INTERVIEW CROISÉE

Par Sébastien Gressier

RGPD : l'environnement autour de la protection des données personnelles n'a pas fini d'évoluer

Depuis son entrée en vigueur, il y a un an, le règlement général sur la protection des données personnelles (RGPD) a obligé de nombreuses sociétés à renforcer leurs dispositifs internes. Or, les lignes n'ont pas fini de bouger dans ce domaine, des évolutions liées au RGPD ainsi qu'à d'autres textes internationaux qui vont prochainement s'imposer aux entreprises.

Entretien croisé avec **Anne-Sophie Nibert**, Corporate Data privacy Lead au sein de Direction Conformité et Responsabilité sociétale de Total SA, et **Myria Saarinen**, associée spécialisée en contentieux commerciaux complexes, données à caractère personnel et compliance chez Latham & Watkins.

Le 25 mai 2018, l'entrée en application du RGPD n'était pas sans susciter des inquiétudes au sein de nombreux groupes. Un an plus tard, qu'en est-il ?

Myria Saarinen : Dans les grands groupes, les inquiétudes se sont plutôt dissipées, même s'ils attendent encore d'en savoir plus sur le risque financier, en raison des sanctions qui tombent pour l'instant au compte-gouttes. Cette catégorie d'entreprises n'a cependant pas découvert la thématique des données personnelles en 2018, elle était déjà familiarisée avec le sujet du fait des textes préexistants (la loi informatique et liberté, la directive européenne de 1995…). Dès lors, l'entrée en application de ce règlement n'a pas constitué un saut dans l'inconnu pour ces entreprises. À l'inverse, le RGPD a constitué une véritable révolution pour des sociétés de plus petite taille, dont certaines se trouvent encore aujourd'hui au milieu du gué. Le niveau d'inquiétude reste toujours élevé pour celles-là faute de maîtrise du sujet.

Anne-Sophie Nibert : Je partage l'observation faite sur les grands groupes. Dans la mesure où la protection des données personnelles n'est pas une problématique nouvelle, nous disposions déjà, chez Total, de dispositifs en interne pour nous conformer à la réglementation applicable. Pour autant, le RGPD est venu renforcer les obligations incombant aux entreprises, introduire le principe d'*accountability* et durcir les sanctions en cas d'infraction, motivant ainsi la mobilisation des diverses compétences pour travailler de concert sur le sujet.

Quels chantiers a impliqués la mise en œuvre du RGPD chez Total SA ?

Anne-Sophie Nibert : Nous disposions, préalablement à l'entrée en application du RGPD, de « règles d'entreprise contraignantes » (*Binding Corporate Rules*, ou BCR), validées par les autorités de contrôle de l'Union européenne, qui constituent un programme fixant les règles pour la protection des données applicables au-delà des transferts intragroupe de ces données. Il prévoit notamment une gouvernance, des procédures pour la mise en œuvre des principes de protection, des dispositifs de formation et de gestion des plaintes. Il nous a toutefois fallu compléter notre programme pour nous conformer aux nouvelles exigences du RGPD. Il nous incombe en particulier de tracer et de documenter toutes les mesures de protection des données personnelles que nous traitons et conservons. De plus, nous avons développé de nouveaux outils de formation et d'information comme des boîtes à outils et un chatbot, afin de répondre aux questions que les collaborateurs se posent dans le cadre de nos activités. Enfin, nous avons regardé pour chaque entité concernée par le règlement – soit pour plus de 200 filiales européennes – si elle avait l'obligation ou non de nommer auprès des autorités de contrôle un *data protection officer* (DPO) en plus de l'organisation déjà en place.

Quelle est la principale difficulté à laquelle le groupe a été confronté dans ce processus de mise en conformité ?

Anne-Sophie Nibert : Il nous a fallu agir vite en anticipant parfois les recommandations des autorités de contrôle pour interpréter les exigences du règlement. Le projet a mobilisé des représentants de toutes nos branches d'activité et de diverses compétences, afin de développer et de déployer dans le délai imparti des outils adaptés pour nos filiales situées dans les 28 pays de l'UE. Nous avons déconstruit certaines idées fausses autour du RGPD, comme la nécessité de recueillir systématiquement le consentement écrit des personnes concernées, alors que le règlement ouvre d'autres possibilités, ou l'obligation de désigner un DPO, alors que c'est le cas uniquement dans des conditions précisées par le règlement.

Myria Saarinen

Anne-Sophie Nibert

Qu'en a-t-il été dans les autres entreprises?

Myria Saarinen: La situation dépeinte pour Total reflète ce que j'ai pu constater avec les autres grands groupes: le nouveau principe d'*accountability* les a en particulier obligés à repenser le flux des données, depuis la collecte, et surtout la manière de documenter ce flux, avec des process écrits plus contraignants. Pour les sociétés chez qui la gestion des données personnelles était moins structurée, la tâche s'est révélée forcément plus complexe. C'est d'ailleurs l'un des enseignements de cette première année post-RGPD: alors que le texte avait été présenté comme une avancée marquant la fin des formalités administratives, et donc de la paperasserie, dans les faits, on en est loin! Le RGPD est générateur de plus de documentation, certes non destinée à être partagée avec les autorités, sauf en cas de demande ou de contrôle: registre des traitements, documentation du consentement, process pour l'analyse d'impact, pour les *data breaches*, pour la prise en compte des droits des personnes, pour la mise en place du *privacy by design*, etc. Une autre interrogation récurrente que j'ai pu constater auprès des grands groupes internationaux au cours de cette première année de vie du RGPD était de savoir si celui-ci ne pouvait finalement pas servir de référentiel pour l'intégralité de leurs opérations de traitement, y compris en dehors de l'Europe, afin de simplifier leur politique globale de gestion des données personnelles. Certains ont en effet opté pour cette solution.

Sur le cas spécifique des DPO, les entreprises souhaitant en recruter étaient confrontées l'an dernier à une pénurie de candidats. Comment se sont-elles adaptées? La situation a-t-elle évolué depuis?

Myria Saarinen: Certains de mes clients ont effectivement rencontré des difficultés pour trouver le bon candidat. Ce faisant, ils ont souvent opté pour des candidats en interne, en privilégiant leur connaissance de l'entreprise et en assurant ensuite leur formation sur la matière des données personnelles. À l'avenir, la donne pourrait toutefois évoluer. Le DPO représentant indiscutablement un métier en devenir, des formations universitaires commencent à se mettre en place. Preuve de l'intérêt croissant des jeunes pour cette profession, et pour la thématique de la protection des données personnelles en général, depuis quelques mois il n'y a pas une semaine au cours de laquelle je ne reçois pas de candidatures de stage ou de collaboration dans mon département. Ce n'était pas le cas quand j'ai commencé à pratiquer cette matière il y a vingt ans!

Anne-Sophie Nibert: Chez Total, nous avons nommé, pour rester près du terrain, des DPO au sein des sociétés concernées plutôt qu'un DPO unique au niveau groupe. Compte tenu du fait qu'il est complexe pour un individu de maîtriser toutes les compétences nécessaires à la fonction (comme la sécurité des systèmes d'information ou le droit de la protection des données personnelles), nous travaillons en réseau. Les DPO peuvent s'appuyer sur d'autres experts du groupe et sur le support fourni au niveau groupe ou de leur branche d'activité. Dès lors, le DPO doit être avant tout un bon pédagogue, de manière à pouvoir embarquer les équipes opérationnelles malgré les contraintes qu'impose le programme.

En janvier dernier, la CNIL a prononcé une amende record à l'encontre de Google (50 millions d'euros) pour non-respect du RGPD. Cette décision marque-t-elle selon vous un tournant dans l'approche des autorités qui, après avoir annoncé leur intention d'accompagner les entreprises, auraient dorénavant décidé de sanctionner sévèrement toute dérive?

Myria Saarinen: À ce jour, la sanction prononcée à l'encontre de Google constitue l'unique sanction prononcée par la CNIL sur le fondement du RGPD. En conséquence, il est délicat de tirer des conclusions générales de cette seule sanction même si, indiscutablement, la CNIL souhaitait frapper vite et fort. Par ailleurs, même s'il s'agit d'un montant record, cette somme de 50 millions d'euros est plutôt faible au regard de la sanction maximale prévue par le RGPD, susceptible d'atteindre jusqu'à 4 % du chiffre d'affaires mondial du groupe. En tout état de cause, la CNIL vient d'annoncer qu'elle se montrerait inflexible sur la conformité au RGPD. Reste qu'elle est forcément bridée par les moyens financiers et humains, limités, qui lui sont accordés. ■