RECOMMANDATIONS CNIL :

CINQ CLES POUR METTRE SON SITE EN CONFORMITE

La loi du 6 août 2004 a modifié la loi informatique et libertés et renforce les pouvoirs de la CNIL. Rappel des obligations et des recommandations pour les sites Internet avec l'autorité compétente en matière de protection des données personnelles.

A. Déclarer son site à la CNIL

Mis à part les sites créés par des particuliers dans un but uniquement privé, tout site Internet diffusant ou collectant des données personnelles doit être déclaré à la CNIL (Commission nationale de l'informatique et des libertés). Il s'agit là des informations permettant d'identifier "directement ou indirectement" une personne physique. Cela peut être bien sûr les noms ou prénoms, l'adresse, mais aussi la taille ou encore le numéro de sécurité sociale. Entreprises, associations et particuliers dont le site n'a pas une vocation privée doivent donc déclarer leurs sites. Elles ont la possibilité de le faire en ligne sur le site de la CNIL en indiquant notamment le prestataire éventuel ainsi que le responsable (organisme ou particulier) chargé de gérer le droit d'accès des internautes. Tout manquement à la déclaration peut entraîner des sanctions pénales. A ce sujet, la loi a accordé à la CNIL des pouvoirs de contrôle et de sanctions administratives, pénales et financières (jusqu'à 300.000 euros).

B. Le correspondant CNIL

Depuis le décret d'application du mois d'octobre 2005, les sites ont une alternative : déclaration ou désignation d'un "correspondant à la protection des données." La création d'un tel poste dispense d'une déclaration à la CNIL, sauf si les données recueillies ont vocation à être transmises à l'extérieur de l'Union européenne. La nouvelle loi "informatique et libertés" 2004, prévoit la création d'un "correspondant à la protection des données." Désigné par le responsable de la mise en oeuvre du site, il doit "bénéficier des qualifications requises" (non précisées) pour veiller à l'application de cette loi. Il lui faut notamment tenir le registre des traitements de données effectués. Interlocuteur de la CNIL, il ne peut être sanctionné pour les actions d'un des responsables du site. Cependant, la CNIL peut le décharger de ses

fonctions en cas de manquement à ses obligations. Un correspondant peut tout à fait ajouter ce rôle à ses autres fonctions. Il peut aussi être mutualisé entre plusieurs sites. Malgré cela, seuls 130 organismes auraient jusqu'à présent fait le choix du correspondant. Pas encore disponible en ligne, la déclaration du correspondant doit être téléchargée et imprimée puis envoyée à la CNIL.

C. Bien informer l'internaute

La transparence vis-à-vis des utilisateurs constitue la base de nombreuses obligations à remplir. Les responsables du site devront veiller à fournir en ligne le maximum d'informations. Ainsi, les renseignements récoltés le cas échéant, par exemple dans un formulaire, devront être accompagnés d'une mention précisant le caractère obligatoire ou facultatif des réponses. Il faut également clairement expliquer la finalité de ces renseignements. Si elles sont susceptibles d'être vendues ou de servir un but commercial, il faudra au site l'accord des utilisateurs, sous la forme par exemple d'une case à cocher. Le site devra avoir une procédure pour les personnes souhaitant modifier les données les concernant. Pour les forums de discussion, l'existence d'un modérateur n'est pas obligatoire mais l'éditeur du site y a tout intérêt puisque il est responsable des propos tombant sous le coup de la loi qui y seraient tenus. La présence d'un modérateur doit être annoncée et il faut rappeler aux participants l'interdiction d'utiliser les données personnelles apparaissant sur le forum.

D. La conservation des données

La CNIL recommande de signaler les procédés de collecte de données (cookies, applets Java), leur raison d'être ainsi que les procédures dans les navigateurs permettant de les modifier ou de les supprimer. Même si les internautes ont donné leur accord pour que des informations personnelles soit conservées, il faut que leur durée de conservation soit "proportionnelle à la finalité de leur traitement." Pour aller plus loin que ce principe général, la CNIL préconise un an maximum ou après le deuxième sollicitation restées sans réponse. Les recommandations ne s'appliquent pas uniquement aux utilisateurs. Pour les sites BtoB notamment, les données des personnes ayant des liens contractuels avec eux ne devraient pas être conservées plus longtemps que "la durée pendant laquelle le contrat peut être contesté."

E. Définir les rôles de ses prestataires

Que le site soit sous-traité pour son développement, son hébergement ou sa gestion, l'organisme présent sur Internet doit s'assurer que les rôles de chacun sont clairement établis.

Un blog, par exemple, fera souvent appel à une plateforme d'hébergement dotée d'un règlement spécifique. Certains professionnels choisissent d'intégrer le blog à leur site pour pouvoir mieux le contrôler. En cas de gestion du site externalisée, il faudra préciser la mission du prestataire en matière de sécurité informatique.

Si les prestataires ont un devoir d'information, la CNIL rappelle qu'il faut vérifier que le contrat liant l'organisme client au sous-traitant engage ce dernier "à prendre les mesures nécessaires pour assurer la sécurité informatique des données." S'assurer aussi de l'obligation de confidentialité du prestataire pour les informations personnelles qu'il aurait à connaître. Enfin, le contrat doit contenir l'interdiction d'utiliser à des fins commerciales ces données. C'est l'organisme possédant le site qui serait pénalement responsable de permettre l'accès des données à un tiers non autorisé.

Baptiste RUBAT du MERAC, JDN