

Protection des données personnelles: un réel défi pour notre société

Par Taïeb DEBBAGH



Docteur en Informatique des organisations Paris Dauphine, Taïeb Debbagh est enseignant à l'Université Internationale de Rabat. Ancien secrétaire général du département de la Poste, Télécommunications et Technologies de l'information, il est vice-rapporteur de la Q22 "Cybersécurité" de l'Union internationale des télécommunications.

L'article premier de la loi 09-08, précise que «l'informatique est au service du citoyen et évolue dans le cadre de la coopération internationale. Elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'homme. Elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens». Selon certains chercheurs, le concept de vie privée est généralement associé à la culture occidentale, qu'il n'est pas universel et reste virtuellement inconnu dans d'autres cultures. C'est dans ce contexte qu'il est nécessaire que les différentes composantes de la société marocaine doivent intégrer ce concept dans leur quotidien.

Cette loi, votée en décembre 2008 et relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, répond à un triple objectif :

1- Mettre à niveau l'arsenal juridique marocain en tenant compte de la directive européenne 95/46/CE, ainsi que la Convention n°108 pour la protection des données personnelles du Conseil de l'Europe;

2- Protéger le citoyen et toute personne vivant sur le territoire marocain contre l'utilisation abusive de ses données personnelles;

3- Favoriser le développement du BPO (Business Process Outsourcing) qui représente des opportunités importantes dans le cadre du plan Emergence. Cet article abordera les obligations des responsables de traitements, ainsi que les droits des personnes quant à la collecte, l'enregistrement et l'utilisation des données à caractère personnel les concernant.

. Obligations des responsables de traitements

Le responsable du traitement est défini par la loi, comme étant «une personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui détermine les finalités et les moyens du traitement de données à caractère personnel». En d'autres termes les dirigeants des banques, des assurances, des opérateurs télécom, des centres d'appel, des entreprises, des administrations, des collectivités locales et des associations sont tous des «responsables de traitements». Car ils sont les premiers responsables de la gestion des données à caractère personnel et pour cela ils doivent se conformer à la loi avant le 31 août 2012 (deux années après l'installation de la CNDP: Commission nationale de la protection des données personnelles). Cette échéance concerne les traitements effectués avant la promulgation de la loi ; par contre les nouveaux traitements doivent faire l'objet de déclaration ou de demande d'autorisation auprès de la CNDP, avant la date de leur mise en œuvre. Le responsable du traitement, tel que définit plus haut, a l'obligation de déclarer à la CNDP l'ensemble des traitements effectués sur des données à caractère personnel; il n'a le droit de les traiter que suite au consentement de la personne concernée. Cependant, le consentement n'est pas obligatoire dans certains cas, tels que le respect d'une obligation légale, l'exécution d'un contrat et la sauvegarde des intérêts vitaux de la personne. Cette déclaration comporte l'engagement que les traitements seront effectués conformément aux dispositions de la loi 09-08, et elle doit être déposée auprès de la CNDP, contre récépissé. Ces déclarations permettront à la CNDP d'exercer ses compétences, en vue de contrôler le respect des dispositions de la loi. Le responsable du traitement est tenu de demander une autorisation préalable auprès de la CNDP lorsque ces traitements concernent des données sensibles (origine raciale, opinion politique, état de santé...), les données relatives aux infractions et condamnations, ou s'il doit utiliser les données personnelles à d'autres finalités que celles pour lesquelles elles ont été collectées. Selon l'article 23 de la loi, «le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre tout autre forme de traitement illicite. Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger».

. Droits des personnes concernées

Le chapitre II de la loi 09-08 est consacré aux droits des personnes concernées par le traitement de leurs données personnelles:

- **Droit à l'information:** Toute personne sollicitée directement, en vue d'une collecte de ses données personnelles, doit être préalablement informée de manière expresse, précise et non équivoque par le responsable du traitement;
- **Droit d'accès:** Toute personne, justifiant de son identité, a le droit d'obtenir du responsable du traitement, la communication des données à caractère personnel la concernant, faisant l'objet d'un traitement, l'information relative à la finalité de ce traitement et les destinataires auxquels ces données sont transmises;
- **Droit à la rectification:** Toute personne a le droit d'obtenir du responsable du traitement l'actualisation, la rectification et l'effacement des données à caractère personnel dont le traitement n'est pas conforme à la présente loi. En cas de refus, la personne concernée peut introduire une demande de rectification auprès de la CNDP;
- **Droit d'opposition:** Toute personne a le droit de s'opposer, pour des motifs légitimes, à ce que ses données fassent l'objet d'un traitement;
- **Prospection directe:** Est interdite toute prospection directe au moyen d'automate d'appel, d'un télécopieur, d'un courrier électronique ou équivalent, qui utilise les coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes. Dans ce cas également la personne concernée peut introduire une plainte auprès de la CNDP.

. Préparation pour la conformité

La conformité à la loi 09-08 nécessitera, pour plusieurs organismes sous l'impulsion de leurs dirigeants, la mise en place d'une équipe projet composée de juristes, de responsables métiers, d'informaticiens et pilotée par le responsable de la conformité (si présent au sein de l'organisation), en vue d'analyser les interactions avec d'autres lois et réglementations en vigueur, et d'établir la cartographie des traitements concernant les données à caractère personnel et sensibles. Suite à cela, un plan d'action rigoureux doit être établi afin d'assurer la conformité de leur organisation avant le 31 août 2012, comme précisé ci-dessus et tel que stipulé par l'article 67 de la loi. A l'instar des pays européens, il serait judicieux de désigner des correspondants de la protection des données personnelles (CDP) pour prendre en charge et coordonner la mise en conformité à la loi 09-08. En France, un texte de loi est en préparation en vue de rendre obligatoire la présence d'un correspondant informatique et liberté (CIL) pour

les organismes répondant à certains critères, alors qu'en Allemagne c'est déjà le cas. Ceci dit, les articles 51 à 66 de la loi prévoient des sanctions qui varient entre 10.000 DH et 300.000 DH d'amende et des peines d'emprisonnement de trois mois à deux ans, selon la gravité de l'infraction commise, à l'encontre de tout responsable, sous-traitant et toute autre personne qui, en raison de ses fonctions, est chargée de traiter des données à caractère personnel et les données sensibles. La sévérité de la loi donnera à réfléchir à plusieurs dirigeants qui devront définir rapidement les rôles et les responsabilités au sein de leur organisation, et mettre les moyens nécessaires à la mise en conformité, d'autant plus que la charge de travail est loin d'être négligeable.

Définition des principaux concepts

- **Données à caractère personnel:** toute information concernant une personne physique identifiée ou identifiable. Cette information peut être sous format numérique de différentes natures tel que fichier, base de données, image, vidéo et son. Les supports papier sont également concernés;
- **Personne identifiable:** individu qui peut être reconnu directement à travers son nom par exemple ou indirectement à travers un identifiant, tel que le numéro de CIN ou le numéro d'immatriculation de son véhicule;
- **Traitement de données à caractère personnel:** toute opération de collecte, de stockage, d'enregistrement, d'extraction, de communication effectuée par des procédés automatiques ou manuels, sur des données personnelles telles que le nom, le prénom, la date de naissance, le numéro de téléphone ou l'adresse;
- **Données sensibles:** les données sur la personne qui révèlent son origine raciale ou ethnique, ses opinions politiques, ses convictions religieuses, son appartenance syndicale, ainsi que les informations relatives à son état de santé y compris les données génétiques.

Exemples d'utilisations abusives des données à caractère personnel

• Mai 2010: Des banques trop curieuses?

La CNIL a reçu une quarantaine de plaintes d'usagers de banques. Clients de leur banque depuis plusieurs années, il leur est pourtant demandé la copie d'une pièce d'identité et /ou de leur envoyer un questionnaire détaillé sur leur situation familiale ou financière. Un texte récent, relatif à la lutte contre le blanchiment d'argent et le financement du terrorisme impose, en effet, aux établissements financiers de recueillir des informations auprès de leurs clients. Les banques recueillent d'autres renseignements sur la situation professionnelle, économique et financière de leurs clients (justificatif de domicile, activité professionnelle exercée actuellement, revenus et autres ressources, patrimoine...), qui ne correspondent pas à la finalité de la problématique du texte relatif au blanchiment d'argent.

- **Mars 2009: Marketing ciblé sur internet: vos données ont de la valeur**

Publicité personnalisée, contextuelle ou comportementale, la CNIL fait le point dans un rapport rendu public sur ces différentes techniques de publicité ciblée en ligne, sur leurs risques d'atteintes à la vie privée et les parades possibles. Vous réservez un billet d'avion pour New York sur Internet. Plus tard, en lisant votre quotidien en ligne, une publicité vous propose une offre intéressante pour une location de voitures à New York. Ce n'est pas une simple coïncidence: il s'agit de la publicité ciblée, basée sur vos données personnelles (adresse IP, destination, etc.). Le modèle économique de nombreuses sociétés phares d'Internet comme Google ou Facebook est basé sur la fourniture de services apparemment «gratuits» pour l'internaute, mais financés majoritairement sinon exclusivement par la publicité.

- **Données de santé: un impératif, la sécurité**

Les responsables de traitement dans le domaine de la santé doivent prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées surtout s'il s'agit d'informations couvertes par le secret médical. La CNIL préconise l'adoption de mesures de sécurité physique et logique qui doivent être adaptées en fonction de l'utilisation qui est faite de l'ordinateur, de sa configuration, de l'existence d'une connexion à Internet et recommande de chiffrer par cryptage les données figurant sur leurs supports numériques (et papier !).

Source: Commission nationale informatique et libertés – France www.cnil.fr