

**Etude réalisée dans le contexte de la conférence AFCDP sur la
NOTIFICATION DES « ATTEINTES AUX TRAITEMENT DE DONNEES
PERSONNELLES »**

Palais du Luxembourg – Paris - 23 mars 2010

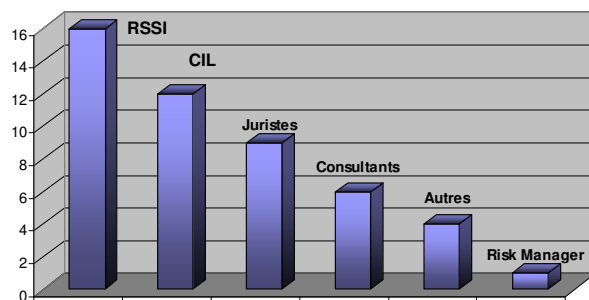
*Pilote du questionnaire : Bruno RASLE, Délégué général AFCDP, charge-mission@afcdp.net
Date : lundi 22 mars 2010*

Contexte : Ce rapide sondage a été réalisé auprès des personnes inscrites à la conférence organisée le mardi 23 mars 2010 afin de disposer d'éléments de réflexion pour alimenter les débats et préparer les travaux du groupe de travail AFCDP « Notification des atteintes aux traitements de données personnelles ». Cinquante questionnaires ont été renvoyés.

Note 1 : Ce questionnaire a été réalisé avant la conférence et reflète donc la position des participants préalablement à la découverte et la prise en compte d'un certain nombre d'éléments qui peuvent les amener à modifier leur ressenti et leur position.

Note 2 : Ce questionnaire n'a pas valeur de sondage du fait, entre autres, de la non qualification du panel.

1 – Quelle est votre fonction principale ?

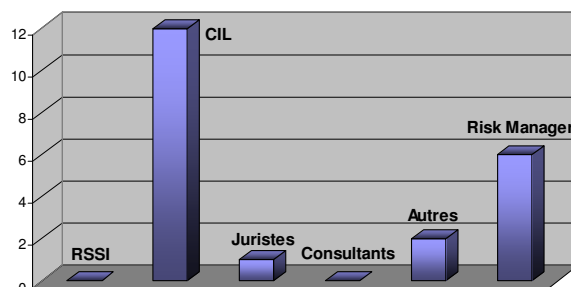


La fonction « Juristes » comporte également les avocats.

Les Consultants sont en majorité spécialisés dans la sécurité informatique.

Parmi les autres fonctions figure un responsable PRA/PCA.

2 – Quelle est votre éventuelle fonction secondaire ?



Nombreux sont les RSSI qui sont également désignés Correspondants Informatique et Libertés auprès de la CNIL.

3 – Quelle organisation mettre en place ? Quels seront les risques juridiques ?

La question était ainsi formulée : « *Que venez-vous chercher principalement à l'évènement organisé le 23 mars par l'AFCDP ?* ».

Les réponses possibles étaient :

- Des réponses à mes questions dans le domaine technique principalement (protection contre les pirates, détection des fuites de données, chiffrement de données personnelles, traçabilité des accès aux données, etc.)
- Des réponses à mes questions dans le domaine juridique (responsabilités, risques associés, clauses contractuelles, etc.)
- Des réponses à mes questions sur l'organisation, sur les méthodologies et les processus liés à une éventuelle notification (personne ou groupe de personnes chargées de ce sujet, rôle du CIL, certification ISO 27001 ou ITIL, certification PCI, Sarbanes-Oxley, information de nos clients, communication de crise, etc.)

80% des répondants viennent chercher des réponses concernant principalement l'organisation à mettre en place (procédures, démarches structurées, etc.) et ils sont 70% à attendre des précisions d'ordre juridique (précisions sur le texte, périmètre d'application, risques induits, etc.).

Compte-tenu de la composition du panel il n'est pas surprenant que seuls 24% d'entre eux aient besoin d'informations techniques, en majorité les juristes et avocats.

4 – 62% des participants sont actuellement favorables à cette mesure

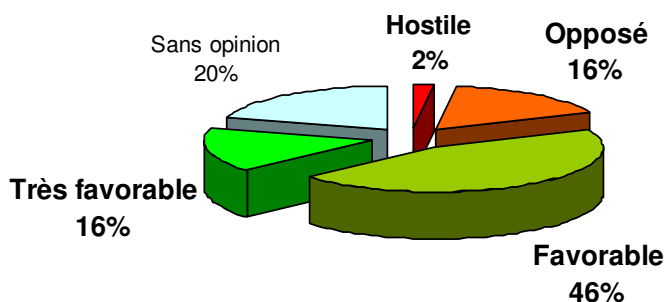
La question était : « *Quelle est, actuellement, votre attitude générale vis-à-vis de la proposition visant à rendre obligatoire la notification des atteintes aux traitements de données personnelles ?* ».

Les réponses possibles allaient de « *J'y suis totalement hostile* » à « *J'y suis très favorable* ».

Un seul répondant (2%) est hostile à la mesure, huit y sont opposés.

62% y sont favorables, voire très favorables.

On notera, sans trop de surprise, que la totalité des consultants sécurité sont très favorables à la mesure...



Voici les réponses remarquables, dans chaque catégorie :

Hostile ou opposé à la mesure :

« *Le texte est trop imprécis : il concerne toute atteinte et il suffit d'une seule personne concernée. De plus, l'avertissement à faire aux personnes est au bon vouloir de la CNIL* ».

« *Cela peut engendrer pour l'entreprise des risques juridiques ou financiers supplémentaires, sans apporter en contrepartie de véritables opportunités ou de moyens nouveaux permettant d'améliorer le niveau de sécurité du SI impliqué ou de réparer les dommages occasionnés, souvent irréversibles* ».

« *Il existe déjà dans la loi actuelle informatique et libertés une incitation forte pour que le responsable du traitement prenne toutes les mesures indispensables pour assurer la protection des données personnelles* ».

« *Nous perdrons le contrôle de notre communication, sur le calendrier et la priorisation de la couverture de nos risques. Et qui prendrait en charge les coûts induits ?* »

« *Il faut définir ce qu'est une faille de sécurité et le processus à mettre en place en cas d'atteinte* »

« Le principe général semble bon mais il me semble très difficile de généraliser des dispositifs qui permettent de centraliser les informations et de garantir un résultat exhaustif et uniforme entre les entreprises. A titre d'exemple, les solutions de type DLP (Data Loss Prevention) qui permettent de détecter d'éventuelles fuites sont aujourd'hui très marginales en France ».

« Je m'interroge sur la compatibilité au regard du respect des droits fondamentaux. Le fait de devoir notifier les failles de sécurité à la CNIL qui dispose du pouvoir de prononcer des sanctions administratives et/ou de transmettre le dossier au parquet ne serait-il pas en contradiction avec le droit de ne pas s'auto-incriminer ? »

« J'y suis opposé... mais uniquement parce que cela ne me paraît pas réaliste. On peut demander à un responsable de traitement de déclarer les atteintes extérieures à la sécurisation des données personnelles qu'il traite, mais il est illusoire de penser que, de lui-même, il le fera pour ses propres failles. Ou alors, il les camouflera d'une manière ou d'une autre et on aura un effet inverse à celui recherché ».

« Deux raisons principales à mon opposition : la première est l'engorgement de la CNIL, la seconde est qu'il faut faire confiance aux entreprises et à leurs CIL : il faut prévoir la possibilité pour le CIL d'avertir la CNIL s'il pense que le sujet est traité à la légère dans l'entreprise, et non une obligation »

Favorable, voire très favorable à la mesure :

« La propagation des données via Internet et les évolutions technologiques laissent prévoir de réels dangers sur les données personnelles, aspects qui sont trop souvent négligés en entreprise, notamment les sociétés privées »

« Enfin un moyen de casser le mur du silence prévalant en France sur ces événements »

« Pour contraindre les entreprises à se préoccuper réellement de la sécurité des informations qu'elles manipulent »

« Cette notification permettra de limiter les risques en matière d'usurpation d'identité »

« Cette loi serait est un levier puissant pour mettre en place, optimiser, procéder ou simplement exploiter les outils existants (ce qui aurait dû être le cas depuis longtemps) »

« Dans le cadre de mon entreprise, cette mesure peut favoriser la désignation d'un CIL »

« Ne serait-ce que pour s'aligner avec le cadre HIPAA HITECH ACT »

« Le CIL devrait se voir confier l'appréciation de l'opportunité de saisir la CNIL, dans les seuls cas de violation grave d'un traitement de données à caractère personnel ».

« Les entreprises vont prendre vite conscience de la nécessité de maîtriser et protéger leur patrimoine informationnel – y compris les données personnelles – pour éviter les impacts financiers et sur l'image de marque »

« La tendance semble être internationalement engagée, notamment au sein de l'U.E., y-a-t-il vraiment possibilité de ne pas suivre ? »

« J'y vois une garantie forte de conformité à la loi Informatique et Libertés »

« Pour renforcer les règles de sécurité. Obligation de notification uniquement si risque de préjudice aux personnes, sinon notification au CIL avec tenu d'un registre interne tenu à disposition de l'autorité de contrôle ».

« Cinq ans après la refonte de la Loi, il peut paraître normal pour la CNIL de ne plus se contenter que des bonnes intentions ».

« Malheureusement c'est la seule façon que soit enfin prise au sérieux la sécurisation des données personnelles et ce serait un levier majeur pour que le CIL prenne de l'importance ».

« Cela va accroître la responsabilité des responsables de traitements et la transparence de leurs traitements vis-à-vis des personnes concernées ».

« Cette mesure va favoriser la transparence et permettre à la CNIL de suggérer/imposer des mesures complémentaires en cas d'impact majeur »

« Cela va obliger les responsables de traitement ne se sentant pas concernés par la sécurité des données personnelles à se saisir du problème ».

« Cette mesure est le meilleur argument dont disposerait un CIL pour convaincre à la fois les dirigeants et les RSSI de leur intérêt à toujours intégrer la protection avant la mise en œuvre d'une application (« Privacy by Design ») »

« La mesure devrait renforcer le CIL, personne en charge de la conformité Informatique et Libertés au sein de l'entreprise, sous réserve qu'il dispose de moyens pour mener à bien ses missions ».

« Cela permettrait de bénéficier d'un levier supplémentaire important pour mettre en place une politique formalisée de sécurité des SI, souvent absente dans les petites et moyennes structures ».

« Cela obligera les acteurs concernés à prendre des mesures réelles pour sécuriser leur système d'information. Indirectement cela permettra aux CIL de travailler dans un contexte plus favorable car la crainte d'une sanction CNIL n'est pas présente chez la plupart des auteurs des traitements. Auteurs qui appréhendent la loi Informatique et Liberté uniquement comme une contrainte et qui estime que la Cnil n'a pas les moyens de sa politique. En stratégie business le risque Cnil est identifié comme faible »

« Cela m'aiderait à diffuser la culture informatique et libertés, surtout en cas de mise en place de nouvelles technologies (cybersurveillance notamment) »

« Ayant moi-même subi la diffusion de mes données par des opérateurs et ayant travaillé pour/avec des sociétés ayant perdu des données sans que les dirigeants prennent la décision d'en avertir les personnes concernées, je suis très sensibilisé à ce sujet ».

« Au delà de la mise au pilori que toute entreprise défaillante peut craindre, les notifications peuvent permettre une prise de conscience plus générale des violations de la vie privée que permet un traitement de données personnelles non conforme »

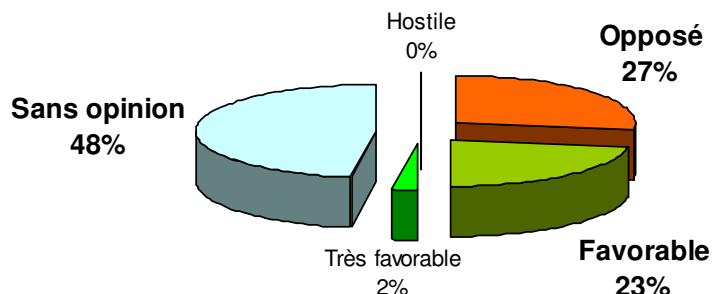
« La mesure va dans le bon sens : renforcement de la protection des données personnelles, renforcement de la protection du patrimoine informationnel de l'entreprise, meilleure gestion de risques, renforcement de la gouvernance des risques ».

« Démultiplication de l'efficacité de la CNIL ».

« La gestion du risque est étroitement liée à la perception de ce dernier. Les notifications des atteintes aux traitements des données personnelles développeront une culture sécurité, qui touchera non seulement les responsables des SI mais aussi les décisionnaires »

« C'est un formidable levier pour adapter les moyens pour la mise en conformité Informatique et Libertés »

5 – Quelle est – à votre avis – la position de votre entité vis-à-vis de la proposition visant à rendre obligatoire la notification à la CNIL des atteintes aux traitements de données personnelles ?



La question était « *Quelle est – à votre avis – la position de votre entité vis-à-vis de la proposition visant à rendre obligatoire la notification à la CNIL des atteintes aux traitements de données personnelles ?* ». Il s'agit bien de l'accueil supposé des organismes (entreprises, collectivités, administration, etc.)

L'un des nombreux répondants « sans opinion » indique que le sujet est trop « neuf » pour que les porteurs d'enjeux au sein de l'entreprise se mobilisent et ajoute « *Quoiqu'il en soit il me semble du devoir et des missions conjointes du CIL et du RSSI de le porter et de se faire sponsoriser au sein de l'entreprise* ».

Quelques réponses remarquables :

Je pense que mon organisme y est opposé, pour la raison principale suivante :

« *Difficulté dans la mise en œuvre d'une telle mesure, à commencer par le périmètre : Nous ne sommes pas certains que le recensement interne de tous nos fichiers à données personnelles soit exhaustif* »

« *Certaines idées ont la vie dure : « On n'a pas grand-chose à protéger... personne n'aurait l'idée de venir nous voler des données personnelles... il y a peu de risques de se faire prendre... » »*

« *Encore une loi qui va gêner l'activité des entreprises* »

« *Risque de contre publicité et dégradation de l'image de la société* »

« *Moins une erreur est visible, meilleures sont les relations avec les clients et les autorités de tutelle* »

« *La mise en place sera très lourde, avec des changements de méthodes et des modification d'outils* »

« *Données personnelles ? Les équipes informatiques ne comprennent tout simplement pas de quoi il s'agit* »

« *Même si le principe général semble bon il me semble très difficile de généraliser un tel dispositif de façon à garantir un résultat exhaustif et uniforme entre les entreprises* »

« *Cela va générer plus de travail et engendrer des coûts supplémentaires* »

« *La peur de la publicité éventuelle qui pourrait en résulter, et la perte consécutive de clients* »

Je pense qu'elle y est favorable, voire très favorable, pour la raison principale suivante :

« *Disposer d'un moyen de pression pour contraindre les entreprises à se conformer à un certain niveau de sécurité* ».

« *Conformité et déontologie vis a vis des réglementations* »

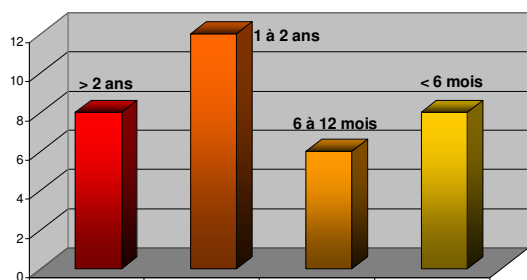
« *Des modalités similaires existent déjà aux Etats-Unis* »

« Notre société est une entreprise citoyenne »

« Nous travaillons dans un secteur hautement réglementé. Tout ce qui est en rapport avec la conformité avec une réglementation est pour nous prioritaire. A contrario, tout ce qui est en dehors d'une réglementation explicite et précise risque d'être considéré comme un peu superflu... »

« Par souci de transparence. A noter que bien que non légalement obligatoire, mon entreprise a déjà reporté à la CNIL une faille de sécurité survenue dans un passé récent ».

6 – Les trois quarts des répondants auront besoin d'avantage de temps pour être en mesure d'appliquer la notification que les six mois évoqués par la proposition de loi.



La question posée était « Dans l'hypothèse où la proposition de loi visant à rendre obligatoire la notification à la CNIL des atteintes aux traitements de données personnelles est promulguée, combien de temps faudra-t-il, à votre avis, à votre entité pour s'y conformer pleinement ? »

Sans surprise les grandes entreprises déclarent avoir besoin de plusieurs années pour être en mesure d'appliquer une

telle disposition.

Voici les réponses remarquables **pour les durées supérieures à un an** :

« Au niveau mondial, nous estimons qu'il nous faudrait quatre à cinq ans pour respecter une telle obligation. Cela nécessiterait une mobilisation de départements très divers, une communication / sensibilisation pour tous nos établissements, l'adaptation de notre politique de sécurité... »

« La multiplicité de nos systèmes d'information et des opérateurs de traitements risque de rendre difficile notre mise en conformité par rapport à cette mesure : organisation, identification des responsables de traitements, sensibilisation/communication, contrôle de l'application de la mesure etc. »

« Analyse des risques et mesure de formation à mettre en œuvre, éducation, et mise à niveau des processus »

« Il s'agit d'une procédure à l'échelle mondiale »

« Ce serait une véritable révolution culturelle pour des européens ! »

« Notre groupe comporte de nombreuses filiales, en France et à l'étranger : Etat des lieux « sécurité » à faire, procédures à installer, budgets à dégager, planification des actions à mener, adhésion des différents acteurs à obtenir, sensibilisation et de communication visant à renforcer la vigilance de l'ensemble des collaborateurs, procédures de notifications à installer en interne pour faire remonter les failles vers le CIL, audit des contrats de sous-traitance pour prévoir des clauses de remontée des failles vers l'entreprise... »

« Il me semble difficile que cela prenne moins de temps : la route est longue pour faire entrer une nouvelle culture dans une grande organisation ».

« La prise de conscience de la sécurité est récente dans l'entreprise et nous n'avons pas encore désigné de CIL malgré mes demandes répétées »

« Prioritisation vis-à-vis des autres projets business »

« Le temps de former le CIL, le temps qu'il mette en œuvre les bonnes méthodes pour traquer les intrusions, le temps d'acquiescer les bons outils de surveillance... »

« Un travail d'évangélisation est nécessaire dans toute entreprise pour expliquer les enjeux de la loi, les juristes devront l'examiner et donner, en s'appuyant sur des experts, les risques pour la société, de plus il faudra considérer la loi dans son ensemble et non pas seulement l'atteinte aux traitements de données personnelles »

« On part de zéro : pas d'étude de valeurs ni de risques, faible formalisme concernant la gestion des identités, des rôles et des accès, mais surtout frein conséquent au niveau des équipes SI ».

« Nous sommes en phase de restructuration ce qui compliquerait fortement la mise en place des structures nécessaires »

« C'est le délai standard nécessaire afin de mettre en place une évolution significatif des systèmes d'information et des processus associés ».

« Le temps de présenter une procédure détaillée à la Direction Générale et de mettre en place les orientations validées par la Direction Générale au sein de l'entité (dont la définition d'une politique de sécurité) »

« C'est essentiellement un problème hiérarchique : les dirigeants de société sont difficiles à convaincre et les moyens donnés au CIL sont inexistantes. Le processus sera donc long ».

Pour les réponses inférieures à l'année :

« J'estime à un an environ la mise en place de nouvelles procédures. Moins si le phasing est très strict et qu'il y a un relai des autorités de tutelle ».

« Il me semble que la mise en œuvre de la proposition ne nécessite pas de moyens très complexe mais surtout un minimum d'organisation »

« Etant déjà soumis à PCI DSS et SOX, un certain nombre de synergies quant aux mesures sont identifiables »

« Pratique et organisation sont déjà en place. Besoin éventuel d'un « ajustement » en fonction des dispositions légales françaises qui seront arrêtées ».

« ...compte tenu du faible nombre de failles constatées jusqu'à présent ».

« Notre société dispose des instances et mécanismes de gouvernance, d'organisation et techniques permettant d'être conforme le cas échéant »

« Nous sommes une petite structure »

« Nous avons l'habitude des cadres réglementaires, nous avons un très fort niveau de sécurité : Nous serions prêts le cas échéant »

« Il faudrait que nous formions notre CIL sur le volet technique, la sécurité informatique »

« Dans mon organisme les données personnelles sont surtout des données de santé, donc très sensibles, toute atteinte serait rapidement détectée, et si la loi le demande, la notification à la CNIL serait rapide »

« Si nous devons notifier, nous le ferons. La difficulté consiste à détecter, le cas échéant, les atteintes »