RGPD, winter is coming

Table ronde animée par Ondine Delaunay

Reportage photographique : Mark Davies

Alors que l'on a fêté, le 25 mai dernier, l'anniversaire de l'entrée en vigueur du Règlement général sur la protection des données (RGPD), les entreprises sont-elles enfin parvenues à se mettre en conformité avec le texte ? Comment font-elles face à un droit en construction alors que des incertitudes demeurent sur l'interprétation des dispositions et sur les positions de la CNIL ? Dans un environnement pour le moins anxiogène, les premiers contrôles sont désormais lancés. État des lieux.

Grégoire Hanquier, Directeur Juridique Europe, Afrique & Moyen Orient – LexisNexis SA, **Stéphane Larrière**, Group Head of Data Privacy and Data Governance, Atos, **Éric Barbry**, Associé, Racine Avocats, **Emmanuelle Bartoli**, Group Data Protection Officer - Group Legal Department, Capgemini, **Jeanne Bossi Malafosse**, Associée, Delsol Avocats, **Bertrand Liard**, Associé, White & Case, **Darine Fayed**, Head of legal et DPO, Mailjet, **Philippe Debry**, Avocat, Directeur associé, Fidal.

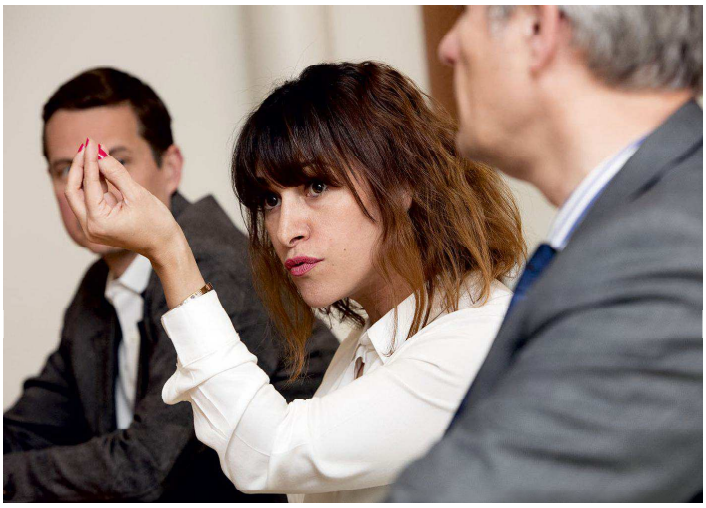
L'appréhension des réformes

Jeanne Bossi Malafosse : Le cadre juridique de la protection des données personnelles a été bouleversé par le RGPD, entré en application il y a un an. La loi du 20 juin 2018 puis l'ordonnance du 12 décembre 2018 sont venues préciser et réécrire la loi informatique et liberté, dont nous aurons une nouvelle version le 1er juin prochain. Survenues en six mois, ces deux modifications de la loi du 6 janvier 1978, qui a fixé le cadre de la protection des données en France pendant 40 ans, ne sont pas source de sécurité pour les acteurs. Mais il convient de rappeler que c'est d'abord le RGPD qu'il faut prendre en compte et qui est d'application directe en droit interne et que, finalement, il n'a pas tant révolutionné les grands principes de protection des données. Le texte national, notre nouvelle loi informatique et liberté vient en soutien du RGPD pour préciser certains aspects ou pour ajouter au cadre européen dans certains secteurs, comme celui de la santé par exemple.

Philippe Debry : Les entreprises étaient déjà sensibilisées à la protection des données, mais la véritable prise de conscience de l'enjeu du RGPD a été progressive. Elle s'est révélée très différenciée suivant les métiers, les tailles ou la localisation géographique de l'entreprise. Il est donc difficile d'avoir une application homogène, quels que soient l'entreprise et les enjeux liés à son métier. C'est un souhait du marché d'avoir une sorte de guide par filière permettant de s'assurer que les thématiques communes, activité par activité, sont traitées de façon homogène.

Bertrand Liard : La date d'entrée en vigueur définie à l'issue d'un processus législatif sans lien avec les réalités des entreprises n'a pas aidé à cette prise de conscience. En effet, le cycle budgétaire des grands groupes pour les dépenses de l'année N se termine au plus tard en octobre

ou novembre de l'année N-1. Très peu d'entreprises ont préparé en 2015 un programme de dépenses sur 2016, et à peine plus en 2016 pour 2017. Le cas le plus fréquent a été la réalisation en 2017 des études d'impact permettant une prévision budgétaire de mise en conformité sur 2018. La CNIL a néanmoins rassuré le marché en annonçant qu'elle ne sanctionnerait le respect des nouvelles obligations (celles qui n'étaient pas déjà prévues dans la loi de 1978) qu'à partir de 2018. En pratique, la plupart des entreprises n'ont donc réellement eu qu'une année de préparation. Assez logiquement, on constate encore aujourd'hui que tout n'est pas prêt dans toutes les entreprises.



Emmanuelle Bartoli,
Group Data Protection Officer - Group Legal Department, Capgemini

Grégoire Hanquier : À l'été 2017, il y a eu une avalanche d'articles de presse tous les plus anxiogènes les uns que les autres. Les entreprises n'avaient plus de budget, mais elles ont pris conscience qu'elles devaient se mettre en conformité. Mais une question s'est rapidement posée : à qui confier cette tâche ? Le directeur juridique a tout de suite été désigné. De qui devait-il alors s'entourer ? Du marketing ? De la DSI ? Ils étaient déjà débordés et il était alors difficile de faire avancer les projets… Finalement, la véritable prise de conscience a été l'annonce du montant de l'amende : 4 % du chiffre d'affaires mondial. Les groupes se sont alors décidés à rapidement réagir, dans un compte à rebours, avec deux solutions : internaliser la fonction ou faire appel à des ressources extérieures.

Emmanuelle Bartoli : Capgemini étant un acteur majeur en IT, la protection des données personnelles a toujours été une priorité. La prise de conscience sur le sujet a été réalisée très en amont du RGPD. Un groupe de travail appelé « projet RGPD » a été mis en place en interne. Il a réuni les différentes parties prenantes nécessaires à la définition d'un plan d'actions, afin d'être prêts pour l'entrée en vigueur du RGPD. Au-delà de la définition des politiques groupe régissant la protection des données, le travail de mise en œuvre effective des politiques et de process est une tâche au long cours qui ne s'arrêtait pas avec la date butoir du 25 mai 2018.

Éric Barbry : L'appréhension du RGPD diffère en fonction des entreprises et de deux facteurs principaux : le niveau de maturité de l'entreprise d'une part et la volonté de ses dirigeants d'autre part. La maturité de l'entreprise au droit des données personnelles est un facteur facilitateur ou aggravant selon que l'entreprise, avant le RGPD, était conforme à la loi de 1978. Pour celles qui l'étaient, la marche pour passer au RGPD était petite ; pour celles qui n'étaient déjà pas conformes au RGPD, le texte est un tsunami juridique,

organisationnel et technique. La volonté des dirigeants est le second facteur clé, car la mise en conformité au RGPD implique des changements et des budgets. Or, nombre d'entreprises, même dotées de DPO particulièrement compétents, ne se sont pas donné les moyens de se mettre en conformité avec le RGPD.

Grégoire Hanquier : Les tâches à accomplir étaient tellement importantes qu'il a fallu prioriser : d'abord multiplier auprès de l'ensemble des collaborateurs des formations dédiés par type de métiers afin de faciliter la mise en œuvre et l'adhésion et, en parallèle, consolider – à la lumière du RGPD – les engagements RGPD de nos entreprises vis-à-vis de nos clients, fournisseurs et salariés.

L'indispensable pédagogie

Philippe Debry,
Avocat,
Directeur
associé, Fidal

Emmanuelle Bartoli : Le sujet de la protection des données personnelles a longtemps été considéré comme un sujet facile – presque le parent pauvre du droit, souvent associé à de simples formalités administratives. En réalité, pour qui prend la peine de se plonger dans ce sujet, on en découvre vite toutes les subtilités. La protection des données étant une affaire d'interprétation et d'évaluation du risque, une connaissance approfondie du sujet est requise, en même temps qu'une expérience pratique de la matière. On lit trop souvent des approximations ou des erreurs. La pédagogie est ainsi un pilier essentiel d'un programme de conformité RGPD. Ce dernier précise d'ailleurs qu'il va falloir continuer à faire de la pédagogie sur le long terme. Cette approche est nécessaire, puisque les acteurs au cœur de la protection des données ne sont pas les experts du sujet, mais bien les salariés qui sont amenés à traiter les données personnelles au quotidien, sans parfois s'en rendre compte.

Darine Fayed : La CNIL, ou d'autres autorités de contrôle comme l'ICO en Grande Bretagne, avaient, au début, un rôle d'accompagnement pour donner les règles clés, diffuser des guidelines, et aider à interpréter les textes. Elles étaient LA source sûre pour vérifier les bonnes pratiques, face à une avalanche de fausses informations.

Jeanne Bossi Malafosse : La CNIL a toujours privilégié le conseil, mais ce rôle est encore accru avec les dispositions du RGPD et ce fameux principe d'accountability qui invite chacun à organiser lui-même sa propre conformité, et donc à se référer aux travaux de l'autorité de protection des données pour être éclairé. Le texte sur ce point oblige aussi la CNIL à adapter ses méthodes de travail.

Grégoire Hanquier : Je regrette néanmoins que ces guides pratiques aient été publiés si tard. En outre, ils ont été publiés en anglais au départ, ce qui s'est révélé être une difficulté pour certaines PME ne disposant pas de ressources. Aujourd'hui, la plupart des lignes directrices sont publiées sur le site de la CNIL.

Éric Barbry : La pédagogie est aussi une affaire de budget et, là encore, les distorsions sont majeures entre les grandes entreprises, les ETI et les PME/PMI. Les grandes entreprises ont les moyens de mettre en œuvre de véritables plans de formation, certaines se lancent dans des MOOCs, d'autres dans des *serious games*… Mais ces grandes entreprises ne sont pas légion. À plus de 95 %, le

tissu économique français est constitué de petites et moyennes entreprises. Comment imaginer qu'elles puissent dégager du temps et de l'argent pour de la formation au RGPD alors qu'elles peinent à survivre ? J'avais beaucoup d'espoir dans le Guide de la CNIL à destination des petites et moyennes entreprises, mais le document se contente de rappeler le RGPD sans tenir compte des contraintes économiques de cette cible. Pour moi, le RGPD est un texte qui ne tient pas compte de cette réalité économique. Il aurait sans doute dû être adapté aux tailles des entreprises.

Philippe Debry : J'ai été frappé par le temps que nous avons passé à faire comprendre. Nous pensions naïvement que les fondamentaux de la loi de 1978 constituaient un acquis, mais, concrètement, il a fallu revenir aux bases. Qu'est-ce que la donnée personnelle ? Qu'est-ce qu'un traitement ? Quels sont les droits des personnes concernées ?

Éric Barbry : Nombreux étaient ceux qui pensaient que le consentement serait la nouvelle règle. Faux et archifaux ! Le consentement n'est pas l'alpha et l'oméga du texte ! Il a fallu se battre pour faire comprendre ce point. Il a également fallu expliquer, et expliquer encore, que l'obligation d'information n'était pas limitée aux seuls clients, mais que les salariés eux aussi devaient être informés sur la manière dont l'entreprise traite leurs données – une longue évangélisation des DRH. Et je ne parle pas des trésors d'imagination qu'il a fallu déployer pour convaincre les entreprises de traiter le cas par-

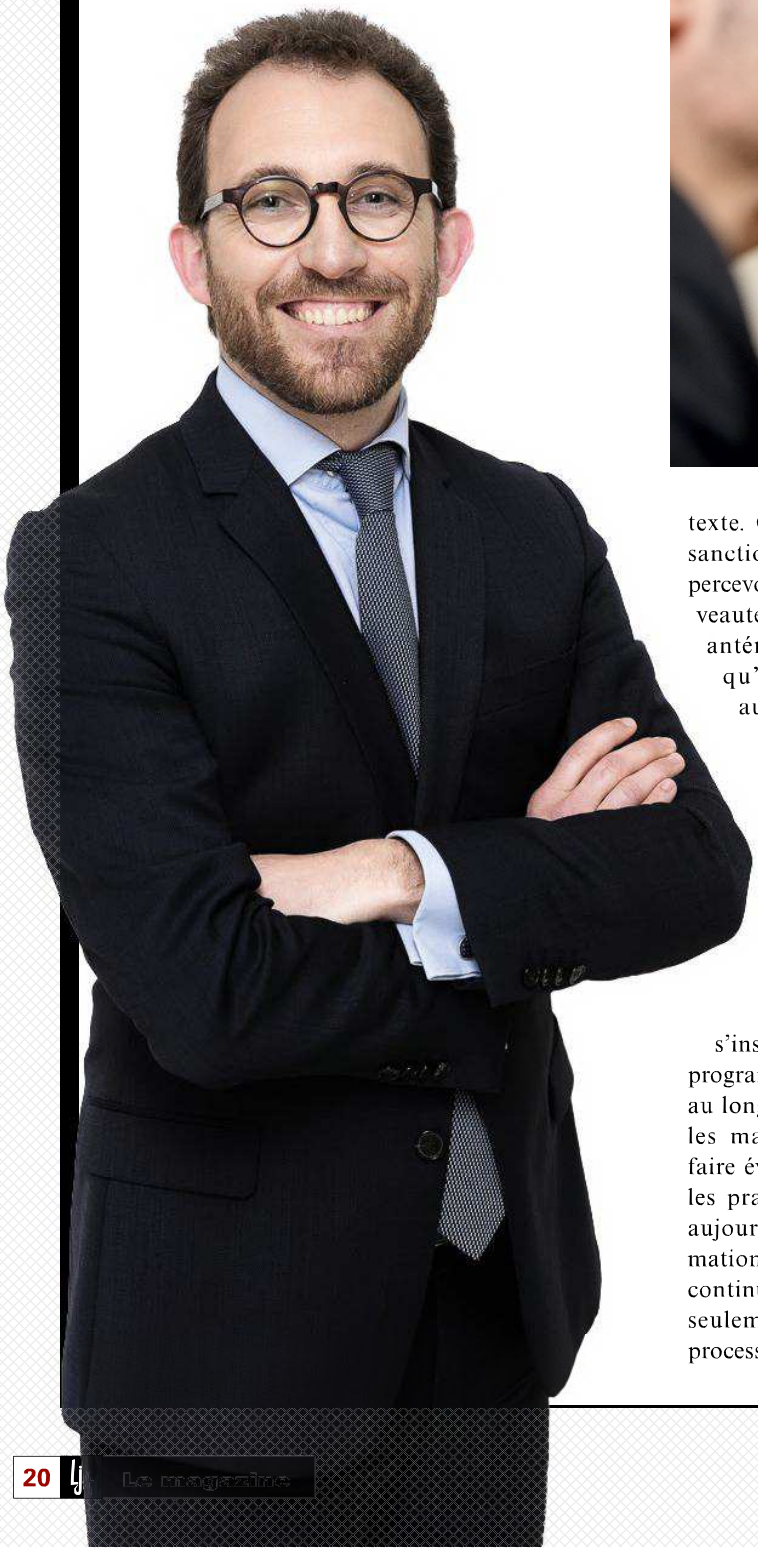
ticulier de leurs sous-traitants, et des nouvelles règles applicables en la matière.

Grégoire Hanquier : Il ne se passe pas une semaine sans échanges avec nos clients et avec nos fournisseurs sur la désignation du responsable du traitement et du sous-traitant. Le RGPD – quittant à peine les fonts baptismaux – devient l'objet de négociations contractuelles et augmente, *de facto*, la charge de travail pour les entreprises.
Rappelons-nous aussi de la « légende urbaine » selon laquelle le consentement était obligatoire pour tout le monde. Nous boîtes pros comme persos croulaient sous ce type d'e-mails autour du 25 mai ! Le RGPD n'a pas changé les règles différenciantes applicables aux e-mails de prospection, que ces derniers soient en B2B ou en B2C. La fiche publiée par la CNIL, fin 2018, sur le sujet devrait être punaisée dans toutes les bureaux de chargés de prospections et chez les *data brokers* ! Le RGPD, c'est d'abord de l'information transparente sur ce que l'on fait, c'est donner au destinataire la capacité de s'opposer au traitement et, suivant les cas, on va chercher en amont le consentement de la personne !

Bertrand Liard : Après une petite période de calme post-25 mai 2018, les clients sont rapidement revenus nous consulter sur toutes les questions complexes et sans réponse posées par le RGPD. Et tout particulièrement son articulation avec tous les autres droits (droit du travail, droit de la consommation, droit international privé, etc.), domaines qui n'ont pas été anticipés par les autorités de protection des données, lesquelles sont, par nature, verticales dans leur approche.

La méthodologie de mise en œuvre du texte

Stéphane Larrière : Le buzz réalisé autour des sanctions a, à mon sens, biaisé l'entrée en vigueur du texte, en le présentant sous un aspect négatif et en lui conférant un côté « tâche



Grégoire Hanquier, Directeur Juridique Europe, Afrique & Moyen Orient – LexisNexis SA

hyperadministrative ». Pour éviter la sanction, les acteurs au sein des entreprises ont voulu concentrer leurs efforts sur l'obtention rapide d'un bon niveau de compliance, omettant parfois peut-être de bien saisir et de comprendre les tenants et les aboutissants du texte. Cette approche par la sanction a empêché de bien percevoir la portée de ses nouveautés par rapport aux lois antérieures et la confiance qu'il pouvait apporter aux acteurs, notamment quand ils opèrent dans le domaine du digital et des technologies nouvelles.

Dès lors, des efforts d'explication et de pédagogie ont été nécessaires, pour faire comprendre que l'exercice devait s'inscrire dans un véritable programme de transformation au long cours, pour proscrire les mauvaises habitudes et faire évoluer l'état d'esprit et les pratiques. Cela nécessite aujourd'hui un effort de formation important, et surtout continu, pour permettre non seulement l'intégration aux process, mais surtout l'assimilation des nouveaux principes, comme celui de la portabilité ou de la responsabilité. Il faut toujours rappeler que loin des aspects parfois trop administratifs liés au principe d'*accountability*, l'objet du RGPD est orienté sur la protection organisée par un ensemble d'acteurs d'une même chaîne, pour permettre à une personne concernée de toujours faire valoir ses droits.

Darine Fayed : Le DPO a un rôle de formation et de sensibilisation dans l'entreprise afin que la culture soit orientée vers la protection des données personnelles. C'est cet enjeu qui doit guider l'organisation en interne. Chez Mailjet, en février et en mars 2017, nous avons démarré la sensibilisation des salariés. Le risque de faille provient du facteur humain, ce sont donc les équipes qu'il faut d'abord éduquer : le marketing, la communication, etc. Il a fallu élaborer

des formations pour les salariés nouveaux entrants, mais aussi des formations continues. On a créé des newsletters DPO que j'envoie toutes les trois semaines.

Philippe Debry : Le DPO joue un rôle essentiel. Il doit être respecté et reconnu au sein de son entreprise. Il doit faire passer un certain nombre de messages importants auprès des directions. Au-delà des moyens, c'est aussi une fonction originale qu'il doit défendre en toute indépendance

Philippe Debry : J'étais CIL de Fidal pendant trois ans, par la suite j'ai donc été nommé DPO du cabinet. Je crois que nous avions sous-estimé les implications du caractère multiforme du RGPD dû au fameux triptyque « le juridique, le technique et le process ». Les premiers mois au-delà de la cartographie ont surtout été consacrés à la mise au point du plan d'actions et à l'identification des priorités. Maintenant, il y a une forme de bascule vers des aspects juridiques bien plus prégnants,

en particulier sur les notions de qualification des relations contractuelles ou la notion de consentement.

Grégoire Hanquier : Au tout début de la mise en œuvre du texte, les entreprises se sont généralement concentrées sur la pédagogie en interne et surtout sur le registre de traitement pour établir une forme de photo des traitements réalisés pour ensuite lancer les opérations. Elles se sont ensuite attelées à poursuivre leur devoir d'information vis-à-vis de leurs clients, à revoir leurs CGV/CGA à l'aune du RGPD, et à adresser de nombreux avenants (article 28) pour mettre à jour les contrats existants. Nos clients, nos fournisseurs se sont mis aussi à adresser leurs propres avenants. Conséquence pour le DPO nouvellement désigné et les équipes des directions juridiques : une avalanche de négociations sur le choix de telles ou telles trames d'avenant.

Éric Barbry : On demande beaucoup, et parfois trop, aux DPO. J'en connais beaucoup qui ne résistent pas à cette pression et le nombre de démissions, voire de burn-out, est assez impressionnant. Le problème des DPO, c'est qu'on leur demande à la fois de mettre l'entreprise en conformité

avec le RGPD et de répondre de leur vrai rôle de DPO, c'est-à-dire conseiller l'entreprise et s'assurer qu'elle maintient sa conformité. Il faut être un « surhomme » ou une « surfemme » pour faire à la fois la mise en conformité et son maintien. Et comme je le disais, nombreux de DPO n'ont pas les moyens de leur fonction.

Jeanne Bossi Malafosse,
Associée,
Delsol Avocats

Jeanne Bossi Malafosse : Le 25 mai 2018 n'était pas une date couperet, comme l'avait rappelé la présidente de la CNIL. La conformité au RGPD peut prendre des mois, il faut donc mener la conformité au RGPD elle-même, c'est-à-dire effectuer la cartographie de ses traitements, mettre en place son registre, mettre à jour ses contrats (en évitant de recopier l'article 28 du RGPD sans réflexion préalable sur le rôle des acteurs), et revoir les notes d'information et ses process, tout en étant capable, dans le même temps, d'appliquer le principe du *privacy by design* pour tout nouveau projet. Cela suppose une grande flexibilité et une capacité d'adaptation.

Bertrand Liard : Les programmes de conformité au RGPD ont été généralement conçus selon une approche « top – down » et si les grands comptes ont pu afficher une conformité au « top » au 25 mai, il est resté beaucoup de travail en aval, pour détailler et adapter aux réalités du terrain.

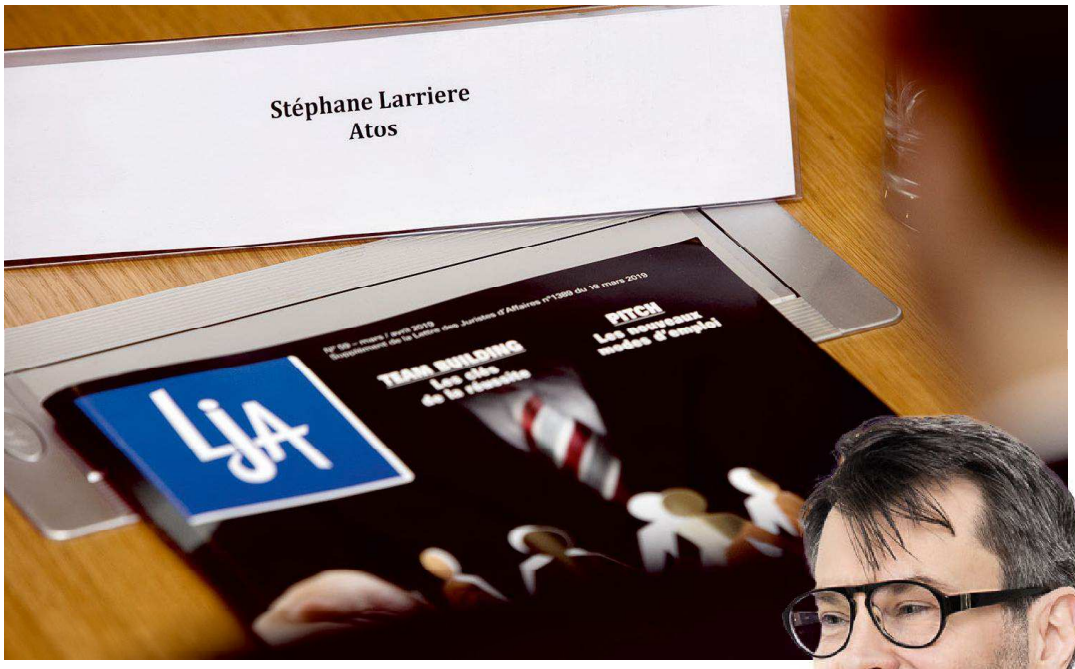
La mise en place d'outils

Emmanuelle Bartoli : L'exigence de mettre en œuvre un registre des traitements a beaucoup occupé et inquiété les entreprises dans le cadre de la préparation du RGPD. L'exercice de cartographie était un prérequis à la mise en place d'un tel registre. Dans une entreprise comme Capgemini, avec plus de 200 000 salariés, nous avons fait le choix, pour mettre en place ce registre, de recourir à un outil permettant d'avoir plusieurs niveaux de lecture de la cartographie de notre entreprise et de prendre en compte les spécificités de notre organisation. Il appartient à chaque entreprise de déterminer quel est le *modus operandi* le plus adapté pour la tenue de son registre, notamment en fonction de sa taille et de sa culture.

Stéphane Larrière : Le modèle proposé par la CNIL semble bien adapté aux petites entreprises. Il faut d'ailleurs en encourager l'utilisation ou le suivi car il revêt une forme de *soft law*. De ce fait, il doit aussi être considéré comme une source d'inspiration ou d'adaptation pour les outils « maison » façonnés dans les grands groupes internationaux, car il exprime une approche, voire une interprétation du texte, impulsées par l'autorité par ce biais. Il va de soi que ces outils doivent, notamment dans les groupes internationaux, être adaptés pour tenir compte de la culture du secteur d'activité et coller à la réalité du business et du risque géré, voire des spécificités de certains pays. La question des mises à jour et de l'évolution de ces outils doit aussi être appréhendée, car les traitements comme la jurisprudence évoluent, que ce soit sur le plan interne ou international. Je vous assure que réconcilier un DPO français et un DPO allemand – tous deux fort expérimentés – autour d'un même outil n'est pas toujours chose aisée ou évidente alors que le texte du RGPD est commun et ses principes partagés !

Jeanne Bossi Malafosse : Le texte laisse des marges de manœuvre aux pays européens pour qu'il soit différemment appliqué.

Philippe Debry : À ce titre, un outil sous-utilisé mais primor-



Stéphane Larrière,
Group Head of Data Privacy and Data Governance, Atos

dial reste l'étude d'impact. Quel que soit le secteur d'activité, cet outil est incontournable pour apprécier les vrais risques liés aux traitements de la donnée personnelle dans son activité.

Jeanne Bossi Malafosse : Elle est comparable à la documentation que l'on devait rassembler auparavant dans le cadre des demandes d'autorisation déposées auprès de la CNIL, avec une nouveauté pour les acteurs qui est de procéder eux-mêmes à une analyse des risques, en grande partie inspirée de la méthode EBIOS.

Stéphane Larrière : Il y a eu, lors de l'entrée en vigueur, beaucoup d'échanges et de débats avec les clients ou avec les fournisseurs sur les clauses à négocier, comme vous le disiez précédemment, mais il n'y a peut-être pas eu assez d'échanges sur la réalité concrète des risques des traitements. Chez certains le fait d'avoir de bonnes clauses en leur faveur apparaissait comme suffisant. Or, pour partager une analyse de risques d'un traitement, il faut en réalité partager les approches et les outils. À titre d'exemple, nous avions à l'époque lancé un outil pour partager une méthode documentée d'analyse des risques. Au départ, il a été très contesté, très discuté, et il n'a pas reçu l'adhésion immédiate de nos clients et de nos fournisseurs, car certains d'entre eux n'étaient pas encore matures pour échanger de manière documentée sur ce type de sujet. Mais les états d'esprit ont changé aujourd'hui, ils en comprennent mieux l'intérêt. Là encore, je crois que dans la mesure où les décideurs étaient avant tout centrés sur le risque de sanction, ils en oubliaient la

philosophie générale de protection de la personne concernée, se montrant du coup hyperdéfensifs sur toutes les approches. Finalement, l'objectif était, au mépris parfois des qualifications légales évidentes de responsable de traitement ou de sous-traitant, de pousser – d'une manière parfois théorique, il faut bien le dire – le maximum de risques vers l'autre partie dans les négociations des contrats, mais aussi lors des échanges à propos du risque à analyser ou des instructions. La collecte des instructions s'avère, elle aussi, un exercice de partage compliqué. Car que se cache-t-il opérationnellement derrière cette notion ? Certains m'affirment même que les instructions sont le contrat ! N'est-ce pas nier le caractère synallagmatique de l'accord… ?

Grégoire Hanquier : Certains m'expliquent qu'ils sont clients, donc que nous sommes sous-traitants !

Éric Barbry : Sur des produits comme les vôtres, en mode SaaS, jamais le responsable de traitement ne donnera les instructions au sous-traitant. C'est le prestataire qui fixe les règles, et les instructions de sécurité sont les siennes. C'est bien toute la limite du texte qui voudrait que ce soit le responsable de traitement qui donne les instructions à son sous-traitant, et non l'inverse.

Darine Fayed : Chez Mailjet, nous avons un rôle de sous-traitant vis-à-vis de nos clients. L'entreprise est une solution d'emailing en mode SaaS. Avec plus de 130 000 clients, nous ne pouvons pas faire du traitement de données sur mesure pour chaque client qui nous en donnerait les instructions.

La difficulté du « privacy by design »

Éric Barbry : Un autre exercice compliqué est celui de la mise en place de la démarche de *privacy by design*, qui est l'un des principes du RGPD. Lorsqu'il y a un contrôle CNIL, les agents de l'autorité de contrôle cherchent à savoir comment l'entreprise traite la question du *privacy by design*. Or, en pratique, cette démarche est rarement mise en œuvre.

Bertrand Liard : Tout dépend des industries. Dans certains secteurs, la valeur ajoutée autour des données a été prise en compte depuis longtemps. Il a suffi d'intégrer le *privacy by design* dans la qualification des différents projets, au travers des questions de sécurité. Mais force est de constater que c'est surtout le cas dans des grands groupes qui ont des approches structurées.

Stéphane Larrière : Il a un impact à la fois sur les processus de développement des produits et sur leurs coûts de recherche. Quand on investit dans un prototype dont on ne sait pas si à terme il marchera, comment gérer la profondeur des spécifications afférentes au principe de *privacy by design*, et à quel stade du *Proof of Concept* est-il le plus adéquat de l'intégrer concrètement ? Ces questions, au-delà des principes, sont compliquées et la mise en œuvre opérationnelle est un vrai challenge pour tous les acteurs. C'est là aussi où le DPO doit jouer son rôle d'évaluation et de mise en balance des intérêts.

Darine Fayed : Chez Mailjet, nous avons un cahier des charges que les équipes doivent remplir à chaque fois que l'on conçoit une nouvelle fonctionnalité dans lequel a été rajouté un chapitre traitant plus particulièrement du *privacy by design*.

Emmanuelle Bartoli : Jusqu'à présent, personne n'a remis en cause le fait que la sécurité informatique devait être un point de contrôle obligatoire sur tous les nouveaux projets. On rajoute désormais une couche plus spécifique à la protection des données personnelles. Comme il s'agit d'un point juridique, on a tendance à le considérer nécessairement comme étant une contrainte. Cependant, il ne faut pas être timide sur ce sujet. Il convient de faire accepter en interne le fait que la protection des données personnelles est un élément essentiel devant être pris en compte dans tout projet. Et ce, dès le début et la phase de design d'un projet.

Grégoire Hanquier : Chez LexisNexis, les nouveaux projets de développement intègrent désormais des spécifications fonctionnelles et techniques RGPD : les équipes, par exemple, savent que la question de la durée de conservation des données obéit à des règles impératives ou bien à des engagements proportionnées aux finalités des traitements de données.

Éric Barbry : La durée de conservation est un vrai sujet. Pourtant, rien de nouveau. Depuis 1978, la règle prévoit que les données ne doivent pas être conservées plus longtemps que cela est légitime. Sur tous les contrôles récents que j'ai vécus, la CNIL contrôle particulièrement ce point. Généralement, elle demande à l'entreprise de lui communiquer

Bertrand Liard,
Associé,
White & Case

des données clients ou prospects sur trois ans, plus de cinq ans, plus de huit ans et gare à ceux qui ont des durées trop longues ou inexpliquées.

Jeanne Bossi Malafosse : C'est l'un de grands principes de protection des données depuis 40 ans ! Mais comme on doit désormais informer les personnes de la durée de conservation des données, tout le monde se préoccupe de l'application réelle de ces durées, et avant tout de leur détermination.

Le temps des sanctions

Darine Fayed,
Head of legal
et DPO, Mailjet

Grégoire Hanquier : Certains s'offusquent, aujourd'hui, que la CNIL change de braquet en abandonnant sa mansuétude « montessorienne » de 2018, et s'engage désormais vers des contrôles ciblés sur de grandes thématiques.

Emmanuelle Bartoli : On a longtemps fait le reproche à la CNIL de ne pas sanctionner assez, rendant ainsi difficile la prise de conscience du risque protection des données par les directions ! Cela me semble donc aller dans le sens de l'histoire que la CNIL passe à l'offensive.

Darine Fayed : Le texte est entré en vigueur depuis un an. Donc si l'entreprise n'est pas déjà en conformité, c'est manifestement la preuve qu'elle a sous-estimé les dispositions. Un an après, il est désormais temps de mettre de la qualité dans la conformité, de créer des fonctionnalités automatisées qui répondent aux exigences.

Philippe Debry : Cette montée en puissance de la CNIL était attendue. Il faut rappeler qu'il s'est écoulé en fait trois ans jusqu'à ce jour depuis son entrée en vigueur !

Bertrand Liard : La CNIL pose sa casquette de pédagogue et prend désormais celle de gendarme. Le règlement est complexe, les clauses qu'il contient sont techniques et les sanctions sont d'un niveau important. Si le régulateur vient sanctionner à tout va, il risque de braquer les entreprises et de tendre les situations.

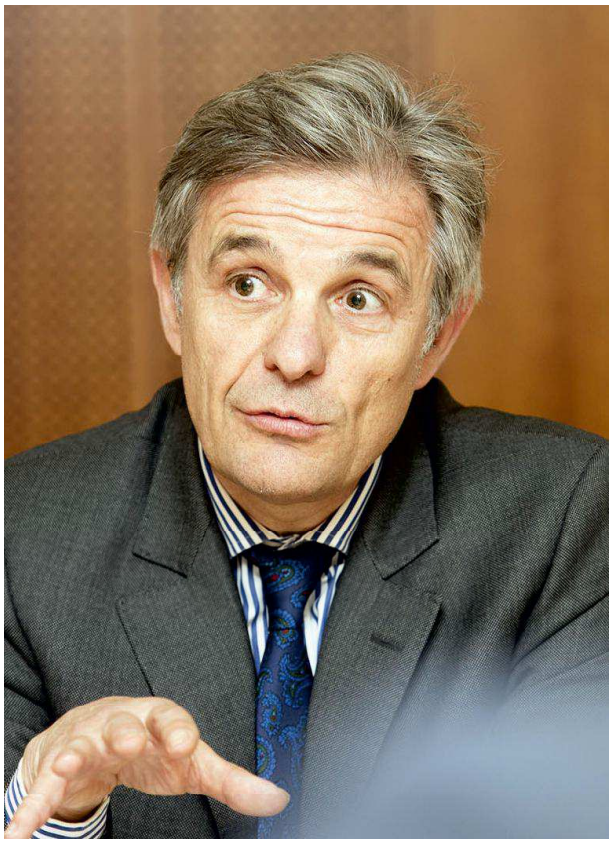
Jeanne Bossi Malafosse : L'Autorité de la concurrence avait fait la même démarche. Le parallèle est instructif.

Bertrand Liard : À la différence de l'Autorité de la concurrence, dont le recours est devant la cour d'appel de Paris puis devant la Cour de cassation, les décisions de la CNIL seront portées devant le Conseil d'État. Or, dans la plupart des cas, il confirme les décisions des autorités administratives indépendantes. C'est un vrai risque à prendre en considération.

Philippe Debry : Il y aura peut-être une évolution avec le plan récent de collaboration mis en place entre la DGCCRF et la CNIL.

Éric Barbry : Le problème auquel nous sommes confrontés est que certaines personnes, consommateurs ou prospects, se plaignent à la CNIL, alors même que leur dossier est en cours de traitement et qu'ils obtiendront satisfaction. L'entreprise devient suspecte par nature. Parfois, cela déclenche même des contrôles de la CNIL ou des demandes d'explications, alors que le cas a été traité comme il se doit.

Bertrand Liard : C'est plutôt une source de complexité supplémentaire. Les traitements de données sont maintenant sanctionnables, au minimum, par la CNIL (ou l'autorité chef de file, si celle-ci est différente), la DGCCRF (ou les mécanismes européens de coopération des agences de protection des



consommateurs) et les tribunaux (sans que les questions d'articulation entre le RGPD et les autres instruments de droit international, notamment de droit européen, aient été abordées). Que faire en cas de solutions divergentes ? Celles-ci ne sont pas une hypothèse d'école, mais bien déjà une réalité.

Stéphane Larrière : Oui, le caractère anxiogène des sanctions est aussi accentué par certaines incertitudes causées par les philosophies parfois opposées de textes de loi, et la nature même de la technologie. Regardez la difficulté d'exercice d'une analyse d'impact sur les dispositifs d'alerte et d'anti-corruption de Sapin 2 à déployer dans un environnement international ! Plus généralement, aussi, avec le digital et ses évolutions en mode continu, les données ont pris un caractère éminemment organique, qu'il est difficile de figer dans une situation donnée et arrêtée de manière définitive. L'évaluation est continue. C'est la réalité technologique.

Jeanne Bossi Malafosse : Les anciennes formalités préalables avaient un pouvoir rassurant pour les acteurs. Désormais, ils doivent assumer leur conformité de façon plus solitaire !

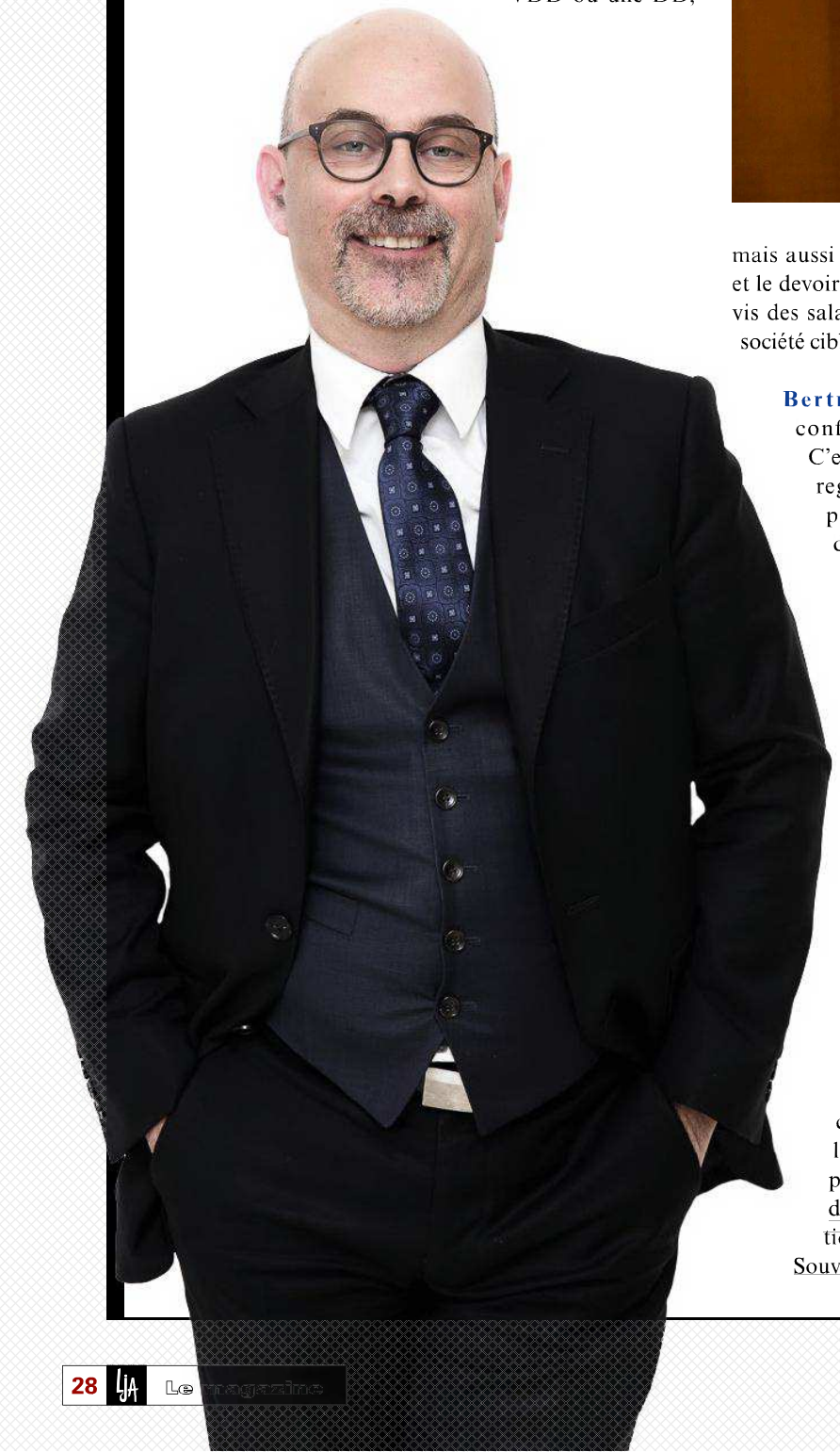
Stéphane Larrière : La nécessité de documenter pour se ménager la preuve de conformité s'accommode parfois assez mal des situations d'urgence extrême pour sauver des systèmes d'information, dont les manquements sont assortis de lourdes sanctions contractuelles. A-t-on d'autres choix que de demander les autorisations ? Il y a dans cette régulation des process parfois compliqués à mettre en œuvre pour faire face à des situations exceptionnelles. J'aurais peut-être aimé que le texte ouvre la porte à quelques exceptions liées au caractère d'urgence.

Jeanne Bossi Malafosse : Mais l'interdit-il ? La protection des données est un jeu d'équilibre entre la nécessité d'échanger et de partager des données au sein d'un monde désormais digital et le respect de nos droits fondamentaux.
À chacun de trouver cet équilibre au sein d'un cadre juridique défini et d'être en mesure d'expliquer ses positions.
Qui peut dire aujourd'hui qu'il est parfaitement conforme au règlement européen ?

Éric Barbry : Lors d'un contrôle, les enquêteurs cherchent avant tout les tableaux Excel et ce que l'on appelle la donnée non structurée, celle qui n'est pas incluse dans un outil métier. Mais qui n'a pas son tableau Excel ? Il est évident qu'il y a un fossé entre

la mise en conformité et la pratique, et c'est un boulevard pour la CNIL.

Philippe Debry : Dans les opérations de M & A, la question de la conformité au RGPD est également devenue importante et récurrente. Ainsi en est-il de l'utilisation des données personnelles qui peuvent être mises à disposition dans une VDD ou une DD,



Éric Barbry,
Associé,
Racine Avocats

mais aussi dans tout le process et le devoir d'information vis-à-vis des salariés impliqués de la société cible.

Bertrand Liard : Je confirme tout à fait. C'est un sujet que nous regardons de plus en plus attentivement dans le cadre des *due diligences* et qui fait l'objet de longues négociations des clauses de déclarations et garanties. L'approche précédente retenant une déclaration générale de conformité n'est plus à l'ordre du jour.

Éric Barbry : Le temps des sanctions est sans doute venu, mais je déplore tout de même que les contrôles opérés par la CNIL ne soient pas aussi un moment d'échange sur les pratiques de l'entreprise. Souvent lors d'un contrôle il m'arrive de poser des questions aux contrôleurs et la réponse est la même : « Nous sommes là pour contrôler et non plus pour expliquer. » Je trouve cela dommage, car le contrôle est aussi un bon moyen de rencontrer la CNIL qui en ce moment est débordée et qui n'a plus le temps de jouer son rôle de conseil.

Bertrand Liard : Nous devons tenir notre rôle de conseil et soulever le problème juridique. Rappelons-nous de la décision de la Cour de cassation de 2013 : une base de données personnelles non déclarée à la CNIL est hors commerce et constitue un objet illicite dont la vente doit être annulée. Après, c'est aux opérationnels de prendre la décision business et d'effectuer un bilan risque-opportunité.

Philippe Debry : Tout n'est pas perdu d'avance. Mais il faut être en capacité de démontrer que l'on a mis en place un plan d'action effectif pour se mettre en conformité.

Éric Barbry : Il n'est pas question de refuser un droit d'accès mais la question est de savoir jusqu'où il faut aller. Lors d'un des derniers

contrôles auxquels j'ai participé, la question a été posée de savoir quelle était l'étendue du droit d'accès d'un client, et notamment de savoir si les courriers et e-mails échangés devaient lui être communiqués. Je n'ai toujours pas la réponse. La même question se pose sur les données auxquelles un salarié peut avoir accès. Faut-il aller jusqu'à lui communiquer tous les e-mails où il est destinataire, expéditeur ou simplement en copie ? Faut-il lui donner aussi les comptes rendus des réunions où son nom apparaît comme participant. Il est urgent que la CNIL se positionne sur le sujet, car les entreprises naviguent dans le brouillard.

Emmanuelle Bartoli : Le département des contrôles de la CNIL est assez stable du point de vue des effectifs et de l'approche. Lors des contrôles, les agents essaient d'être pragmatiques. Ils identifient ce qui a déjà été mis en place et pointent du doigt les insuffisances. Cependant, l'entreprise dispose en général d'un délai d'un ou deux mois afin d'apporter des éléments à la CNIL concernant les mesures mises en place afin de pallier les insuffisances remontées par la CNIL. Ils ne prennent donc pas le bâton immédiatement. Même si la nouvelle présidente a récemment exprimé sa volonté de renforcer les sanctions, l'approche des enquêteurs devrait demeurer la même. Afin de faciliter le travail des entreprises et d'anticiper la nature des contrôles, il sera toujours utile pour ces dernières de disposer de *guidelines* de la part de la CNIL. Typiquement, un guide pratique sur la question du droit d'accès sera particulièrement utile pour les entreprises au regard du nombre croissant de demandes d'accès, qui, si elles étaient mal traitées, pourraient donner lieu à des contrôles de la CNIL.

Jeanne Bossi Malafosse : Ce n'est pas forcément négatif, et cela nous permet d'avoir notre propre interprétation. J'ai par exemple travaillé sur le dossier d'un salarié qui avait quitté l'entreprise depuis longtemps et qui ensuite exerçait son droit d'accès. Quelles données transmettre ? Jusqu'où remonter dans le temps, éviter de communiquer des données qui auraient dû, au titre des durées de conservation, être supprimées ?

Darine Fayed : N'oublions pas qu'on a le droit de refuser une demande de droit d'accès !

Éric Barbry : Le dernier contrôle subi par l'un de mes clients est justement fondé sur le fait que l'on n'a pas satisfait à 100 % une demande de droit d'accès. Nous n'avons, par exemple, pas communiqué les échanges de courriers entre mon client et son contestataire, en expliquant qu'ils n'étaient pas des données personnelles. Mais il y a un débat. Autre incertitude : quand le salarié demande un droit d'accès, doit-il avoir également accès au compte rendu de réunion où est inscrit son nom ? Aux mails qu'il a reçus ? C'est d'une complexité inouïe !

Bertrand Liard : L'exercice du droit d'accès, surtout des salariés, est effectivement plus que complexe. D'autant plus qu'il mêle le droit des données personnelles et le droit du travail. La recherche de solutions équilibrées, protectrices des droits de chacun (lanceur d'alerte, demandeur de droit d'accès, victime de harcèlement, autorité de poursuite, etc.), tourne alors au cauchemar juridique. ■