Paris, le 15 janvier 2011

Contribution de l'AFCDP à la Consultation de la Commission Européenne « Une Approche Globale de la Protection des Données à caractère Personnel dans l'Union Européenne »

Le Délégué à la protection des données : l'acteur essentiel du nouveau dispositif global de la protection des données personnelles.

L'AFCDP (Association Française des Correspondants à la Protection des Données Personnelles) a été fondée en 2004 après la création de la fonction de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour **Correspondant Informatique et Libertés**). Le CIL est la transposition en droit français « détaché à la protection des données à caractère personnel » prévu par la Directive 95/46/EC.

L'AFCDP est l'association représentative de cette profession émergente : plus de la moitié des entités ayant désigné un Correspondant Informatique et Libertés y adhère. Elle a pour objectif de :

- promouvoir la fonction de Correspondant et d'en faire un métier,
- proposer un cadre d'échanges en développant un réseau en France et à l'international,
- identifier les bonnes pratiques utiles aux Correspondants,
- représenter la fonction, en ayant la primeur de l'information, en agissant pour faire valoir la position de ces professionnels.

La richesse de l'AFCDP réside dans la diversité des profils des adhérents : CIL, juristes et avocats, responsables RH, informaticiens, professionnels du marketing et du e-commerce, déontologues, Risk Manager, universitaires et étudiants, experts en sécurité, qualiticiens …

Les travaux de l'association s'appuient sur une quinzaine de groupes de réflexion sur des sujets tels que : Durée de conservation, Géo localisation et Libertés, Données de santé, Données Clients et Prospects, Rôle et Missions du Correspondant Informatique et Libertés, Flux transfrontières, Notification des violations de traitements de données personnelles, Référentiels et labels, Réutilisation des données publiques.

S'appuyant sur sa connaissance concrète de la fonction de CIL et des pratiques des organisations en matière de protection des données personnelles, l'AFCDP souhaite apporter sa contribution à la Communication de la Commission sur les dispositions concernant l'« *Approche Globale de la Protection des Données à caractère Personnel dans l'Union Européenne* ».

Elle souhaite faire également un retour sur l'expérience acquise depuis 2004 par les DPO français pour éclairer le débat.

Le « DPO » en France

Le « DPO[1] » à la française a été introduit dans nos textes par la loi du 6 août 2004 modifiant la première loi de protection des données personnelles en France, la loi du 6 janvier 1978, dite « Loi Informatique et Libertés ». Il y est désigné comme le Correspondant à la protection des données personnelles qui est plus couramment dénommé CIL (pour Correspondant Informatique et Libertés). Sa mission est « *d'assurer, d'une manière indépendante, le respect des obligations prévues par la présente loi* ». Il ne se substitue pas au responsable de traitement qui reste responsable de la conformité du traitement aux exigences légales[2].

Sa désignation est laissée à la discrétion des responsables de traitement qui bénéficient toutefois de deux incitations :

- une incitation d'origine législative : ils sont exonérés de formalités de déclaration à la CNIL, sauf lorsque le traitement est assorti d'un flux hors de l'Union Européenne, ce qui est regretté
- une incitation à l'initiative de la CNIL, qui a créé un service et des outils spéciaux pour les Correspondants afin de leur apporter une aide spécifique dans l'exercice de leur mission.

Depuis cinq ans le nombre de CIL a très fortement cru : environ 8000 organismes ont nommé un CIL, certains partageant leur correspondant, plus de 2000 individus exercent cette fonction en France : chaque Français a aujourd'hui une partie de ses données personnelles traitée par un organisme qui agi sous la vigilance d'un CIL.

Depuis sa création en 2004, l'AFCDP a été témoin d'une réelle évolution des mentalités à la fois au sein des responsables de traitement et des « chargés » de la protection des données. Les premières interrogations levées, l'association a pu constater que le CIL est aujourd'hui la référence en matière de bonne protection des données à caractère personnel.

L'utilité du DPO est affirmée; tant pour les personnes concernées, qui trouvent en lui un interlocuteur, intermédiaire auprès du responsable de traitement, que pour le responsable de traitement qui bénéficie ainsi d'un avis expert sur la mise en œuvre des systèmes d'information de plus en plus nombreux et sophistiqués.

Bien au contraire, le nombre de professionnels du domaine, en interne comme en externe, ne cesse de croître, au point que l'on assiste à l'émergence d'une véritable profession, ce dont l'AFCDP se félicite.

---

[1] « Data Protection Officer »

[2] Le CIL peut être externe à l'entreprise lorsque moins de 50 personnes participent à la mise en œuvre du traitement ou y ont accès. Une proposition de loi adoptée par le Sénat le 23 mars 2010 ferait disparaître la distinction entre CIL interne et externe et rendrait obligatoire la désignation d'un CIL pour tout responsable de traitement lorsque plus de 100 personnes participent à la mise en œuvre ou ont accès au traitement, ou encore pour certains traitement particulièrement sensibles au point qu'ils sont soumis à autorisation préalable de la CNIL. Cette proposition n'a pas été encore été portée à l'agenda de l'Assemblée Nationale pour discussion.

L'approche globale de la Commission sur la protection des données personnelles

Les propositions de la Commission d'amélioration du cadre de la protection des données personnelles vont dans le sens des besoins perçus par l'association ; **et en particulier de sa volonté d'assurer une mise en œuvre concrète des règles par les Responsables de traitement.**

L'AFCDP est convaincue que les objectifs de la Commission ne peuvent être atteints que si les textes s'appuient sur le DPO.

En effet, si la protection des données doit être l'affaire de tous, l'expérience montre que la matière n'est pas d'abord facile. La règle juridique n'est pas toujours aisément transposable en pratique, que ce soit au niveau technique comme organisationnel. Le DPO joue ainsi un rôle essentiel auprès du responsable de traitement avant la mise en œuvre de tout traitement afin de veiller à sa conformité de bout en bout aux règles de protection des données (appréciation du respect du principe de légitimité et proportionnalité, mentions d'information, fonctionnalités pour l'exercice des droits, mesures de sécurité etc.). Le DPO est aussi présent auprès des préposés du responsable de traitement pour les sensibiliser aux règles qu'ils doivent respecter.

Ainsi, certains objectifs de la Commission mis en avant dans sa Communication, seront mieux servis en présence d'un DPO :

- **La transparence – mentions d'information**
  Quels que soient les efforts de transparence du responsable de traitement pour communiquer, les personnes concernées peuvent avoir du mal à comprendre certaines mentions d'information qui recouvrent des réalités complexes (publicité comportementale, utilisation de technologies émergentes, partage d'informations avec des tiers …); dans ces cas, **le DPO paraît être l'interlocuteur privilégié** pour apporter une réponse à leurs interrogations. Il pourrait être utile que les responsables de traitement ayant désigné un DPO communiquent ses coordonnées dans les mentions d'information destinées aux personnes concernées par le traitement.

- **La transparence - notification des violations de données**
  Afin d'éviter un engorgement au niveau des autorités de protection des données, d'éviter des émois inutiles et d'épauler le responsable de traitement, sans pour autant substituer à lui, **le DPO peut utilement jouer un rôle de filtre des violations** nécessitant une notification à l'Autorité d'une part, aux personnes concernées d'autre part, ou éventuellement un classement avec un ajustement des mesures de sécurité.

- **Améliorer le contrôle sur les données - droits d'accès**
  Il est plus simple et efficace que les demandes d'exercice des droits d'accès, de rectification ou d'opposition soient **centralisées auprès d'un DPO** afin qu'elles ne soient pas égarées et qu'elles soient traitées uniformément.

- **Responsabiliser le responsable de traitement**
  Le DPO, de par sa proximité avec l'organisation et le métier du responsable de traitement, doit être au cœur des initiatives relatives à l' « Accountability » telles que les **analyses d'impact**, les codes de conduite, les travaux menant à la certification et à l'autorégulation, la prise en compte du « **Privacy by Design** » et du « **Security by Design** ».

  En France, le CIL intervient en amont de tout projet de traitement de données ; et pour mener à bien sa mission doit procéder à une **analyse des conséquences** du projet sur la vie privée et les libertés individuelles des personnes concernées. C'est à partir de cette analyse qu'il va indiquer au responsable de traitements si le projet nécessite l'intégration de certaines fonctionnalités au stade même de la conception. Le DPO joue donc un rôle clé dans le processus de « **Privacy by Design** » et du « **Security by Design** ».

  En outre, les textes français prévoient que le CIL doit établir un bilan annuel qui est remis au responsable de traitement. Cette spécificité française nous paraît une mesure concrète répondant à l'objectif de « responsabilisation » du responsable de traitement.

Pour ces raisons, **les autorités européennes devraient faire du DPO un acteur incontournable de la nouvelle approche de la protection des données personnelles. Il s'agit à notre sens de la mesure phare de mise en œuvre du principe d' »Accountability », prôné par la Commission dans son approche nouvelle de la protection des données personnelles.**

Par conséquent, il nous paraît important pour la protection des données que les lois des Etats membres réservent toutes une place à la fonction de DPO, ce qui n'est pas le cas à l'heure actuelle où cette question a été laissée à la discrétion des Etats membres.

Il est également essentiel de rendre attrayante la nomination d'un DPO, sa présence auprès d'un responsable de traitement étant le meilleur moyen pour garantir le respect de la vie privée à l'heure numérique, par l'autorégulation. Un allègement de formalités, y compris en cas de transfert hors UE[3], accompagné d'un certain nombre d'autres mesures incitatives pourraient engendrer la nomination d'un nombre significatif de DPO, ce qui éviterait le risque d'une obligation qui pourrait être impopulaire.

Si le principe de la désignation obligatoire était retenu, il serait préférable de retenir un critère qualitatif et non quantitatif, car le risque que représente un traitement dépend moins du nombre de personnes qui interviennent dans le processus que de la sensibilité des données, de la finalité ou de la technologie utilisée.

[3] Lorsque les données sont protégées par les Clauses Standards de la Commission ou des BCR approuvées par les Autorités compétentes.

Par ailleurs, l'obligation de désignation d'un DPO entraînerait plusieurs milliers de désignations. Il conviendrait d'accompagner ce mouvement pour garantir que le DPO obligatoire améliore réellement le niveau de protection des données personnelles. Plusieurs mesures du pourraient y contribuer fortement :

- Une définition précise du cadre d'exercice de la fonction ;
- Un délai de mise en œuvre de l'ordre de 36 mois afin de permettre aux personnes ayant vocation à exercer ces fonctions de s'y préparer, notamment par de la formation et de permettre aux responsables de traitement de se préparer à accueillir cette nouvelle fonction;
- Laisser au responsable de traitement le libre choix de recourir à un ou plusieurs DPO interne ou un DPO externe, comme un consultant ou un avocat par exemple, en fonction de son organisation, de ses besoins et de ses capacités.

Nous appelons également à un débat autour de la qualification des DPO, toujours dans l'optique d'améliorer leur efficacité et le sérieux de la fonction. A terme, une réglementation de la profession peut être envisagée.

En tout état de cause, pour que la mesure soit efficace, il faut que le texte adopté soit suffisamment précis quant aux missions, moyens et garanties encadrant la fonction de DPO. A ce titre, l'étude comparative réalisée par l'AFCDP montre une grande disparité dans les régimes adoptés par les Etats membres. Une harmonisation serait souhaitable et offrirait de meilleures garanties aux consommateurs, salariés et autres personnes dont les données sont traitées au sein des frontières européennes.

En juin 2009, l'AFCDP a élaboré un tableau comparatif des différentes législations européennes ayant adopté un « délégué à la protection des données », qui figure en pièce jointe.

Enfin, s'inspirant du principe de réciprocité mis en avant par la Commission, l'AFCDP aspire à la reconnaissance d'un « DPO européen » qui pourrait officier pour un groupe de sociétés présent dans différents pays de l'Union Européenne et le faire bénéficier des avantages liés à la fonction de DPO dans chacun de ces pays par réciprocité.

L'AFCDP reste à la disposition de la Commission pour contribuer aux réflexions qu'elle souhaiterait mener sur la fonction de DPO.

* *

Annexes : tableaux comparatifs des délégués à la protection des données personnelles en Europe (3 documents)