Option Droit & Affaires

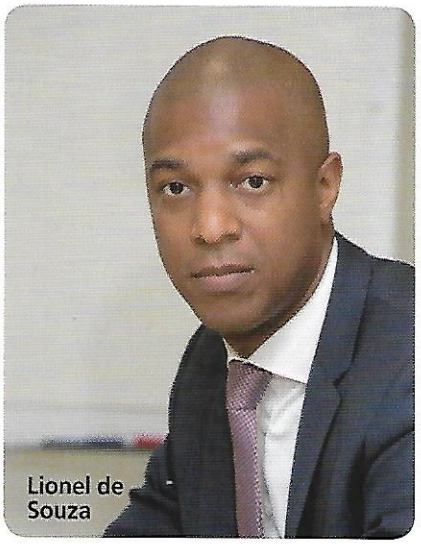
Supplément d'Option Finance n°1422 du 10 juillet 2017 et d'Option Droit et Affaires n°360 du 28 juin 2017 - ISSN / 2105-1909

LES RENCONTRES D'EXPERTS

Un supplément des magazines Option Finance Option Droit & Affaires

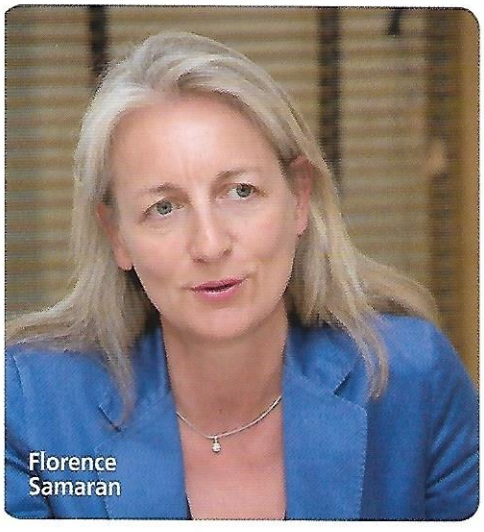

Myria Saarinen


Valérie Valais


Lionel de Souza


Frédéric Sardain

RGPD : LE COMPTE À REBOURS A COMMENCÉ


Florence Samaran


Laure Trottain


Sandrine Cullaffroz-Jover

Les tables rondes d'Option Droit & Affaires

RGPD : le compte à rebours

Photos : Gilles Danger

Le nouveau règlement européen sur la protection des données (RGPD) entrera en application le 25 mai 2018 et il devrait avoir des incidences sur la stratégie de nombreuses entreprises. Beaucoup d'interrogations demeurent sur ce règlement : l'adoption de ce texte doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Est-ce véritablement le cas ? Quels sont les points forts et faiblesses de ce règlement ? Comment mettre en œuvre l'ensemble des chantiers au sein de l'entreprise ? Quels sont les points demandant une vigilance accrue ? La réponse avec nos experts.

commencé

De gauche à droite (en haut) :
- **Myria Saarinen,** associée, Latham & Watkins
- **Laure Trottain,** responsable du département juridique Données personnelles, Sécurité et Fraudes, Orange France
- **Florence Samaran,** director of legal corporate center & France, Unibail Rodamco
- **Sandrine Cullaffroz-Jover,** directeur avocat, PwC Société d'Avocats
- **Frédéric Sardain,** associé, JeantetAssociés
- **Lionel de Souza,** DPO, Atos
- **Valérie Valais,** senior director, public affairs & corporate development, Dassault Systèmes et membre du Cercle Montesquieu

L'objectif du règlement

Valérie Valais : En quelques mots, ce règlement avait notamment comme objectif d'harmoniser les réglementations locales. Une directive sur la protection des données à caractère personnel est en vigueur depuis plusieurs années maintenant et des législations locales différentes ont été adoptées pour la transposer. Toutefois, étant donné la masse de données personnelles traitées avec l'arrivée des nouvelles technologies, il était important d'harmoniser ces législations au sein de l'Europe, notamment en termes de droits, d'obligations, de traitement de données et de sanctions, mais aussi d'augmenter la protection des individus, de renforcer leurs droits et de faciliter le libre-échange des données.

Myria Saarinen : Effectivement, la directive à laquelle vous faites référence datait de 1995 et la Commission européenne a émis la volonté de mettre à jour ce texte, puisque 1995 correspondait aux débuts de l'Internet grand public. Elle a jugé que, finalement, l'instrument juridique comportait certes l'essentiel des principes mais qu'il méritait d'être affiné. Par ailleurs, la Commission européenne souhaitait harmoniser les textes pour, disait-elle, mettre fin aux contraintes budgétaires pour les entreprises, notamment liées aux formalités auprès des autorités nationales, et qui se chiffraient à plusieurs milliards par an. En mettant en avant ce point, elle tentait bien évidemment de présenter le texte sous son meilleur jour, occultant le fait que des sanctions significativement accrues allaient suivre.

Lionel de Souza : Je pense qu'il y avait aussi une volonté de responsabiliser davantage les acteurs, comme nous pouvons d'ores et déjà le constater au niveau des engagements pris et de la manière dont ils traitent les données à caractère personnel. De plus, les sous-traitants seront réellement intégrés dans la responsabilité des obligations qui s'imposent au titre du nouveau règlement. Et puis, j'aurais tendance à dire que ce nouveau règlement vise à répondre aux défis qui ont été posés par les GAFA, c'est-à-dire les sociétés extra-européennes qui agissaient, traitaient des données personnelles de citoyens européens et affirmaient parfois qu'elles n'étaient pas soumises au règlement européen parce qu'elles n'étaient pas établies sur le territoire de l'Union européenne.

Sandrine Cullaffroz-Jover : D'ailleurs, je pense que c'est un point très intéressant à soulever parce que, sous le sceau de la conformité, les aspects économiques et la portée compétitive du règlement sont trop souvent négligés. Ce règlement renforce la position des acteurs européens dans un monde globalisé, avec des échanges mondialisés, offre une protection certaine des secteurs et des personnes concernés, ce qui induit une plus grande confiance dans l'économie numérique. Il participe aussi à positionner l'Europe comme un acteur majeur du développement de l'économie numérique dans le monde.

Laure Trottain : Il y a, effectivement, une grande question sur la territorialité du texte et l'aspect sectoriel. Mais, je voudrais également souligner le changement de paradigme dans le sens où la volonté est de placer l'individu au cœur alors que, jusqu'à présent, le système de déclaration était la base. Je suis tout à fait d'accord, la responsabilisation des acteurs est énorme d'un point de vue pratique, mais en plus il y a une réelle volonté derrière.

Florence Samaran : Cela va permettre d'élargir le périmètre des autorités de protection des données et de jouer un autre rôle au-delà des enregistrements résiduels, et des recommandations. Elles seront désormais encore plus tournées vers les entreprises, pour contrôler l'application du GDPR voire sanctionner…

Laure Trottain : Oui, d'ailleurs, il est important de noter que le niveau des sanctions est très proche de ceux constatés en concurrence par exemple. Les données personnelles et la concurrence sont deux sujets assez proches.

Sandrine Cullaffroz-Jover : En effet, l'Autorité française de la concurrence, avec son homologue allemande, a publié l'année dernière un document, justement sur les impacts du big data dans le jeu concurrentiel. Il s'agit d'un texte assez important qui, je crois, doit se lire en analyse croisée avec les nouveaux textes. Je ne parle pas uniquement du règlement européen. En France, plus récemment, la loi pour une République numérique, déjà, a fait naître un certain nombre d'obligations et puis un renforcement des sanctions.
Un autre point qui me semble important, dans ce règlement, est la prise d'acte de l'aspect tridimensionnel de la protection des données. Il ne concerne pas uniquement le juridique, mais aussi la gouvernance des données et la cybersécurité, d'où les passerelles avec d'autres textes, à l'instar de la directive NIS (Network Information Security) et du futur règlement e-privacy. Très clairement, les enjeux réglementaires du GDPR dépassent la simple conformité administrative.

Laure Trottain : Oui, il s'agit de la conformité au sens très global et c'est l'une des difficultés dans la mise en place sur les grosses structures. Arriver à agencer le juridique et la sécurité pour en faire quelque chose d'intelligible, de malléable, d'utilisable basiquement pour les opérationnels, tel est le challenge…

Florence Samaran : C'est pourquoi ne raisonner qu'en termes de conformité n'est pas l'approche la plus opérationnelle. Il est important d'utiliser ce règlement comme un outil de marketing et/ou de concurrence, car une entreprise vertueuse dans ce domaine gagnera nécessairement des parts de marché.

Sandrine Cullaffroz-Jover, directeur avocat, PwC Société d'Avocats

«Ce règlement renforce la position des acteurs européens dans un monde globalisé, avec des échanges mondialisés, offre une protection certaine des secteurs et des personnes concernés, ce qui induit une plus grande confiance dans l'économie numérique.»

Frédéric Sardain, associé, JeantetAssociés

«La logique économique du texte était déjà présente, mais demeurait embryonnaire. Le règlement transforme totalement l'essai à cet égard. Il se situe vraiment dans l'ère d'Internet, du commerce électronique et de l'explosion des réseaux sociaux.»

Laure Trottain : Il faut le penser comme un service, finalement.

Florence Samaran : Exactement.

Laure Trottain : Un service à proposer aux clients.

Lionel de Souza : C'est quelque chose que nous ressentons chez Atos. En tant que sous-traitants, les clients nous demandent aujourd'hui ce que nous mettons en place pour le nouveau règlement, si nous sommes déjà en conformité et comment nous entendons traiter cette problématique. Donc, pour nous, être en mesure de répondre est également un moyen de se positionner vis-à-vis de nos concurrents. Nous devons pouvoir indiquer la manière dont nous allons travailler avec nos clients, car il ne faut pas oublier qu'il s'agit d'un véritable travail de co-construction. A mon sens, cette collaboration à mener entre le responsable de traitement et son sous-traitant est l'un des apports majeurs du règlement. D'une part, le sous-traitant ne peut plus se cacher derrière le responsable de traitement et, d'autre part, ce nouveau texte induit une plus grande responsabilisation du responsable de traitement vis-à-vis de son sous-traitant, puisqu'il lui demande de documenter la manière dont il traite toutes les mesures de sécurité.

Une évolution nécessaire

Frédéric Sardain : Pour bien comprendre l'évolution que marque le GDPR, il convient de revenir à l'objectif et à l'origine de ce texte. Cela a été dit tout à l'heure, la Commission a notamment voulu prendre en considération l'émergence des fameux GAFA, tous américains. Google date de 1998, Apple a su renaître de ses cendres en 2000, Amazon a été créé en 1995, puis est arrivé en France en 2000, et Facebook est né en 2004. Or, comme cela a été dit précédemment, la directive 95/46/CE avait été adoptée antérieurement à l'apparition de tous ces acteurs majeurs du numérique. Bien que la directive ait été adoptée sur le fondement du principe de libre circulation des données, elle s'inscrivait plutôt dans la logique historique de la loi de 1978 de protection des individus contre les fichiers étatiques, de protection des libertés publiques contre les potentielles dérives des Etats. La logique économique du texte était déjà présente, mais demeurait embryonnaire. Le règlement transforme totalement l'essai à cet égard. Il se situe vraiment dans l'ère d'Internet, du commerce électronique et de l'explosion des réseaux sociaux. La logique n'est plus celle de la déclaration préalable des traitements aux autorités de contrôle nationales, mais celle de l'«accountability» de chaque opérateur économique. Par ailleurs, aujourd'hui, les entreprises ne travaillent plus avec un seul sous-traitant identifié. Tout est très éclaté. A l'heure du «cloud», toutes les entreprises traitent des quantités de données avec une multitude de sous-traitants. L'intérêt du règlement est qu'il va leur imposer de faire tout d'abord du «data mapping» et donc d'identifier très précisément quelles sont les données, quels sont les flux, où elles sont stockées, si elles sont transférées dans l'Union européenne ou en dehors, etc. Donc, corrélativement, le rôle du

sous-traitant, bien évidemment, est davantage mis en avant et le responsable du traitement n'endosse plus seul la responsabilité qui découlerait d'une non-conformité éventuelle.

Lionel de Souza : Je rajouterai un point pour compléter ce que vous dites. Le règlement a mis quatre ans et demi à être adopté, et six ans et demi ont été nécessaires entre le premier projet et la date de mise en œuvre. Je n'ai pas fait l'historique de la directive, mais, si elle a été adoptée en 1995, en étant optimiste, le premier projet a probablement été publié aux alentours de 1990. Je dirais presque que la magie de ce texte, c'est qu'étant neutre technologiquement, il s'applique encore, même s'il est en retard, et ce malgré l'évolution significative de l'écosystème.

Myria Saarinen : Je voudrais revenir sur ce changement d'esprit, que vous notiez tout à l'heure, entre la directive et le règlement. L'évolution est la même au niveau de la CNIL. Quand elle a été créée en 1978, elle était plutôt vue comme le garant des libertés individuelles, en se plaçant entre l'Etat et le citoyen. Aujourd'hui, ce n'est plus du tout l'essentiel de son rôle. Il ne s'agit plus pour elle de protéger le citoyen contre l'Etat, mais plutôt de protéger l'individu contre des entreprises privées qui monnayent ses données à caractère personnel comme une matière première. Comme ses autres homologues européens, la CNIL est donc devenue avant tout un régulateur économique à part entière.

Valérie Valais : Pas uniquement.

Myria Saarinen : En grande partie, oui, comme en témoignent les sanctions émises contre les GAFA qui s'inscrivent dans la régulation économique d'un secteur.

Lionel de Souza : Effectivement, leur rôle a beaucoup évolué. En 1978, nous étions à l'ère Safari et l'objectif était de protéger l'individu contre l'Etat. A partir des années 1990/95, il a aussi fallu protéger l'individu contre les entreprises, d'où la notion de régulateur économique. A l'heure actuelle, avec les dérives constatées dans certains Etats et les mesures prises sur le renseignement et sur la surveillance des individus, le rôle de régulateur vis-à-vis des Etats revient également…

Frédéric Sardain : Les textes relatifs aux données se sont multipliés, avec plusieurs strates, parce que les données traitées par les opérateurs économiques ont explosé. A l'époque, en 1978, une seule loi suffisait. Aujourd'hui, le GDPR est censé être le futur socle commun pour l'ensemble des pays de l'Union européenne. Comme vous l'avez évoqué, s'y ajoutent notamment le règlement e-privacy qui va arriver pour les opérateurs de communications électroniques, la directive NSI (Network Security and Information) de 2016, les dispositions relatives aux données personnelles dans le règlement eIDEAS (signature électronique) de 2014, ainsi que l'ensemble des textes qui seront adoptés par chaque Etat, au niveau national, afin de compléter le GDPR. Donc, dans la mesure où le volume des données explose, les textes, d'une certaine façon, se multiplient également, certains présentant davantage un angle économique, d'autres un aspect sécuritaire…

Sandrine Cullaffroz-Jover : Je rejoins ce que vous dites, particulièrement sur l'évolution du rôle de la CNIL. Aujourd'hui, elle se positionne tant en régulateur qu'en laboratoire d'idées, notamment en travaillant sur les algorithmes, sur le big data, sur l'IoT… Elle lance des consultations auprès des industries et invite à prendre part aux réflexions sur ces nouveaux sujets.

Florence Samaran : C'est certain ; elle est de plain-pied dans le business des uns et des autres et elle a une approche économique des problématiques, tout en protégeant les libertés individuelles.

Sandrine Cullaffroz-Jover : C'est ce qui est intéressant.

Florence Samaran : Elle tient ce rôle depuis quelques années.

Sandrine Cullaffroz-Jover : Elle fait un effort également dans la création de packs de conformité sectorielle, dans le dialogue et la compréhension des business models, ce qui offre une approche plus pratique de la conformité. Ces outils permettent de démystifier les textes.

Florence Samaran : Si ce n'est que leur mise en œuvre peut s'avérer un peu complexe.

Laure Trottain : Oui, parce que, comme vous le disiez, ce texte a été essentiellement pensé autour des GAFA et, en fait, les grosses entreprises arrivent bien à le cerner. A l'inverse, je pense que c'est un monstre législatif pour la TPE du coin et pour la plupart des start-ups, qui doivent être complètement démotivées et ne savent pas par où commencer.

Florence Samaran : Ces entreprises sont plus fragiles alors que plus exposées, contrairement aux nôtres, qui disposent éventuellement d'une structure dédiée, tout au moins d'équipes et en tout état de cause de process établis.

Valérie Valais : A ce titre, nos sociétés seront également plus exposées vis-à-vis des autorités, et observées attentivement par ces dernières.

Laure Trottain : C'est déjà le cas !

Sandrine Cullaffroz-Jover : Pour les petites structures, il

Myria Saarinen, associée, Latham & Watkins

«Il ne s'agit plus pour la CNIL de protéger le citoyen contre l'Etat, mais plutôt de protéger l'individu contre des entreprises privées qui monnayent ses données à caractère personnel comme une matière première.»

existe tout de même quelques dérogations, notamment pour la tenue d'un registre dans le cadre des micro, petites et moyennes entreprises comptant moins de 250 employés. Mais, je vous l'accorde, il n'y en a pas beaucoup ! Ces dérogations sont rares dans le texte, et surtout elles ne s'appliquent plus si le traitement effectué est susceptible de comporter un risque pour les droits et des libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des données sensibles, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions.

Zones d'ombre

Myria Saarinen : Le règlement comporte de nombreuses zones d'ombre ou d'interprétation qui ne sont d'ailleurs pas toutes involontaires. Certains de ces points seront réglés par le G29 dans le cadre des guidelines que ce dernier commence déjà à publier dans la perspective de l'entrée en application du règlement. Le comité européen de la protection des données prendra le relais. Nous savons aussi qu'il y pourra y avoir une granularité plus fine au niveau national, puisqu'un certain nombre de pouvoirs restent encore dévolus aux autorités de contrôle nationales. Dans certains secteurs, ces dernières pourront ainsi émettre des règles plus spécifiques, comme en matière de droit du travail ou de la santé.

Sandrine Cullaffroz-Jover : Elles sont même parfois souhaitables, notamment en ce qui concerne la neutralité technologique du texte dont vous parliez tout à l'heure. Autant les dispositions du GDPR prennent en compte les impacts de l'analytics dans le traitement des données, autant en ce qui concerne la blockchain, ou d'autres technologies un peu plus disruptives, il fallait une formalisation générale et pas trop spécifique justement pour assurer la pérennité des dispositions et laisser une marge d'interprétation et d'adaptation.

Laure Trottain : Même dans le général, le texte entre dans une granularité extrêmement fine. Regardez le niveau d'information que nous sommes censés apporter au client par catégorie de données et sur les durées de conservation. De base, nous devrions tous le faire mais, dans la mise en œuvre pratique, gérer une masse de données colossale demande une granularité et un tamis extrêmement fins, et la difficulté est de trouver le juste milieu.

Lionel de Souza : Ainsi que les outils technologiques qui sont en mesure d'extraire cette information. Aujourd'hui, des bases de données permettent de dire si nous avons des données sur telle ou telle personne. Toutefois, il faut bien être sûr que d'autres données ne traînent pas dans des systèmes fantômes et qu'elles sont effacées une fois la durée de conservation passée. Tous ces aspects technologiques viennent en surabondance et c'est un vrai challenge.

Laure Trottain : Oui, c'est une cartographie particulièrement fine et qui est assez compliquée dans la pratique.

Valérie Valais : Le plus difficile est de réaliser l'état des lieux de l'existant. Une fois ce travail effectué, il faudra mettre en place un suivi et une mise à jour régulière de la cartographie et la tâche sera donc a priori plus simple.

Florence Samaran : Il est indispensable.

Laure Trottain : Le travail de l'état des lieux en tant que tel est la brique la plus massive de l'ensemble. Après il sera, en effet, plus facile de savoir ce qu'il nous faut encore faire pour être «compliant». A partir du moment où un client nous demande de ne plus utiliser ses données, il faut savoir couper les vannes, et toutes ! Et c'est valable pour toutes les entreprises.

Lionel de Souza : Chez les sous-traitants aussi.

Frédéric Sardain : Sans doute la conformité parfaite ne sera-t-elle pas possible à atteindre. La logique du texte étant de dire que chacun doit être garant de la conformité de ses propres traitements, il faut espérer, dès lors que l'entreprise aura fait en sorte de maximiser ce qui est dans ses possibilités techniques et juridiques afin d'être conforme, que les autorités de régulation seront clémentes ou, a minima, ouvertes à la discussion.

Laure Trottain : J'aurais une petite réticence sur la clémence, étant donné le vécu d'Orange sur le sujet mais, sur le principe, je me dis que l'essentiel est d'arriver à démontrer que nous avons institutionnalisé un certain nombre de choses, ce qui permet d'avoir une documentation, une traçabilité et un contrôle. L'idée est d'être le plus près possible de l'objectif et puis surtout d'arriver à démontrer la volonté de l'entreprise, ce qui implique que ce soit aussi porté par les comex. C'est essentiel.

Frédéric Sardain : Bien sûr, il y a besoin de moyens financiers et humains. C'est très transverse.

Florence Samaran : C'est certain, il y a différents départements concernés : les directions marketing et commerciale, la direction informatique, la direction de l'audit interne, la direction juridique bien sûr…

Frédéric Sardain : Dès lors que cela peut impacter les produits ou les services fournis par l'entreprise à ses clients, qu'il faut étudier le privacy by design, dès la phase amont de conception, il faut avoir tout le monde autour de la table.

Myria Saarinen : Il faut revoir les structures et les schémas d'organisation pour s'assurer d'impliquer toutes les personnes concernées.

Sandrine Cullaffroz-Jover : D'ailleurs, pour rebondir sur ce que vous disiez, je constate, chez la plupart des clients que nous accompagnons, un effort de formalisation de la gouvernance des données pour éviter cette dilution des responsabilités entre les métiers. Par exemple, certaines entreprises n'ont pas forcément de data owner, ou de responsable par lignes de métier. Ce n'est pas le cas de certaines industries très matures car très réglementées depuis très longtemps qui ont des réflexes et des automatismes. Mais d'autres secteurs, d'autres industries, partent de plus loin et les sociétés doivent faire un effort de formalisation de la gouvernance, établir des procédures pour s'assurer que tout nouveau projet qui inclut un traitement sera porté par un comité, que le DPO sera informé, que des études d'impact seront réalisées le cas échéant.

Florence Samaran : Ce qui est intéressant, c'est la liberté qui est laissée justement pour cette gouvernance. Chaque société, comme vous le disiez, n'a pas le même historique, pas le même niveau de maturité, pas les mêmes traitements, et pas les mêmes contraintes non plus, suivant qu'elle traite des données sensibles ou un programme de fidélité, qu'elle est établie dans un pays ou plusieurs. Le règlement laisse à chaque société une grande liberté.

Laure Trottain : Oui, la mise en œuvre est très libre. En fonction des secteurs, les maturités sont très différentes. Prenons un exemple concret, avec la notification des failles de sécurité. Le secteur des télécoms a, depuis longtemps, cette obligation. Donc il est vrai que nous avons un temps d'avance, en tout cas sur cette partie-là, parce que nous avons dû mettre en place la gouvernance et les process de remontée. Nous faisons partie des secteurs qui ont beaucoup de données. Par contre, sur certains points, le règlement est quand même éloigné des mises en œuvre pratiques. Le problème est que si nous rebondissons par exemple sur les notifications, pour ne prendre que ce point, les délais qui sont donnés ne sont pas du tout pratiques. Regardez, 72 heures pour faire une notification, c'est un rêve que nous aimerions pouvoir remplir sans problème. Autre point peu pratique : les niveaux d'information qu'il faut savoir donner dès le départ à un client…

Florence Samaran : Il y a une grande liberté et des zones d'ombre, d'autant que cet exemple rentre dans le champ laissé aux pays européens qui pourront légiférer, différemment donc, sur le sujet.

Quelle méthodologie pour la mise en place de ce nouveau règlement ?

Frédéric Sardain : Sur ces problématiques, nous accompagnons des clients français ou étrangers, notamment américains, qui sont de grands groupes et qui ont déjà bien avancé dans leur réflexion. Ils viennent nous consulter le plus

Valérie Valais, senior director, public affairs & corporate development, Dassault Systèmes et membre du Cercle Montesquieu

«On fait souvent face, en pratique, à des mouvements de recul liés à un sentiment d'inconfort dans la perspective de contraintes, de travail et de ressources supplémentaires à mettre en place.»

souvent dans la phase post-data mapping, sur des points assez techniques d'interprétation du GDPR et nous demandent de prendre position sur les zones d'incertitude du texte par rapport à leur activité propre et à la méthodologie qu'ils mettent en œuvre. Donc nous proposons rarement un plan tout fait à l'avance, il s'agit essentiellement de sur-mesure.

Sandrine Cullaffroz-Jover : Nous avons trois typologies de clients pour lesquels nous sommes amenés à traiter ce genre de question. En premier lieu, nous avons, effectivement, des filiales de groupes étrangers qui sont très avancées dans leurs réflexions, et finalement l'accompagnement est ponctuel sur des points très spécifiques d'interprétation et de mise en application, à l'instar de la portabilité des données.
Nous avons également des clients qui, pour le coup, ont besoin de réaliser un état des lieux. Dans ce cas, nous proposons une démarche de diagnostic, avec une feuille de route et un plan de mise en conformité. Pour ces clients-là, nous allons d'abord préconiser de trouver un bon sponsor en interne pour que cela fonctionne, de mener une sensibilisation très en amont pour pouvoir faire adhérer les personnes au projet au sein des différentes lignes de métiers, car cela ne sert à rien de réfléchir à l'élaboration d'une feuille de route si personne n'est enclin à la mettre en application ou n'en comprend pas les enjeux. Il y a aussi un autre point qui me paraît fondamental, c'est de trouver des projets contributeurs. Ce sont des projets internes qui emportent l'adhésion, par exemple un projet déjà lancé mais qui conduit au traitement de données à caractère personnel ; il ne faut pas attendre la fin du diagnostic pour traiter le problème, traitons-le en parallèle et gagnons l'adhésion à ce moment-là pour embarquer les équipes le plus tôt possible.
Un autre point de projet contributeur, ce sont les réglementations connexes. Il y a par exemple le futur règlement e-privacy, et la directive NSI – directive sur la sécurité des réseaux et des systèmes d'information. Dans certains secteurs, la directive sur la distribution d'assurance, autrement appelée DDA, qui évoque le profilage justement, ou la directive sur les services de paiement 2 sont autant d'éléments qui peuvent servir à soutenir le projet et justement à transformer la conformité en opportunité, dans une démarche concurrentielle pour ce deuxième type de client.
Enfin, en dernier lieu, nous conseillons des clients qui viennent nous voir avec un projet précis. Le projet peut être un nouveau produit ou service qui va exploiter une nouvelle technologie comme la blockchain, ou qui va nécessiter l'intégration d'une plateforme IoT ; le client va devoir faire dès le commencement du privacy by design, il va donc rechercher un accompagnement juridique. De l'accompagnement sur la portée des obligations du GDPR,

Laure Trottain, responsable du département juridique Données personnelles, Sécurité et Fraudes, Orange France

«Le travail de l'état des lieux en tant que tel est la brique la plus massive de l'ensemble. Après il sera, en effet, plus facile de savoir ce qu'il nous faut encore faire pour être "compliant".»

sur les aspects juridiques des spécifications fonctionnelles, mais aussi sur la contractualisation avec les prestataires tiers en vue de négocier des clauses juridiques plus ou moins contraignantes, afin d'obtenir une répartition cohérente des responsabilités et des obligations de chacun et des garanties en phase avec ce qu'exige le règlement européen.

Frédéric Sardain : S'agissant d'un aspect très pratique, le directeur juridique d'une banque européenne m'indiquait l'autre jour, lors d'un séminaire à Vienne, que la première chose qu'il avait faite était de donner un nom à son projet de mise en conformité, pour qu'il puisse être mieux approprié par les équipes en interne. Il m'indiquait qu'à défaut, la direction générale ne sait pas trop de quoi vous parlez et ne saisit pas l'intérêt des e-mails sur le sujet.

Laure Trottain : Oui, d'ailleurs pour s'approprier un projet, il y a un travail de formation et de sensibilisation assez colossal, tout autant que la partie technique, de gestion, etc. Il faut faire comprendre à l'intégralité des salariés, qu'ils soient ou non en face des clients, les termes de cette nouvelle réglementation et à quoi elle va leur servir dans leur métier. De fait, il faut faire des déclinaisons de formation en fonction des typologies de métiers concernés. Par exemple, un vendeur en boutique ou quelqu'un qui reçoit des clients au téléphone doit posséder un vernis.

Myria Saarinen : La formation et la sensibilisation vers le bas sont effectivement nécessaires. Vers le haut, elles le sont tout autant, si ce n'est plus. Il n'est pas rare que la première étape de la préparation au règlement consiste à informer le management des enjeux de ce nouveau texte, pas seulement sous l'angle des sanctions mais aussi sous celui des avantages concurrentiels qu'il peut présenter. Le rôle de l'avocat est alors recherché pour sa qualité de tiers à l'entreprise pouvant porter par essence une parole plus libre, qui sera plus écoutée par la direction. Ainsi, convaincre le management de l'importance du texte permet ensuite de débloquer les moyens financiers et humains nécessaires à la mise en conformité avec le texte.

Valérie Valais : L'aspect humain est important. Comme dans tous les projets d'envergure, il faut une adhésion forte du comex et de toutes les personnes qui auront à traiter des données. Pour ce qui concerne la mise en œuvre du règlement, je souhaiterais ajouter que, dans notre groupe, nous avons travaillé sur un plan d'actions dès la sortie du projet de règlement en décembre 2015 et avons donc, dès cette date, réfléchi aux implications que ce règlement pourrait avoir sur toutes les divisions et les directions concernées dans le groupe. Dès le départ, le comex a ainsi été informé et impliqué. A l'instar d'autres projets conduisant à des changements au sein des entreprises, on fait souvent face, en pratique, à des

mouvements de recul liés à un sentiment d'inconfort dans la perspective de contraintes supplémentaires, de travail supplémentaire et de ressources supplémentaires à mettre en place. Mais cela est temporaire si l'on prend le temps nécessaire pour expliquer les nouvelles réglementations qui s'imposent à nous et pour obtenir l'adhésion des personnes au projet afin que celui-ci soit un succès.

Florence Samaran : C'est aussi une telle opportunité en termes économiques, c'est la raison pour laquelle je trouve qu'on ne peut pas parler de résistance.

Valérie Valais : Oui, c'est un passage obligé qui ne donne aucun choix, mais il faut aussi démontrer quels sont les bénéfices de ce travail. J'en ai parlé avec beaucoup de représentants d'entreprises au sein du cercle Montesquieu et il serait utopique de penser qu'à partir du moment où nous avons démontré la valeur ajoutée d'une telle réglementation, les entreprises achètent cet argument et sont prêtes à mettre immédiatement à disposition toutes les ressources et l'argent nécessaires. Non, nous savons que cela ne se passe pas ainsi dans la vraie vie. Pour autant, nous savons aussi que la mise en conformité de nos entreprises à ce règlement est un avantage compétitif et que les entreprises qui seront prêtes en mai 2018 seront plus compétitives que les autres. Elles pourront réduire les risques liés à un usage impropre des données à caractère personnel qu'elles traitent et réduire les risques liés à leurs propres responsabilités, fournir des produits et services conformes à la législation, et démontrer ces actions à leurs clients qui seront ainsi rassurés. La confiance pourra ainsi perdurer ou s'instaurer dans le cadre d'une relation gagnant-gagnant avec le client. Toutefois, le plan d'actions est dense, nous avons deux ans pour le mettre en place et il y a énormément de travail à faire pour atteindre cet objectif. Mais vous avez raison, une adhésion de tous est fondamentale et nous devons former tous ceux qui auront à traiter les données.

Laure Trottain : Oui, c'est un gros travail de sensibilisation pour pouvoir comprendre l'utilisation des outils qui permettent de tracer et de documenter, de pouvoir expliquer. Il faut aussi que cela devienne un réflexe pour toutes ces personnes de se dire que, quand elles auront un projet, il faudra qu'elles passent par tel outil s'il a été mis en place et que ça devienne quelque chose qui soit assez inhérent au lancement d'offre par exemple, ou à autre chose.

Valérie Valais : Vous parlez là de données personnelles. Mais l'intérêt que j'y vois également, c'est que la gouvernance qui va être mise en place pour le traitement des données personnelles pourrait également être mise au service du traitement de n'importe quel type de données, telles que les données industrielles. Il serait donc judicieux de mettre en place des process de gouvernance pour le traitement de toutes les données. C'est d'autant plus crucial à l'heure actuelle où la valeur économique des données, notamment celle des données industrielles, est un sujet majeur pour toutes les entreprises.

Laure Trottain : Nous revenons à ce que vous disiez sur la valeur économique. Plus les données sont protégées, plus il est possible d'utiliser le savoir-faire acquis comme du marketing basé sur la qualité d'opérateur de confiance, quel que soit le secteur d'activité. D'un point de vue économique, il y aura nécessairement des ressentis car le client n'est pas du tout indifférent à la question.

Florence Samaran : Certainement, et parce que dans la réalité, quand le plan d'actions et la gouvernance mise en place passent par la prise en compte des intérêts et contraintes des uns et des autres, l'adhésion se fait naturellement. C'est la raison pour laquelle, pour une plus grande efficience, toutes les parties prenantes doivent être intégrées au projet pour élaborer les solutions ensemble. C'est pour cela qu'il y a peut-être un problème initial d'adhésion, mais, en même temps, il me semble assez inhérent, comme vous le disiez, au projet lui-même. Mais ce n'est que par l'intégration des parties impactées qu'émergeront les solutions les plus adaptées, sur le mode de gouvernance, la sécurité…

Laure Trottain : C'est fédérateur dans les entreprises, dans le sens où il permet un croisement des métiers qui ne se serait peut-être pas fait.

Florence Samaran : Ce n'est pas du top-down.

Lionel de Souza : C'est de la co-construction, c'est-à-dire faire évoluer les process en interne. Forcément, quand nous faisons du privacy by design ou que nous réfléchissons à la manière dont nous allons documenter les instructions du client, que nous nous assurons que nous nous conformons bien aux instructions du client, nous nous réinsérons dans les process en fait. C'est là qu'est tout le sel de cet exercice. C'est d'arriver à co-construire avec les équipes opérationnelles qui souvent nous voient comme mettant en place des limites et contraintes dans le développement de l'activité. Et, au moment où nous leur annonçons que nous nous réintégrons dans leurs process, plutôt que de leur dire comment il faut faire, demandons-leur comment faire en sorte que les choses avancent de manière constructive et que nous soyons en conformité. Faire du data protection by design représente un coût dans le développement, dans la construction des offres. Nous devons arriver à créer et définir quelque chose ensemble, et c'est beaucoup plus efficace et beaucoup moins contraignant au final.

Florence Samaran : Et là où cela devient palpitant, c'est pour une société européenne comme la nôtre, présente dans 11 pays, et qui a dû envisager ce projet comme projet paneu-

ropéen ! Non seulement, il y a des zones grises parce que le règlement n'est peut-être pas très défini sur un certain nombre de sujets, mais, en plus, nous savons que nous allons rencontrer les zones grises des éventuelles législations locales. Par exemple, nous travaillons à l'heure actuelle sur un consentement uniformisé, tout en restant en veille de la Suède à l'Espagne, en passant par l'Allemagne et l'Autriche, sur des spécificités locales éventuellement à venir.

Frédéric Sardain : C'est un des objectifs ratés du règlement.

Laure Trottain : Raté, je ne suis pas tout à fait d'accord, il est compliqué mais offre des avantages.

Frédéric Sardain : A la place de la directive, le règlement se voulait un texte d'harmonisation et d'application directe, sans différence d'interprétation d'un pays à un autre. Nous nous retrouvons effectivement avec un règlement, mais il y a quand même une cinquantaine de dispositions dans le texte qui vont permettre aux législateurs nationaux d'adopter des points de vue qui potentiellement sont différents. Nous étions censés avoir une autorité de contrôle «one stop shop» avec un principe simple désignant l'autorité compétente comme étant celle du pays de l'établissement principal au sein de l'Union, mais nous nous apercevons qu'en pratique, cela va être beaucoup plus complexe à mettre en œuvre.

Florence Samaran : Mais à ce stade, sans visibilité, il ne faut préjuger de rien !

Frédéric Sardain : On aurait tout de même pu espérer qu'avec un règlement, d'application directe et obligatoire dans tous les Etats membres (donc sans lois de transposition nationales), les choses seraient plus simples, que nous aurions la même chose dans tous les pays, ce qui aurait été formidable. Visiblement, ça ne sera pas le cas.

Florence Samaran : C'était un vœu pieux, mais je trouve globalement l'entreprise réussie et le règlement assez achevé, sauf certains sujets évidemment.

Frédéric Sardain : Les conditions de validité du consentement des personnes, par exemple, constituent un point très important sur lesquels les différentes législations nationales pourront varier, ce n'est pas un point de détail.

Florence Samaran : Je ne peux qu'être d'accord.

Myria Saarinen : Très clairement, le règlement impose aux entreprises de revoir la manière dont les business units et les fonctions travaillent entre elles pour s'assurer du privacy by design et de l'accountability de bout en bout.

Lionel de Souza : Nous voyons dans les appels d'offres qui évoluent forcément ne serait-ce que la question de la coresponsabilité du traitement. La question qui peut se poser est également celle de la création d'un «marché» dans la coresponsabilité de traitement. En fonction du rôle qu'un sous-traitant pourrait prendre vis-à-vis d'un responsable de traitement, il pourrait s'impliquer plus ou moins dans la manière dont sera mis en œuvre le traitement de données à caractère personnel, les durées de conservation, les mises en œuvre, etc. Et, dans la répartition des rôles, plus le responsable de traitement prendrait de responsabilités et plus il deviendrait coresponsable du traitement et partagerait la responsabilité. Au final, cela peut être aussi une question de positionnement pour certaines offres.

Myria Saarinen : Pour ma part, de plus en plus de mes clients agissant en tant que responsable du traitement sont dans la situation de négocier et conclure dès aujourd'hui des contrats dont la durée ira au-delà de mai 2018 et de l'entrée en application du règlement. Ils me demandent s'ils peuvent déjà mettre des clauses qui sont conformes au règlement, plus précisément à l'article 28 du règlement relatif à la sous-traitance. Je leur réponds oui ! Il faut arriver à les négocier immédiatement quitte à prévoir qu'elles n'entreront en vigueur qu'en mai 2018. Il est important de poser cette exigence dès aujourd'hui, y compris au stade de l'appel d'offres, car cet élément doit constituer un élément pertinent dans le choix du prestataire. C'est sur cette base-là que j'invite mes clients à comparer et à juger les offres qu'ils reçoivent.

Lionel de Souza : C'est une vraie difficulté pour les sous-traitants, parce qu'on attend d'eux qu'ils soient déjà en conformité.

Valérie Valais : C'est vrai, dans les négociations, de nombreux clients souhaitent que leurs co-contractants s'engagent à être conformes au nouveau règlement dès maintenant. Or, même si ces entreprises y travaillent activement, elles ont souvent encore besoin de temps pour mettre en œuvre toutes les mesures prévues afin d'atteindre le niveau de conformité requis sur tous les points traités par le texte.
En fait, ce qui est assez intéressant dans ce règlement, c'est que, contrairement à certaines réglementations qui passent un peu à la trappe ou dont le commun des mortels n'entend pas beaucoup parler, tout le monde en a connaissance. Ceci est notamment dû au fait que ce nouveau règlement nous touche tous en tant qu'individus.

Laure Trottain : Le fait que tout le monde en entende parler peut entraîner une difficulté. Il y a énormément d'articles sur le sujet, il y a une sensibilité des clients, des prospects, de manière générale des individus sur leurs données. Un écart peut alors se creuser, nous pouvons déjà le constater car, malgré une formation, même universitaire, nous ne sommes pas tout à fait certains que les juges possèdent une connaissance aussi globale que nous qui sommes les acteurs du sujet.

Florence Samaran, director of legal corporate center & France, Unibail Rodamco

«Ne raisonner qu'en termes de conformité n'est pas l'approche la plus opérationnelle. Il est important d'utiliser ce règlement comme un outil de marketing et/ou de concurrence.»

Sandrine Cullaffroz-Jover : L'expérience et la spécialisation permettent d'appréhender de mieux en mieux les sujets. En matière de contentieux informatique ou sur la communication d'identification de personnes concernées sur la base d'adresses IP par exemple, pour ne prendre que ces cas-là, je trouve justement que les juges sont de plus en plus aguerris.

Myria Saarinen : Il y a en réalité une multitude de juges qui interviennent en matière de données à caractère personnel. Les décisions de la CNIL relèvent du Conseil d'Etat qui n'est pas nécessairement aguerri à la matière. En cas d'actions par les individus eux-mêmes, c'est le tribunal de grande instance ou d'instance qui traite l'affaire. En sus, il peut aussi y avoir des actions au pénal, ce qui requiert que le juge pénal soit également familier de la matière. En somme, il y a une multitude de juridictions qui sont concernées et qui doivent disposer d'une connaissance solide en matière de données à caractère personnel.

Laure Trottain : Sur le plan pénal, il va aussi y avoir un travail de pédagogie.

Valérie Valais : Comme cela est le cas dans tous les domaines d'expertise.

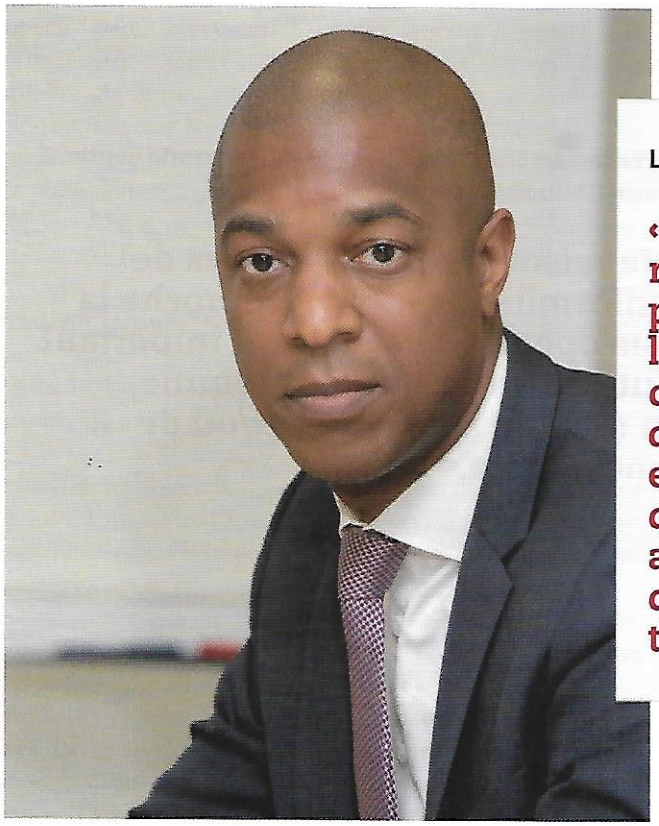
Frédéric Sardain : A terme, il n'est pas exclu qu'il y ait peut-être une spécialisation de certaines juridictions, soit administratives, soit pénales, en droit des données. Quand vous avez des dossiers énormes de contrefaçons de brevets, il faut des juges qui soient un peu spécialisés parce que c'est très technique et c'est ce qui a été fait avec la création de la troisième chambre du TGI de Paris. Si le volume des contentieux explose, vraisemblablement cela se fera aussi pour les données personnelles.

Sandrine Cullaffroz-Jover : La création au sein du parquet financier d'une cellule cybercriminalité illustre bien cette tendance vers la spécialisation des magistrats.

Laure Trottain : Nous pouvons envisager une spécialisation de certaines chambres à un moment donné.

Le DPO

Sandrine Cullaffroz-Jover : Le DPO doit être capable d'appliquer la règle de droit, de comprendre l'environnement technique du traitement, et de mettre en musique le tout à l'aide de mesures organisationnelles, c'est un chef d'orchestre dont la diversité des compétences peut être difficile à trouver aujourd'hui. Il lui faut des relais.



Lionel de Souza, DPO, Atos

«Ce nouveau règlement vise à répondre aux défis qui ont été posés par les GAFA, c'est-à-dire les sociétés extra-européennes qui agissaient, traitaient des données personnelles de citoyens européens et affirmaient parfois qu'elles n'étaient pas soumises au règlement européen parce qu'elles n'étaient pas établies sur le territoire de l'Union européenne.»

Lionel de Souza : Je ne vais pas vous mentir en vous disant que je suis un expert de la technique parce que je suis un avocat, et je reste persuadé que le DPO n'agira en fait jamais tout seul, et qu'il doit s'appuyer sur une organisation. Nous avons aujourd'hui une organisation de protection des données personnelles qui regroupe à peu près 80 personnes dans le monde et qui s'appuie sur deux jambes, une juridique et une sécurité. Ce qu'on appelle les DPO, chez nous, ce sont les membres de l'organisation sécurité et les DPLE (legal expert) proviennent du département juridique. C'est la combinaison de ces deux fonctions qui permet justement de répondre aux problématiques à la fois juridiques et techniques. Les personnes qui ont cette double capacité doivent «apprivoiser», c'est le mot que j'ai envie de dire, le règlement pour en faire quelque chose qui soit compréhensible et lisible par des opérationnels. De notre côté, nous sommes arrivés à faire une représentation graphique pour indiquer, par exemple, quelles sont les exigences, d'un point de vue sécurité.

Florence Samaran : Faites-vous les audits vous-mêmes, ou passez-vous par un autre département, l'audit interne par exemple ?

Lionel de Souza : nous avons deux types d'audits. Les auditeurs internes agissent régulièrement, et, par ailleurs, nous faisons des audits tous les ans, ce qui fait partie de nos engagements au titre des BCR («binding corporate rules»). Nous avons donc différents courants de contrôles que nous devons réaliser annuellement et tous les trois ans nous réalisons un audit interne global.

Laure Trottain : Nous, c'est semblable, nous avons des auditeurs internes et un lien avec tout ce qui est compliance officer aussi et nous avons également des audits purement sécurité qui sont effectués par des entreprises spécialisées.

Lionel de Souza : C'est une organisation matricielle, au final, tout se regroupe un petit peu entre les audits externes et les audits internes avec la sécurité et l'IT. Il y a tout un maillage qui est fait au plus fin pour éviter la déperdition avec ce qu'on appelle les divisions, les différents types de service. Donc, je ne travaille pas tout seul, mais dans une organisation qui tourne et qui permet d'aborder tous les aspects.

Laure Trottain : Ce qui nécessite en termes d'organisation de repenser globalement les schémas. Pour un sujet comme le nouveau règlement, il faut être multimétier et multidomaine. Il faut savoir écouter les besoins des uns et des autres pour se replacer dans la chronologie des étapes. ■

Propos recueillis par Lucy Letellier
et Coralie Bach