIP Santé, dont l'objectif est de garantir la qualité et la confidentialité des données à caractère personnel. Ces référentiels concernent tous les acteurs. Principalement, il s'agit de la **certification d'identité** des professionnels de santé (le répertoire partagé des professionnels de santé tenu par l'ASIP Santé), du référentiel d'identification du patient : le numéro de sécurité sociale devient l'**identifiant national de santé** (INS). L'encadrement des hébergeurs de données de santé évolue de la procédure d'agrément vers la certification. Il est enfin nécessaire de suivre les travaux sur le cadre national d'interopérabilité des systèmes d'information.

Le Règlement définit très précisément le rôle des responsables de traitements et des sous-traitants : il est donc important de revoir les contrats pour intégrer les nouvelles obligations des sous-traitants. Les **responsables de traitement** se doivent d'être vigilants quant à leurs obligations mais aussi quant à celles qu'ils mettent à la charge de leur sous-traitant. La relation entre le responsable et le sous-traitant est un processus dynamique dont le principal outil est le contrat. Il faut que ce contrat contienne les bonnes clauses qui permettent d'attirer l'attention du sous-traitant sur le respect des obligations. Si les activités sont réparties sur le territoire de l'Union européenne, cela ne pose aucun problème car tous les Etats respecteront les mêmes principes. Si les données sortent de l'Union européenne, un cadre juridique particulier est nécessaire : il faut alors s'assurer que les données transmises vont bénéficier d'une protection équivalente à celle du règlement européen.

Il est aussi important de bien comprendre les nouvelles dispositions du chapitre IX de la loi Informatique et Libertés qui concerne l'ensemble des traitements effectués à des fins de recherche, d'étude ou d'évaluation dans le domaine de la santé. Ce sont à ces nouvelles dispositions qu'il faut dorénavant se conformer. Il organise également les conditions d'accès au nouveau **Système National des Données de Santé** (SNDS) qui va réunir toutes les grandes bases médico-administratives françaises : SNIIRAM, PMSI, Causes médicales de décès et MDPH/CNSA. Une critique d'ores et déjà adressée aux nouvelles procédures d'accès à cette base est qu'elle opère une distinction entre le secteur privé et le secteur public qui n'apparaît pas dans tous les cas justifiée.

> « L'actualité est donc très riche, tant au niveau européen que national. »

L'actualité est donc très riche, tant au niveau européen que national. La protection des données personnelles est devenue un sujet important, un sujet de direction, qui doit être porté aux plus hauts niveaux de l'organisation. Il est très important de s'imprégner de ce cadre éthique et juridique pour pouvoir mener les projets le mieux possible. ■

SNDS Système National des Données de Santé

INS Identifiant National de Santé

« Malgré la complexité du sujet, Maître Bossi Malafosse a rendu le sujet de cette conférence compréhensible, vivant et dynamique, en explicitant les aspects techniques tout en intégrant les enjeux réputationnels pour les sociétés et les laboratoires. BMI SYSTEM, finalise des solutions qui permettront l'encryptage tout en garantissant le droit à l'oubli, de réaliser l'analyse d'impact, d'éditer un registre dynamique, et d'intégrer la data privacy by design dans les logiciels existants. Nous avons enfin réfléchi à la meilleure façon de protéger les données et nous pouvons assurer nos partenaires que ces données seront conservées sur le territoire sur lequel ils les stockent et les utilisent.

La mise en oeuvre du GDPR est un nouveau défi pour notre industrie, pour chacun de nous en tant que citoyen, que nous allons relever ensemble. »

Jérôme **MARTINEZ**
Président de BMI SYSTEM