Les principales lois informatiques françaises

Patrick Kineider,
animateur du Groupe de Travail « Juridique et Internet du futur »

À l'époque des grands et moyens systèmes, puis à celle de la micro-informatique, le droit français, en la matière, concernait surtout la protection de la propriété intellectuelle (logiciels), du droit d'auteur et aussi des données personnelles quant à leur utilisation unique en vue de finalités déclarées
Le droit français sanctionnait les ingérences malveillantes dans les systèmes informatiques. La banalisation de l'Internet a fait naître, par ailleurs, des droits et devoirs en matière d'éthique des données, réseaux et systèmes de messageries interpersonnelles, mais la répartition des serveurs du web dans des pays ayant des législations diverses, induit des difficultés d'adaptation des textes existants.

Les grandes lois

Cette liste n'est pas exhaustive, cependant, elle identifie les trois principaux textes de lois de nature à protéger les données informatiques dans le contexte actuel et l'avenir à court terme.

Loi « Informatique et Libertés» (1978 et 2004)

En 1978 a été promulguée la première version de la Loi « Informatique et Libertés » protégeant les données personnelles. À la suite du développement d'Internet et après une révision de la loi en 2004 conférant des droits (consentement, retrait, modification) aux personnes figurant sur les fichiers, la fonction de « C.I.L » (correspondant informatique et libertés) s'est progressivement mise en place dans les organismes informatisées.
Ce correspondant a un rôle d'expert, de conseil, et également, de correspondant de la Commission.

Loi « Confiance dans l'Économie Numérique » (2004)

Elle est destinée à assurer la transparence des connexions, en facilitant les contrôles, et à préciser la responsabilité réelle des hébergeurs de sites, et des fournisseurs de service vis-à-vis des contenus, en particulier sur deux 2 points :

- les hébergeurs sont tenus de conserver, en vue d'éventuelles recherches, les données relatives aux équipements terminaux de communication utilisés, aux connexions ainsi que la date, l'horaire et la durée de chacune de ces connexions ;
- les hébergeurs ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des données d'un utilisateur de leurs services, s'ils n'avaient pas effectivement connaissance de leur caractère illicite ou de circonstances faisant apparaître ce caractère.

Lois « DADVSI » et « Hadopi2 » (2008-2010)

Ces textes prennent une importance croissante.
À l'origine, ils répondent à une directive européenne de 2001 sur les droits d'auteur. Ils visent, dans un premier temps, à identifier et réprimer les téléchargements illégaux d'œuvres (musicales, cinématographiques) sur Internet à l'aide de dispositifs dits « de riposte graduée » pouvant aller jusqu'à la coupure d'une connexion par le FAI, ordonnée par un juge.
Dans un deuxième temps, ils visent à développer des systèmes dits « plateformes légales » afin de pouvoir rémunérer, en défendant leurs droits, les artistes et auteurs, avec l'objectif à plus long terme d'élaborer un modèle économique viable pour les industries et commerces concernés.

L'opinion publique semble d'accord avec la nécessité de légiférer en la matière, mais, en même temps, est consciente des multiples difficultés d'application d'Hadopi :

- existence de contournements par des systèmes de streaming ;
- fragilité au plan sécurité des liaisons WIFI ;
- non-unicité de l'adresse IP ;
- difficulté de l'application en entreprise....

Par ailleurs, peu de personnes et d'institutions croient à un réel impact économique à terme, sur les artistes et auteurs. Après des débats de plus d'une année, en Mars 2010, seuls deux décrets « Hadopi2 » sur les 15 prévus avaient paru au J.O.

Pour toutes ces raisons, la loi, bien que suivant ses étapes ordinaires de promulgation, continue à diviser les usagers, les milieux politiques et associations diverses.

En février 2010 est venu en discussion au Parlement un autre ensemble de textes appelé « LOPPSI2 » (= loi d'orientation et de programmation pour la performance de la sécurité intérieure). LOPPSI2 recoupe le dispositif Hadopi2, en permettant entre autres aux autorités publiques chargées d'identifier et de réprimer la cybercriminalité, de filtrer les connexions aux ordinateurs personnels ayant des contenus illégaux (en matière de pédophilie, par exemple).

Historique de la « Loi Informatique et Libertés »

La « Loi n°78-17 du 6 Janvier 1978 relative à l'Informatique, aux fichiers et aux libertés » vise à protéger les données personnelles informatisées des fichiers exploités sur le territoire français, créés en vue de finalités précises (gestion, statistiques, information...), et ce, vis-à-vis d'une utilisation qui ne serait pas conforme à ces finalités.
La publication initiale de la Loi s'est accompagnée de la création de la « Commission Nationale de l'Informatique et des Libertés », organisme indépendant constitué d'un président, d'un vice-président, d'un trésorier, de deux représentants de l'État et de quinze commissaires.
La Loi impose des déclarations écrites des fichiers concernés à la Commission, qui engagent par sa signature l'autorité « Maitre d'Ouvrage » de ces fichiers (l'employeur pour des fichiers en entreprise).
Le suivi de ces déclarations aboutit à un avis, qui n'autorise l'exploitation des fichiers que s'il est favorable, auquel cas un il autorise le traitement par un décret en Conseil d'État.
Une cinquantaine de normes simplifiées ont été créées, couvrant certains types de fichiers personnels d'entreprise ; contrats ; fichiers fiscaux, RH, etc.
À la suite en particulier, de la directive européenne n°95/46 (24/10/1995), le texte initial a été complé té en 2004 par des dispositions pratiques organisant :

- l'**information** des individus titulaires de ces données et l'exercice par eux des droits de retrait, de modification, de suppression des données,
- l'**expertise** et le contrôle, éventuellement l'action en justice.
  Cette révision a également créé en entreprise, la fonction de Correspondant Informatique) et Libertés (C.I.L.) dans les organismes publics ou privés (voir plus loin).

En 2009, la CNIL a traité 72 000 déclarations, effectué 7 000 délibérations, 200 contrôles et 600 saisines de la justice. 300 « affaires » ont donné lieu à des débats en séance plénière.

Points forts et points faibles de la Loi

La CNIL aborde à ce jour, de façon quasi systématique, l'aspect légal et éthique de tous les dispositifs informatisés et à mémoire, pouvant porter atteinte aux libertés individuelles :

Ses principaux points forts

- Suivi de déclaration et avis sur les fichiers nominatifs, soit résidant sur des serveurs, soit utilisés sur des sites Internet.
- Surveillance des malveillances spams commerciaux ou non conformes à l'éthique (avec suivi de bases de données de spams recensés par les internautes), phishing, etc.
- Ressources humaines dans l'entreprise.
- Fichiers de contrôle d'accès à des locaux (privés, d'entreprises...), vidéosurveillance et vidéoprotection, dispositifs « RFID » (puces électroniques), carte d'identité électronique, dispositifs biométriques, vidéoscans.
- Dossiers personnels médicaux, fichiers de sécurité sociale (les données de santé d'une personne sont considérées comme propriété intégrale de cette personne).
- Fichiers de police et de justice (STIC, JUDEX, EDVIGE., projet LOOPSI), facilitant la coopération européenne en la matière, fichiers électoraux, éthique du « vote électronique »,
- Fichiers des sites de réseaux sociaux, etc.

À noter également, la séparation de plus en plus importante entre « sphère publique » et « sphère privée/d'entreprise », en ce qui concerne les données textuelles ou d''image sur les déplacements et les activités des personnes.
D'une manière générale, la protection des données sensibles et des libertés est garantie, dans le premier cas par les autorités publiques (Ministère de l'Intérieur), dans le deuxième cas, par la CNIL.

Ses principaux points faibles

La CNIL disposait en 2008, de 120 postes budgétaires, soit 50 % de plus qu'en 2004, alors que son activité a été multipliée par 7 dans le même temps. Son budget est d'environ 13 M€, mais c'est peu par rapport au budget des institutions équivalentes dans certains pays européens.

La CNIL possède un pouvoir d'alerte et de conseil et peut transmettre des dossiers, si elle les juge non conformes à la Loi, au Procureur de la République, mais ne peut elle-même aller en justice au titre de personne morale.

Son action de contrôle sur les réseaux sociaux actuels peut paraître insuffisante, compte tenu de leur montée en puissance et leur banalisation très rapides.

Elle ne peut légiférer de façon uniforme sur les « durées de conservation des données », qui dépendent de chaque traitement, en particulier en fonction des recherches à mener (situations bancaires, enquêtes pénales ou correctionnelles, badges d'accès à un service public, etc.).

Les correspondants Informatique et Libertés « CIL »

Les premiers CIL d'entreprise ont été nommés à l'automne de 2005.
Le CIL est un salarié de l'entreprise, le plus souvent rattaché à la Direction générale, et dont la finalité, outre celle de correspondant de la Commission, est l'appui à l'identification et à la déclaration des fichiers à données personnelles concernés et la protection des individus qui y figurent.

En 2009, 5 500 entreprises avaient désigné des CIL, pour certains mutualisés, dont plus de 90 % d'entreprises du secteur privé, dans tous les secteurs d'activité.

Il s'agit aussi bien de grandes entreprises telles que TOTAL, SAFRAN, MICHELIN, etc. que de petites ou moyennes entreprises.

À ce jour, le « CIL » est bien implanté dans le paysage économique français, car il apporte une expertise de conformité juridique et informatique de l'organisme dont il dépend, et donc une aide au management ainsi qu'au RSSI dans la gestion du patrimoine « dématérialisé ».

Perspectives

La CNIL participe à un groupe de travail européen, le G29, en liaison avec la mise en place d'une « Autorité Européenne de Protection des Données ».

En dépit d'une intégration lente, l'Europe semble être actuellement, le périmètre de défense des libertés et de coopération judiciaire, le plus pertinent.▲

patrick.kineider@numericable.fr