Attention RGPD, la dernière ligne droite

Présentations des intervenants

Claire Levallois-Barth :

Claire Levallois-Barth ouvre la conférence en positionnant le RGPD dans un processus historique depuis la loi « Informatique et Libertés » créant la CNIL en 1978 en passant par la directive européenne 95/46/CE sur la protection des données, puis de retour en France la loi pour une République Numérique (LRN) en 2016.

C'est parce que la directive de 1995 retranscrite en droit national de chaque pays a été jugée inopérante que la nécessité du RGPD s'est fait jour. Avec comme objectif celui d'obtenir effectivité et surface d'action de dimension internationale et non plus seulement nationale.
Pour bien introduire la conférence Claire précise la définition de la donnée à caractère personnel : elle correspond à toute donnée relative à une personne qui permet de l'identifier de manière certaine – directe ou indirecte. Suivant le contexte dans laquelle elle réside ou circule, cette donnée ou jeu de données est de nature différente. A ce stade on estime que 69% du contenu des Bases de Données numériques dans notre société digitale constituent de la donnée à caractère personnel.
Un rappel est fait au sujet des sanctions en cas de perte ou vol de données à caractère personnel : cette sanction existait depuis 1978, et est déjà de l'ordre de 3 millions d'euros depuis la LRN. A partir du 25 mai 2018, le RGPD fera passer cette sanction à un maximum de 20 millions d'euros ou 2%/4% du CA de l'entreprise suivant la criticité de l'incident. La perte ou le vol de données devra être renseigné auprès de la CNIL dans les 72 heures, qui suivant le cas pourra juger de révéler publiquement l'incident. L'objectif est que l'impact potentiel sur l'image de marque agisse comme un levier pour responsabiliser les acteurs sur la nécessité de protéger leurs données numériques.
La mise en oeuvre du RGPD touche tous les métiers. Ce qui oblige une prise en compte au niveau de la gouvernance des données au plus haut niveau. Et qui débouche sur des nouveaux process.
Le groupe de travail européen G29 sur la protection des données rassemblant les autorités de contrôle nationale dont la CNIL va être remplacé en mai 2018 par le nouveau Comité Européen de la Protection des Données. Il sera en charge de mettre en musique l'application du RGPD et de participer à la co-construction du droit et de la jurisprudence résultant du RGPD.
Claire rappelle plusieurs points :

- Le RGPD s'applique aux données numériques à caractère personnel de tout citoyen ou résident dans l'Union Européenne, et même si ces données sont traités ou hébergées hors de l'Union.
- Le RGPD s'applique à toute organisation, entreprise, acteur économique, administrations et aussi à toutes les associations. Seule l'utilisation de données à caractère personnel dans le cadre privé sort du champ du RGPD (ex : carnet d'adresses personnel sur smartphone, …).
- Le RGPD a un volet important sur le droit à la portabilité des données accordé à tout citoyen européen
- Le RGPD a un volet important sur le droit à l'oubli.

Garance Mathias et Amandine Kashani-Poor :

Elles choisissent de présenter sous forme de dialogue entre elles le rôle du délégué aux protections des données (DPO), avec l'objectif de démystifier son rôle. Il est rappelé que le DPO est la clef de voute dans l'application du RGPD sur le terrain pour chaque organisation.
Il est désigné, avec un rôle inscrit dans son contrat de travail. A ce jour on note qu'il a un profil très souvent juridique mais rien n'interdit qu'un profil technique soit désigné. Il doit avoir en tout cas un « background » juridique, et travailler avec une vision transverse entre le monde technique et le droit.
Au quotidien Amandine s'appuie quant à elle sur le RSSI, qui traduit les objectifs qu'elle établit en exigences techniques (architecture, processus, solutions de cyber-sécurité). Elle fait le lien avec tous les auditeurs internes, et s'appuie sur les référents métiers de l'entreprise.
Afin de répondre aux aspects anxiogènes de cette échéance du 25 mai 2018 et de la difficulté de ce nouveau rôle et de ces nouvelles obligations qui s'imposent à l'entreprise, Garance tient à préciser plusieurs points :

- Pour ceux qui attendent les détails : le texte de retranscription dans le droit national est à venir.
- Les entreprises qui agissent sous le régime de la loi de 1978, de la directive de 1995 ne partent pas de zéro. Les autorités nationales qui jouent le rôle de régulateur en tiendront compte. Il faut au minimum démontrer avant le 25 mai que les processus de mise en oeuvre des actions de protection des données sont enclenchés et que la responsabilité vis-à-vis de la protection des données à caractère personnel est bien incluse dans la gouvernance de l'entreprise.
- Certes les administrations et les entreprises qui gèrent intrinsèquement des données à grande échelle ont l'obligation de nommer un DPO. Pour les autres, il faut considérer le DPO comme une faculté et à ce titre il est possible de « sous-traiter » cette fonction à un prestataire de service qui pourra jouer ce rôle.
- Il est rappelé que le DPO ne peut pas être le responsable des données ou du traitement des données (qui est le « *data owner* »). Il ne porte aucune responsabilité pénale en cas de problème.

David Hozé :

David Hozé met en avant son background ingénieur Télécom et son expérience de consultant en organisation pour présenter les grandes lignes d'un processus de mise en conformité tel qu'il le conseille à ses clients. Il précise que cela se traduit par une animation de multiples actions et processus s'échelonnant sur de nombreuses années. Il n'y a pas de projet coup de poing définitif qui pourrait mettre en conformité l'entreprise avant l'échéance de mai 2018 et qui pourrait s'achever une fois pour toute par la suite.
Sa pratique sur le terrain lui permet de dire que le travail commence à peine chez les PME et les petites ETI. Il conseille aux acteurs économiques et associations de ne plus tarder pour initier le travail, qui est toujours plus long que ce que les décideurs ou responsables pensent être au départ.
Plusieurs cas de figures sont constatés dans l'initiation de la démarche par le top management : dans les grandes entreprises, le personnel dirigeant en charge de la gestion des risques pilote à 100 %.
Dans les petites entreprises, c'est au DG ou à la personne jouant le rôle de DG d'initier et de piloter la démarche.
David constate que la demande de consultants vient très souvent après la nomination et l'implication d'un juriste qui a initié le projet. Reprenant un schéma classique par les métiers de la cybersécurité, à savoir le pilotage par le risque (ISO 27001), le soutien du consultant permet de mettre en conformité l'entreprise en suivant 10 processus organisés en 4 chantiers :

- Les chantiers juridiques reposant en grande partie sur les départements juridiques ;
- Les chantiers transverses reposant sur les équipes métiers et le DPO ;
- Les chantiers techniques reposant sur la DSI et le RSSI ;
- Les chantiers de cadrage de la démarche reposant sur l'organe de gouvernance RGPD déployé au sein de l'organisation.

Malgré cette répartition, il est clair qu'il y a besoin à chaque fois de compétences mixtes, car des arbitrages sont très souvent nécessaires, résolus au travers d'un échange entre le juriste et le technicien.
David donne également quelques cas précis sur le terrain qui traduisent le résultat de ces arbitrages comme par exemple dans une société qui se trouve dans l'obligation de traiter de nombreuses demandes de droit à l'oubli émises depuis de multiples pays européens, y compris d'Europe de l'Est. Dans ce cas précis, il est décidé que le « *dispatch* » des demandes se fassent par le DPO, alors que ce n'est pas son rôle à priori.

▶ **Patricia del Carmen :**

Patricia s'applique à présenter l'impact des transferts internationaux des données à caractère personnel.
La mappemonde représentant les pays implémentant des protections de données personnelles est détaillée. Elle devra être revue en 2018 par le Comité Européen de la Protection des Données.
Pour l'heure, 110 pays implémentent une réglementation sur les données personnelles. Des pays sont reconnus comme « adéquats » pour permettre le transfert de données à caractère personnel comme : Andorre, Argentine, Canada, Iles Féroé, Guernesey, Ile de Man, Nouvelle Zélande, Israël, Jersey, Suisse, Uruguay.
Dans tous les cas, il est nécessaire que les transferts de Données Personnelles soient:

- sécurisés
- précisément documentés dans le registre du DPO
- vers un pays avec lequel la Commission a signé un traité (« *Privacy Shield » par exemple*) ou dans la liste des pays reconnus comme adéquats par la Commission
- accompagnés de procédures spécifiques suivant le type de transfert

Les questions et débats de la table ronde :

1. Plaçons-nous du côté d'une entreprise : que va-t-il se passer le 25 mai pour elle ?

Il s'agit à cet horizon de pouvoir montrer que le travail de mise en conformité a commencé. Il faut considérer que la CNIL a une pratique qui consiste plus à accompagner qu'à sanctionner, et que les acteurs sont présumés de bonne foi. La CNIL a cependant la prérogative de rendre public un incident de perte ou vol de données à caractère personnel. Ce risque touche à l'image de l'entreprise très directement, ce qui contribue au surcroit de responsabilisation qui est désormais exigé.
Garance reformule en décrivant cette situation nouvelle comme un changement de culture. Le temps est fini où on « se lavait les mains » après avoir fait sa déclaration de fichiers à la CNIL. La conformité de la protection des données à caractère personnel appartient à celui qui les stockent et les manipulent.
David précise que les moyens techniques de protection ont intrinsèquement un périmètre d'action englobant toutes les données sensibles, dont font partie les données à caractère personnel. Ce qui fait des processus de mise en conformité au RGPD, des projets de sécurisation globaux. Pour les entreprises qui ont des « *data lakes* » dans lesquels les données sont relativement peu structurées et

d'origines diverses, la cartographie et l'identification des données à caractère personnel est plus difficile. Clairement les entreprises qui détiennent ces « *data lakes* » ne sont pas encore prêtes.

2. Question sur les labels ?

Une des réponses qu'il est possible d'apporter pour construire sa conformité au RGPD est de travailler à l'obtention de label qui offrent un processus de conformité clef en main et un signe de confiance facilement reconnu. Malheureusement pour l'instant, la certification de ces labels au niveau du groupe de travail G29 a pris du retard. David fait la remarque que l'interprétation et l'implémentation technique de ces labels est difficile.
En corollaire, l'articulation avec les labels du domaine de la santé est posée. D'autres cadres législatifs interviennent en effet dans ce cas, notamment la loi Touraine de 2016 qui régit directement l'hébergement de données de santé.

3. Questions sur les enjeux business :

Finalement, à entendre les spécialistes du droit et du RGDP présents à cette table ronde, une certaine continuité semble se dessiner du point de vue du business. Les polémiques sur la préparation de la directive *e-privacy* semblent montrer le contraire. Ce sujet ne sera pas plus développé dans la table ronde.
Par contre, s'il faut identifier un impact « business » contraignant, on peut toutefois citer celui du droit à la portabilité qui donne à chaque citoyen le droit de réclamer et d'obtenir la portabilité de leurs données. Cette portabilité constitue un risque de perte client et d'acquisition tout à la fois (churn).

4. Y a-t-il un changement de comportement du consommateur qui se profile avec l'arrivée du RGPD ?

En effet, des sondages commencent à mesurer que des stratégies d'évitement augmentent (usage d'« adBlockers » etc…). Ce qui entre en conflit avec notre économie de la donnée qui considère que ces comportements constituent un frein incontestable.

5. Question sur l'effacement des données :

L'obligation de déclarer un temps de conservation des données ne date pas du RGPD. La durée d'archivages des données est fonction suivant les cas d'autres réglementations. Le droit à l'oubli du RGPD ne change rien.
A cette occasion, une question corollaire sur la signature numérique est posée. Il est rappelé que la signature sur un document, qu'il soit numérique ou pas, est régie par le code civil qui s'appliquerait en premier lieu si la question de l'effacement se pose.

6. Question sur l'anonymisation des données ?

L'anonymisation véritable est très difficilement réalisable. De nombreux cas ont témoigné qu'il est toujours possible par recoupement de retrouver l'identité anonymisée au départ. On parle plutôt de pseudonymisation et d'anonymisation partielle.

7. Le RGPD ne serait-il pas un handicap potentiel de l'UE vis-à-vis du reste du monde ?

Nous sommes devant un choix de société qui va en effet changer les comportements et le marché. Il est encore trop tôt pour tirer des conclusions. Handicap ou avantage concurrentiel à l'horizon des années futures ? Rien n'est encore sûr.