Préface

Le guide proposé par Laure Isabelle Ligaudan annonce clairement son objectif dès le titre : il s'agit de rendre opérationnel un des textes probablement les plus fondamentaux de ces quinze dernières années : le Règlement UE 2016/679 dit Règlement Général sur la Protection des Données, plus connu sous son acronyme RGPD.

Le RGPD est un texte en effet fondamental mais aussi d'une grande complexité. On peut voir deux raisons principales à cette situation.

Tout d'abord, le texte mêle tout à la fois des dispositions du domaine des libertés publiques et des droits fondamentaux, d'autres dispositions qui viennent s'ajouter ou préciser le droit spécial des données personnelles existant en France depuis 1978, des dispositions aussi du domaine du droit de la consommation, d'autres, du droit des contrats ou encore du droit du travail. Cette multidisciplinarité est une première difficulté.

Ensuite, sa rédaction et sa conception le rendent par essence complexe. Le RGPD a été conçu et rédigé comme un texte de loi, mais, comme tous les textes communautaires, il doit réaliser le consensus des pays européens. Cet exercice de haut vol a pour conséquence qu'après les principes posés, il comporte souvent une liste d'exceptions demandées par les uns et les autres pour rejoindre le consensus. Ces exceptions

sont autant de casuistiques qui devraient être du domaine des tribunaux et pas de la loi à qui il devrait être assujetti de fixer seulement le cadre. Ceci rend l'accès au texte difficile.

Or, le RGPD a une ambition qui nécessite la collaboration de tous. Il cherche le changement de comportement, de pratiques.

Un exemple passé doit nous revenir à l'esprit, celui du droit comptable et financier mis en place dans les entreprises. Ce droit exige la production annuelle de bilans et comptes de résultat, documents complexes et normés, la conservation de documents comptables tels que factures, là encore documents précisés dans la loi quant à leurs contenus, le recours obligatoire dans certains cas à des commissaires aux comptes, le respect des règles de prudence comptable, etc. Il ne viendrait pas à l'idée du plus petit des commerçants individuels jusqu'à la multinationale en bourse, de déroger à ces règles impératives pourtant très complexes. Tous savent ce qu'ils ont à faire et comment le faire, car ils ont compris les enjeux et les règles posées. Le RGPD, à sa manière, a cette ambition de la création d'un nouveau droit comptable de la donnée personnelle du plus petit au plus grand.

Pour arriver à ce changement radical, le RGPD a besoin de la coopération de ceux à qui s'adresse le RGPD en priorité, à savoir les citoyens, consommateurs, parents, salariés et toutes personnes physiques que le texte appelle les personnes concernées. Il doit aussi être rejoint par les acteurs de la matière, *controlers* (responsables de traitement) et *processors* (sous-traitants). La CNIL et les tribunaux ne pourront pas seuls imposer un tel changement.

Voilà pourquoi, l'œuvre de simplification menée par Laure Isabelle Ligaudan est fondamentale car elle doit permettre à tous d'entrer de plain-pied dans le droit comptable de la donnée personnelle. Depuis plus de vingt ans, que nous nous croisons dans différents endroits ou sur différentes initiatives où ces thèmes sont traités, je peux témoigner que

pour l'autrice, cette démarche confine à l'obsession et on ne peut que la remercier.

Léonard de Vinci disait que « la simplicité est la sophistication suprême ». Oui, pour parler et écrire simple, il faut une maîtrise totale. Cette maîtrise et cette simplicité, chacun pourra les constater dans ce « petit » traité à lire absolument.

Olivier Iteanu,
avocat à la Cour

Introduction

Ce guide opérationnel est à l'usage des DPO (Délégué à la protection des données) et des responsables de traitement qui souhaitent mettre en œuvre une démarche *privacy* au travers d'une méthode simple qu'il suffit de suivre pas à pas pour voir la conformité apparaître comme par magie.

Le RGPD (Règlement Général sur la Protection des Données) est un texte juridique à visée éthique pour favoriser la confiance dans l'économie numérique.

Qu'est-ce que la confiance dans le numérique ?

Elle dépend de la transparence des flux informationnels et de la capacité à en auditer le fonctionnement au regard des obligations de la réglementation afin d'identifier les risques d'impacts pour la vie privée et de les minimiser au maximum.

C'est pour organiser cette transparence que je travaille depuis plusieurs années afin d'identifier ces flux et de les mettre en conformité.

Ce sont ces flux et leurs cartographies qui permettent d'auditer les pratiques et de mettre en conformité les traitements de données qui en sont issus.

Ce sont ces flux qu'il faut retrouver quand on est face à des traitements identifiés dont on ne comprend pas les

pratiques professionnelles et qu'il est nécessaire d'auditer pour améliorer ou certifier.

Pour mettre en conformité ces flux informationnels, il faut s'assurer de leurs mises en conformité effectives et non simplement déclarées.

Cette mise en conformité effective dépend également de l'organisation et de sa mission. On peut mettre en conformité des systèmes d'information, des technologies complexes mais leurs conformités sont contextuelles aux objectifs définis et identifiés de la mission de l'entreprise.

Pour faire une analogie facile, le nucléaire produit de l'électricité dont les impacts pour les personnes sont positifs (même si cela est remis en question au vu de l'urgence écologique actuelle) mais il peut également engendrer des bombes atomiques dont les impacts sur les personnes sont nettement et directement plus préjudiciables.

Un des apports que mon expérience peut fournir à la conformité et l'usage éthique des données personnelles est dans cette notion de définition de la mission d'une organisation. Cette mission est identifiée dans les mises en conformité comme une « finalité d'usage ». Elle doit être spécifiquement identifiée dans tous les contextes d'activités. Elle permet ainsi de relativiser une conformité à une finalité d'usage et de pouvoir remettre en question l'utilisation de ces mêmes systèmes et technologies au bénéfice de finalités d'usage différentes.

Ainsi, l'ensemble des technologies du nucléaire seront acceptables dans le cadre de la finalité d'usage de la production d'électricité mais ne pourront être acceptables sans une seconde démarche de mise en conformité dans le cadre de la fabrication d'une bombe nucléaire.

Je vous invite donc à définir pour les organisations dont vous avez la charge, de démontrer de la protection de la vie privée et de la protection des données personnelles, de

définir clairement les finalités d'usage des traitements qui seront déclarées dans le cadre des process métiers nécessaires à leurs fonctionnements.

> Exemple : Fournir un service de mise en relation *via* des rendez-vous audio et vidéo entre des plateformes de vente de produits en ligne *via* des conseillers et des conseillères et des acheteurs potentiels ayant vocation à inciter à l'acte d'achat.
>
> Exemple : Fournir des informations issues de personnes physiques, d'associations, de collectifs ou de gouvernements à des organisations à but non lucratif et à vocation humanitaire pour anticiper des missions ou des campagnes de prévention ou d'assistances aux personnes en danger *via* une plateforme qui agrège et organise les informations collectées afin de créer des rapports permettant l'aide à la décision opérationnelles des acteurs humanitaires.
>
> Exemple : Fournir à partir de critères de requêtes préétablies des informations à des journalistes, des experts, des acteurs politiques, issues des médias nationaux mais également alternatifs dans des pays où la liberté de la presse est muselée, *via* une plateforme permettant le *crowdsourcing*.

J'ai apporté toutes mes connaissances, mon expérience, mes expertises et nous avons partagé nos compétences afin de faire de cette méthode une solution écrite et une solution numérique (www.privanciel.com).

Pourquoi ce fut long et compliqué ?

Depuis déjà quelques années, vous trouvez des solutions numériques d'accompagnement à la mise en conformité. Sans être mauvaises, elles ne sont pas assez techniques, elles ne sont pas le reflet des pratiques opérationnelles précises et elles ne tiendront pas face à un audit sérieux.

Elles sont souvent figées dans le temps et supportent mal l'amélioration continue ou la conformité dynamique que le RGPD exige.

Elles ne permettent pas de répondre aux questions simples mais essentielles que nécessite le démarrage d'une mise en conformité : quels sont mes traitements à déclarer ?

Si elles le font, c'est souvent à partir d'une liste qui n'est que de loin pertinente pour chaque typologie opérationnelle d'organisation.

Certaines sont plutôt bonnes à condition que la compétence en charge du projet ait déjà une méthode personnelle pour son projet de mise en conformité.

Le constat, dans le temps, va d'ailleurs vers l'abandon des solutions numériques dès que la compétence a trouvé comment faire car la solution ne s'avère pas assez complète pour répondre à ses exigences.

Les solutions qui pourraient y répondre sont très onéreuses et peu d'organisations peuvent s'offrir de tels outils. Dans tous les cas, aucune d'entre elles ne propose une méthode ayant l'exigence de refléter une réalité opérationnelle.

Pourtant, la CNIL et toutes les autorités de contrôle et de régulation en Europe fournissent de nombreuses informations complémentaires et des précisions de mise en œuvre de la réglementation. L'EDPB (*European Data Protection Board*) publie également des lignes directrices qui permettent de mieux comprendre et de cerner certains aspects pratiques de la réglementation.

L'outil PIA (*Privacy Impact Assessment* : analyse d'impact sur la protection des données) de la CNIL est issu de ces travaux collaboratifs et collectifs.

Ce guide ne va, d'ailleurs pas, vous lister les articles du RGPD ou les textes juridiques, vous les connaissez certainement et si ce n'est pas encore le cas, il ne vous sera pas

difficile de les trouver au fur et à mesure de vos besoins lors de votre démarche de mise en conformité.

Ce livre n'a pas non plus la prétention de vous conseiller, plutôt celle de vous proposer comment faire pour avancer pas à pas.

Il se peut que vous ayez besoin d'aide à certains moments où l'expérience et la créativité pourraient vous faire défaut car certaines mesures de sécurité ne sont pas faciles à identifier. Dans ces cas-là, cette connaissance vous permettra d'avoir une demande périmétrée et qualifiée, ce qui vous évitera des mésaventures avec certains prestataires tant juridiques que techniques et ainsi, trouver les meilleures solutions pour votre projet selon vos zones de confort personnelles et vos budgets.

Grâce à ce livre vous resterez en maîtrise de votre projet de conformité. C'est de la complexité que naît la simplicité.

Comme de nombreux et nombreuses collègues, la complexité du RGPD dans la mise en œuvre opérationnelle ne m'a pas échappé et c'est en essayant, en recommençant, en améliorant et quelques fois en changeant tout, que petit à petit, j'ai trouvé comment répondre à mes exigences tout en facilitant le travail des opérationnels.

Mon objectif a toujours été d'autonomiser le plus vite les organisations sur ce sujet tout en leur permettant de faire évoluer leur conformité en fonction de leurs pratiques. Ce challenge est relevé.

Cette méthode écrite permet, et j'en suis particulièrement heureuse, de vous lancer sereinement dans votre projet de mise en conformité ou d'auditer le projet RGPD pour l'améliorer en continu.

Une des raisons fondamentales de la difficulté de la mise en œuvre du RGPD est la différence entre le conseil et l'opérationnel.

Vous avez certainement fait appel à du conseil en RGPD.

Le conseil vous dit ce qu'il faut faire au regard des obligations de la réglementation. Ce que le conseil ne vous dit pas, c'est comment le faire, cela est laissé à la libre interprétation des opérationnels, les acteurs de la conformité.

Une autre difficulté réside dans le fait que la maîtrise de la conformité nécessite de pouvoir actualiser les mesures de sécurité en fonction des changements de pratiques professionnelles. Souvent, les mises en conformité sont figées à un instant T, elles ne répondent donc pas à l'objectif premier de la réglementation qui souhaite une amélioration continue mais plutôt à l'urgence de la peur d'un contrôle imminent.

Cela dit, si le contrôle apparaît dans deux, trois ou cinq ans, souvent personne ne saura exactement ce qui a été fait, et ce que cela signifiait au moment où les questions ont été posées.

Il y a donc une différence entre conseiller dans la mise en œuvre de la conformité et faire de la conformité initiale et dynamique.

Je connais les deux facettes de cette unique pièce.

Je sais que la plupart des entreprises que j'ai conseillées, malgré la rigueur et l'exigence de mes recommandations n'ont pas pu faire des conformités à la mesure de mes exigences, et de celles de la réglementation pour des raisons de coûts, de ressources, d'engagement, d'outils, et de temps.

Je sais aussi que j'ai pu mettre en place des conformités initiales et dynamiques dont l'évolution est parfaitement maîtrisée et pourra le rester. C'est un pourcentage infime mais c'est de ce pourcentage qu'est sortie la méthode délivrée dans ce livre.

Nous tenons à ce que le plus grand nombre d'entreprises puissent mettre en place la réglementation dans leurs activités.

C'est pour nous, le levier d'un numérique responsable et d'un développement économique durable. C'est donc un petit livre pour nous faire du bien !