Droit et éthique de l'informatique

Résumé du cours de P. Glineur

Vincent Dieltiëns Aurélien Malisart Angelo Cuttitta

Juin 2009

Table des matières

Avant-propos

« Les faits bruts imposent l'intervention du législateur ».

Les faits dictent le droit. Face à l'apparition d'un phénomène technique nouveau, le législateur crée de nouvelles règles ou modifie des normes existantes :

- en rapport direct avec le phénomène et ses conséquences ;
- en rapport aux conditions nouvelles de vie.

Règles en rapport avec le phénomène et ses conséquences

L'adoption de ces règles est faite pour :

1. parer aux **dangers** potentiellement présentés par la nouvelle technique
   → *e.g.,* création des normes protectrices pour la vie privée face aux traitements informatiques des banques de données à caractère personnel ;
2. régler les **effets** considérés comme **néfastes** ;
3. **favoriser la généralisation** de la nouvelle technique (si elle est bénéfique)
   → *e.g.,* nouvelles normes relatives à la voirie favorisant les développements de l'automobile (malgré les dangers que cela apporte).

Il est également possible que des normes soient adaptées suite à l'apparition d'une nouvelle technique, *e.g.,* adaptation des normes suite au passage du papier à l'électronique.

L'évolution technologique impose une adaptation constante des textes normatifs et cette adaptation se fait plus ou moins rapidement selon l'Etat.

Règles en rapport avec les conditions de vie

Lorsqu'une technique entraîne de profonds changements sur la vie quotidienne, sur la manière d'être, de penser, de nouvelles normes s'imposent ou des normes anciennes doivent être adaptées pour répondre aux conditions de vie ainsi apportées (*e.g.* l'automobile a permis des communications rapides ce qui a facilité le passage des frontières, ce qui a un effet sur les règlements de l'émigration, des règles de procédures criminelles, *etc*).

L'informatique et la télématique auront un effet sur l'ensemble des normes aujourd'hui en vigueur, des effets profonds allant bien au delà d'une simple réglementation du phénomène informatique lui-même.

Le droit à l'informatique

Informatique : science qui étudie la collecte, le stockage, le traitement, la réunion, la distribution et la communication de données au moyen de systèmes automatisés.

Cette discipline **touche à tous les domaines du droit** (droits intellectuels, droit pénal, droit bancaire, *etc.*).

Le **but** de ce cours et de donner un aperçu de certains problèmes posés aux juristes par les technologies de l'informatique et de la télématique et leurs applications.

Conséquences de l'informatisation sur la démocratie

- Il faut garder la séparation des pouvoirs pour ne pas que cela dégénère ;
- les nouveaux moyens informatiques sont entre les mains des exécutifs ;
- il faudrait peut-être repenser la répartition et les relations entre les pouvoirs (« redéfinition de la place de l'Etat-nation ») ?

Au niveau de la relation entre l'Etat et ses administrés, on constate une rupture d'équilibre due à l'intervention de l'informatique au niveau du processus décisionnel de l'administration. Un « abandon de toute réflexion humaine dans les rapports avec les administrés ».

Deux articles de la loi française de 1978 « relative à l'informatique, aux fichiers et aux libertés » imposent l'exigence d'une réflexion humaine lorsqu'une décision est prise à la suite d'un traitement informatique et ont contraint le pouvoir à informer les administrés des critères retenus au niveau des procédures automatisées (*e.g.* empêcher l'expropriation de personnes suite à un tracé d'autoroute calculé par un ordinateur).

En France, une deuxième loi garantit le droit de toute personne à l'information en posant le principe de la liberté d'accès aux documents administratifs à caractère non nominatif et prévoit que « les documents administratifs sont de plein droit communicables aux personnes qui en font la demande (...) ».

En Belgique, il a fallu 20 ans pour que ces exigences minimales soient rencontrées.

Introduction générale

Existence du droit de l'informatique

En Belgique

La naissance du droit de l'informatique[1], dans notre pays, remonte à plus de 30 ans.

Premier colloque en 1971 : par l'institut de Belgique des sciences administratives. Il abordait des thèmes essentiels tels que les répercussions politiques, institutionnelles et administratives du développement de l'informatique, le droit à l'informations, *etc.*

Loi du 8 décembre 1992 : relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Autres réglementations spécifiques apparues entre-temps :

- registre national des personnes physiques ;
- autres banques de données publiques ou semi-publiques ;
- statistiques publiques ;
- comptabilité automatisée ;
- propriété intellectuelle (semi-conducteurs entre-autres).

Sur le plan international

Divers organismes internationaux se sont livrés à des travaux importants :

- le **Conseil de L'Europe** et l'**OCDE**[2] : le traitement des données nominatives et le problème de la fraude informatique ;
- **ONU-CEE**[3] : facilitation des procédures du commerce international ;
- l'**OMPI**[4] et l'**UNESCO**[5] : propriété intellectuelle.

⟶ Arrivée de revues spécialisées (*e.g.,* « Revue de droit de l'informatique et des télécoms »).

[1] Au sens d'une législation spécifique.
[2] Organisation de coopération et de développement économiques.
[3] commission des Nations Unies pour l'Europe
[4] Organisation mondiale de la propriété intellectuelle.
[5] Organisation des Nations Unies pour l'éducation, la science et la culture.

Tentative de définition du droit de l'informatique par son objet

Les technologies nouvelles de l'information ne connaissent pas de secteurs ou de matières sociales, économiques ou politiques, dans lesquels elles n'ont pas de répercussion et toutes les branches traditionnelles du droit sont aujourd'hui affectées par des phénomènes comme la dématérialisation des biens et la disparition du papier.

⇒ caractère hétérogène ou éclaté = « droit carrefour » ⇒ **nécessité d'une discipline juridique spécifique**.

Le droit de l'informatique a une certaine spécificité :
- il possède des **textes normatifs** qui lui sont **propres** (*e.g.,* la réglementation des banques de données à caractère personnel) ;
- il relève d'une **haute technicité**, l'informatique a permis d'affiner de façon remarquable les règles du droit commun (droit privé, droit pénal, *etc.*) qu'on entendait lui appliquer ;
- il procède à une **fusion**, parfois difficile, de **règles nouvelles et de règles de droit commun** (*e.g.,* registre national des personnes physiques et identifiant exclusif de chaque individu pour ses rapports avec l'autorité).

Caractères du droit de l'informatique

1. **Hétérogène :**
   - par les disciplines qu'il concerne ;
   - par ses sources nationales et internationales ;
   - par les autorités qui sont chargées de l'appliquer[6] ;
2. **Evolutif :** la technologie est en évolution permanente.

[6] Chaque Etat dispose d'une législation qui possède l'autorité spécifique d'appliquer ou de définir l'une ou l'autre norme propre à la matière informatique. En Belgique, ce rôle est rempli par la **Commission de la protection de la vie privée**

Chapitre 1

Informatique et droit au respect de la vie privée - protection de l'individu contre les traitements de données à caractère personnel

1.1 Notion et fondement du droit à la vie privée

Première moitié du XXème siècle : « droits de l'homme de la seconde génération » ou « droits économiques et sociaux » :

- droit à la sécurité d'existence ;
- droit à la sécurité sociale ;
- droit au travail ;
- droit à la santé ;
- droit à l'éducation et à la culture.

Deuxième moitié du XXème siècle : nouveaux droits de l'homme. Ce sont la conséquence des « méfaits des bienfaits du progrès » : *e.g.,* le droit au respect de la vie privée (article 8 de la convention européenne de sauvegarde des droits de l'homme de 1950).

Article 8 du droit à la vie privée : confère à chacun un droit au respect de sa « vie privée » et familiale, de son domicile et de sa correspondance.

Insertion dans la loi belge :

Article 22 : « chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi ». Cependant, ni la loi ni la Constitution ne définissent ce qu'est la « vie privée ».

Le droit au respect de la vie privée recouvre la nécessité d'une protection contre la collecte, l'encodage, le stockage, le traitement et la diffusion d'informations sur les individus lorsque ces opérations sont susceptibles d'entraîner une immixtion dans le domaine privé qui semble intolérable aux intéressés.

1.2 Dangers de l'informatique

Les dangers de l'informatique sur la vie privée des citoyens sont nombreux et profonds. *e.g.*, chaque belge figure dans plusieurs milliers de fichiers privés qui servent à fournir à ceux qui les tiennent, à leur associés ou à leurs clients qui en font la demande, une **image assez imprécise**, mais **fort incontrôlée** de notre personne. Les dangers les plus importants résident dans les **banques de données** à caractère personnel.

Banque de donnée : ensembles de fichiers automatisés donnant des informations les plus souvent factuelles mais également numériques, sur les individus. Ces informations sont en règle générale immédiatement utilisables lors de l'interrogation du fichier.

Dans les banques de données, les dangers pour la vie privée existent à toutes les phases du traitement et de l'utilisation et ce, depuis la recherche des données jusqu'à leur destruction éventuelle (détails dans les sous-sections suivantes).

1.2.1 Dangers de la collecte des informations

La généralisation de l'informatique a fait que chacun des aspects de notre vie figure dans l'un ou l'autre fichier (*e.g.*, les hôpitaux et les médecins ont informatisé les dossiers médicaux).

⇒ Aucun aspect de notre vie n'échappe donc aux fichiers informatisés.

Les dangers d'erreurs et d'abus sont nombreux. On peut collecter, volontairement ou involontairement, non des données vraies, mais des ragots, voir des mensonges délibérés.

1.2.2 Dangers de la transcription des données

Le danger réside dans une faute lors de la transcription des données (*e.g.*, faute de frappe ou erreur humaine).

1.2.3 Danger de l'application (ordinateur)

L'ordinateur peut faire l'objet d'erreurs humaines, être l'objet de fraudes, d'infractions mais peut « se tromper tout seul » suite à des événements extérieurs tels que la chaleur ou l'humidité.

Le programmeur peut volontairement ou involontairement faire des erreurs dans la réalisation du programme[1].

⇒ On ne peut pas faire confiance à l'ordinateur, si perfectionné soit-il.

1.2.4 Dangers de l'interprétation du résultat et des données

Ces dangers sont dus à l'existence même des banques de données. L'informatique donne à son utilisateur la possibilité d'obtenir à propos d'un individu une série d'**informations innocentes en principe**, ce dernier peut en retirer une série de **conclusions non innocentes**.

[1] Par exemple, en 1979, un ordinateur de la Défense des Etats-Unis à fait croire faussement qu'un missile soviétique se dirigeait vers les USA.

1.2.5 Dangers de la diffusion de l'information

Les dangers sont présents dans la diffusion soit **volontaire**, soit **involontaire** de l'information. Les données peuvent être subtilisées à l'insu de leur possesseur (*e.g.*, via un cheval de Troie).

1.2.6 Dangers dans la capacité d'enregistrement des ordinateurs

Les techniques actuelles permettent de supprimer la nécessité de toute destruction de l'information ou des données anciennes grâce (à cause ?) de la possibilité illimitée d'enregistrement.

« Pourquoi donc supprimer des informations, dès lors qu'elles pourraient avoir, dans un futur plus ou moins éloigné, une quelconque utilité » ?

Cette particularité va à l'encontre d'une idée généralement reçue dans les états démocratiques : toute information concernant des infractions, des délits ou plus généralement des méfaits doit être détruite après l'écoulement d'un certain laps de temps (on ne doit pas subir toute sa vie les conséquences d'erreurs pardonnées ou réparées, voir d'erreurs commises par des proches).

⇒ La possibilité de stockage illimité que donne l'ordinateur ne peut pas faire oublier la valeur morale sous-tendue.

1.3 Relativité du concept du droit au respect de la vie privée et relativité des dangers de l'informatique

Le droit au respect de la vie privée **n'est pas un droit absolu**. En effet, la loi autorise une série d'ingérences du pouvoir dans l'exercice du droit au respect de la vie privée. Ces ingérences ne sont pas le fait de l'informatique : elles sont voulues par le législateur, elles s'expriment sous son contrôle et il peut y mettre un terme quand il l'entend. En utilisant l'informatique, l'autorité ne fait que mettre en oeuvre au moyen d'une technologie nouvelle, les ingérences voulues par le législateur.

Les exemples d'ingérence dans la vie privée voulue par le législateur abondent. En effet, il existe de nombreux exemples dans lesquels le législateur impose la collecte de renseignements, touchant à la vie privée, et la transmission de ces derniers[2].

Remarque : ce qui différencie la démocratie des dictatures, c'est que les ingérences de l'autorité sont toujours prévues par la loi.

Avec les technologies, ce qui est différent, c'est le volume et la rapidité avec laquelle les ordinateurs peuvent enregistrer, traiter et diffuser les informations. Grâces aux ordinateurs, on peut relier entre eux divers registres dans des « banques de données » susceptibles de fournir immédiatement, de manière fort complète, et sans limitation de distance, un très grand nombre d'informations sur les personnes.

⇒ Le problème posé par les banques de données informatiques serait donc celui d'un seuil qualitatif et non d'un seuil quantitatif ?

La seconde question, à savoir le respect par l'Administration des normes existantes en matière de protection de vie privée, se résout aisément, abstraction faite de l'outil informatique utilisé. L'**information administrative doit toujours être compatible avec les exigences suivantes** :

- être celle que l'Administration à le droit de recueillir, de traiter et de conserver ;
- avoir été obtenue par des moyens licites ;

[2]Par exemple, bien entendu, les législations fiscales et sociales belges.

– être utilisée conformément au but déterminé par le législateur, et être communiquée uniquement aux personnes autorisée par le législateur.

Grâce aux ordinateurs, on peut interconnecter ou jumeler entre eux différents registres ou fichiers et les réunir dans des banques de données qui peuvent, en un espace de temps limité, donner d'une manière quasi intégrale et pratiquement sans limite, une image précise du citoyen. **La véritable grande crainte réside en ces interconnexions**. Il est permis de se demander si le législateur aurait autorisé, il y a trente ans, les même possibilités d'ingérence dans la vie privée, s'il avait connu les moyens techniques actuels.

1.4 Problématique d'une réglementation de l'informatique – aspects internationaux et nationaux

La réglementation des rapports de l'informatique et de la vie privée doit prioritairement être abordée sur le plan international car :

– les données traversent sans difficultés les frontières des Etats ;
– les règles prises par un Etat en matière d'organisation d'une protection des données personnelles pourraient être facilement contournées par le fait d'un traitement effectué, à l'étranger, sous l'empire d'une législation plus libérale.

⇒ Un Etat isolé n'est donc par en mesure de répondre adéquatement au problème de flux transfrontaliers des données, flux qui sont de la nature des systèmes informatiques contemporains et futurs.

Les **solutions internationales actuelles** prônent une libre circulation des données à caractère personnel entre les divers Etats contractants, moyennant l'élaboration d'un noyau inconditionnel uniforme de droits garantis dans chaque Etat.(*i.e.*, une harmonisation des législations internes tendant à l'obtention d'un minimum de la protection de la vie privée dans chaque Etat).

En **1981**, une convention (numéro 108) fût soumise à la signature des Etats membres « pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La Belgique, signataire de cette convention, n'a adopté la loi portant son approbation que le 17 juin 1991.

En **1990**, la Commission a approuvé une communication destinée au conseil, assortie de six propositions d'actions concrètes visant à assurer, dans la communauté, une protection des données et une sécurité accrue et harmonisée des systèmes d'information.

En **1995**, un des textes les plus importants adoptés suite à ces propositions est une directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Cette directive a pour but d'éviter que la libre circulation de l'information entre les Etats membres de l'Union soit limitée de façon excessive au nom des droits et des libertés des personnes.

1.4.1 Convention numéro 108 de 1981

Cette convention du Conseil de l'Europe semble être devenue **le texte de référence le plus important**, en droit international, notamment si elle est destinée à servir de support aux relations entre la Communauté et les Etats membres avec les pays tiers et, surtout, les pays de l'Europe de l'Est.

Elle prévoit trois types de disposition :

– **Elle énonce les principes de base.**
Elle prévoit, pour les Etats, l'obligation d'introduire dans leur législation interne les dispositions normatives pour que soient observés les principes essentiels tels que le principe de finalité légitime du traitement, le droit

d'accès et de correction, l'obligation de la sécurité, ...
- **Elle prévoit l'interdiction pour un Etat** de soumettre les flux transfrontières à destination d'un autre Etat contractant, à des autorisations spéciales.
- **Elle prévoit la désignation dans chaque Etat d'une autorité de liaison** chargée d'établir les règles de procédure pour les plaintes et les requêtes qui émanent de personnes résidant à l'étranger.

Cette convention n'a réglé que fort timidement cet aspect des flux transfrontières en admettant la possibilité de dérogation au principe de la libre circulation par l'Etat d'origine : « lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire d'un territoire d'une autre partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation ». La lacune de ce texte est évidente ; comment l'Etat d'origine pourrait-il connaître le pays de la destination finale des données ?

Une internationalisation plus grande des normes s'impose donc.

1.5 Aperçu du droit positif belge en matière de banques de données et de protection des données à caractère personnel

1.5.1 Existence des banques de donnée administratives

Il existe une multitude de fichiers informatiques du secteur public qui sont créés :

- par le législateur ;
- par le pouvoir exécutif ;
- par les services administratifs (dans le cadre de leur mission légale et en dehors de tout contexte normatif).

Parmi les grands fichiers publics on note :

- Le Registre national des personnes physiques (RNPP) ;
- le Registre national des personnes morales (RNPM) devenue la Banque carrefour des entreprises (BCE) ;
- la Centrale des risques devenue la Centrale des crédits aux entreprises ;
- les fichiers de l'Institut national de statistique (INS) ;
- abonnés au téléphone, fichiers de police, véhicules immatriculés, fichiers spécifiques à l'ONSS / ONEM / INAMI / INASTI, ...

En Belgique, il faudra attendre 1992 pour que soit adopté un texte légal réglementant, de manière globale, la protection des individus en matière de traitement automatisé de données à caractère personnel (nonobstant l'existence des « grands fichiers administratifs »).

1.5.2 Registre national des personnes physiques

1.5.2.1 But

Il s'agit d'un service rendu aux administrations communales pour la gestion de leurs fichiers de population. Il « facilite la tenue à jour des fichiers de l'ensemble des administrations publiques ».

1.5.2.2 Historique

Il a été créé en 1968 sans aucune consécration législative par le Gouvernement de l'époque. L'absence de toute réglementation organique de ce registre était fort inquiétante et en 1983 la loi « Nothomb » apporte quelques dispositions timides de protection.

1.5.2.3 Personnes concernées

Registre national : système « de traitement d'informations qui assure, conformément aux dispositions de la loi de 1983, l'enregistrement, la mémorisation et la communication d'informations relatives à l'identification des personnes physiques ».

Les personnes physiques qui y sont fichées sont :

- les personnes inscrites au registre de la population ;
- les personnes inscrites au registre des étrangers ;
- les personnes inscrites au registre tenu dans les missions diplomatiques et postes consulaires à l'étranger ;
- les demandeurs d'asile, les SDF et les gens du voyage.

1.5.2.4 Données enregistrées

Le RNPP tire ses informations des registres de population tenus par les communes, registres qui contiennent de nombreuses données relatives à la vie privée. Le registre n'en retient prioritairement que dix et leurs mises à jour et leur date de prise d'effet :

1. les noms et prénoms ;
2. le lieu la date de naissance ;
3. le sexe ;
4. la nationalité ;
5. la résidence principale ;
6. le lieu et la date de décès ;
7. la profession ;
8. l'état civil ;
9. la cohabitation légale ;
10. la composition du ménage.

A toutes ces données, s'ajoute un numéro d'identification unique (**numéro de registre national**[3]). Des informations autres que les onze informations de base peuvent être enregistrées à la demande d'une commune (et ne seront accessibles qu'à celle-ci).

But avoué : « permettre une communication plus sûre et plus aisée des informations entre les différents organismes habilités à l'utiliser et à échanger des informations à caractère personnel ». En d'autre termes, ce numéro est notamment destiné à faciliter l'interconnexion des banques de données habilitées à en faire usage à des fins externes.

On a pu craindre, dès l'adoption de la loi Nothomb, que ce numéro ne remplace, en fait, le nom des individu dans leurs rapports avec l'autorité.

Le **danger** essentiel pour la vie privée ne réside pas dans l'utilisation obligatoire d'un numéro ; il réside dans l'existence même d'un numéro identifiant unique, car pareil élément constitue la clé suffisante pour l'interconnexion généralisée des banques de données à caractère personnel ... sans négliger l'aspect psychologique négatif que pareil numéro comporte !

1.5.2.5 Fonctionnement et communication des données

La loi Nothomb a organisé trois flux de données principaux :

[3]Celui-ci est basé sur la date de naissance, le sexe et le numéro d'ordre de la personne.

1. **Flux vertical de données**
   ⇒ du RN vers les communes et inversement
   Depuis la loi :
   - les communes ont l'obligation de communiquer au RN les informations de base (dans le but d'être **exhaustif**).
   - La **responsabilité de l'exactitude des données** initiales pèse sur les communes (et missions diplomatiques et consulaires) qui les ont transmises.
   - Elles ont le droit d'accéder aux informations de base contenues dans le registre national même si ces informations ont été enregistrées à l'initiative d'une autre commune (ou poste diplomatique ou consulaire).
   - Les « administrations communales » peuvent utiliser le numéro d'identification unique.
2. **Flux horizontal**
   La loi a posé le principe de la **soumission de l'accès au registre** à une autorisation d'abord par voie d'arrêté royal, maintenant par le Comité de surveillance sectoriel[4] et soumise à la tutelle de la Commission. Cette autorisation ne peut être consentie :
   - qu'aux **autorités publiques** ou,
   - aux **organismes d'intérêts public** ou,
   - aux **notaires**, aux **huissiers** de justice et aux Ordres des **avocats**, ou
   - aux organismes **sous-traitants**.

   De nombreux organismes ont, depuis, reçu l'autorisation d'accès :
   - le Ministère de la justice (autorités publiques) ;
   - la gendarmerie (autorités publiques) ;
   - la Caisse d'Assurance Sociale des Travailleurs Indépendants ;
   - la BCE ;
   - ...

   Notons que, conformément au droit commun administratif, l'autorisation ne peut pas porter indistinctement sur l'ensemble des informations mais uniquement sur celles dont la connaissance est indispensable pour l'accomplissement de sa mission par l'autorité ou l'organisme en cause.
3. **« Switching » ou transit obligatoire**
   Il s'agit d'un flux d'informations des communes vers les autorités publiques et les organismes d'intérêt public transitant par le RN, ce dernier ne jouant d'un rôle de « relais ». Les informations ainsi transmises ne peuvent être conservées au registre national.
   Il existe plusieurs procédures de switching actuellement réglementées. La première était dans le cadre de la loi sur le prélèvement et la transmission d'organes (cfr. page 38 des notes).

1.5.2.6 Flux d'informations résultant de l'usage du numéro d'identification

L'autorisation d'utiliser le numéro d'identification confère à l'autorité ou l'organisme habilité à l'utiliser :

- soit la possibilité d'un usage à des **fins internes** ; (*e.g.*, gestion de fichiers propres, établissement de statistiques) ;
- soit la possibilité d'un usage à des **fins externes** (*i.e.*, en tant qu'identifiant lors de rapports avec d'autres autorités ou organismes).

L'**usage généralisé d'un numéro d'identification** en tant qu'identifiant « unique » dans le cadre de la gestion administrative des grands secteurs publiques (rapidité des recherches administratives pour l'identification des personnes et à la localisation des informations qui les concerne) permet une réforme fondamentale des méthodes d'organisation et la **réalisation d'économies dans les frais de fonctionnement** : temps de recherche réduits, non redondance des informations (*e.g.* il y avait avant 1.300.000 changements d'adresse par an en Belgique, à enregistrer dans des centaines de fichiers).

[4] sorte de mini-commission pour la protection de la vie privée

Le **danger** de l'usage généralisé de ce numéro ne doit toutefois pas être caché pour ces raisons économiques !

1.5.2.7 Délais de conservation des données

Les données enregistrées *i.e.*, toutes les informations passant par le registre, à l'exception de celles résultant du switching qui ne peuvent être maintenues, sont conservées pendant **30 ans** à compter du jour du décès de la personne concernée.

1.5.3 Banque-Carrefour de la sécurité sociale

En Belgique, le système de sécurité sociale est extrêmement morcelé : différentes branches gèrent indépendamment les allocations familiales, les assurances, la santé, les accidents du travail, le chômage, les pensions, ...

Il en résulte souvent des collectes répétées des mêmes informations.

1.5.3.1 Statut et missions

Banque-Carrefour de la sécurité sociale : est un « organisme public doté de la personnalité civile ».

La Banque-Carrefour de la sécurité sociale n'a pas pour mission de centraliser la collecte des données sociales ou l'enregistrement ou le traitement de celles-ci (c'est le rôle des organismes de sécurité sociale). Elle fait uniquement office d'**organisme carrefour** par l'intermédiaire duquel doit normalement se dérouler tout **échange de données entre les organismes de sécurité sociale ou entre ces organismes et des tiers**.

Cela comprend :
- organiser, coordonner et contrôler le fonctionnement du réseau ;
- transformer les données disponibles en informations statistiques, sociologiques, économiques et financières.

La Banque-Carrefour de la sécurité sociale **coordonne** et **contrôle le fonctionnement du réseau**, *i.e.*, l'ensemble constitué par les banques de données sociales, la Banque-Carrefour de sécurité sociale et le Registre National.

Ceci permet de limiter l'enregistrement multiple et superflu de données en divers endroits et d'optimiser ainsi les garanties concernant la validité et le caractère confidentiel de l'information.

Lorsque les organismes de sécurité sociale collectent des informations qui ne sont pas encore disponibles dans le réseau, elles ont l'obligation de communiquer immédiatement à la Banque-Carrefour de la sécurité sociale la nature des informations complémentaires dont ils disposent désormais, de telle façon que chaque organisme, dans le réseau, puisse y faire appel si nécessaire.

La Banque-Carrefour de la sécurité sociale peut **enregistrer et conserver** un certain nombre de données d'identification à caractère personnel. Il s'agit de **données dont plusieurs organismes de sécurité sociale ont régulièrement besoin** pour l'exécution de leurs missions et qui ne peuvent pas être puisées dans un RN accessible à ces organismes.

1.5.3.2 Liens entre la Banque-Carrefour de la sécurité sociale et le Registre National – sort du numéro identifiant

Les données de base contenues dans le RN, ainsi que le numéro identifiant, sont accessibles à la Banque-Carrefour de la sécurité sociale. Celle-ci peut également utiliser ce numéro identifiant.

Pour les personnes non inscrites au Registre national, un numéro identifiant spécifique au réseau de la Banque-Carrefour de la sécurité sociale a été prévu.

1.5.3.3 Etendue du réseau - schéma et fonctionnement

L'étendue du réseau informatique couvert par la Banque-Carrefour de la sécurité sociale est très large :

- ensemble des régimes d'assurances sociales[5] ou d'aide sociale ;
- ensemble des institutions publiques de sécurité sociale et l'ensemble des institutions coopérantes ;
- la Banque-Carrefour de la sécurité sociale ;
- le Registre National ;
- les fonds de sécurité d'existence.

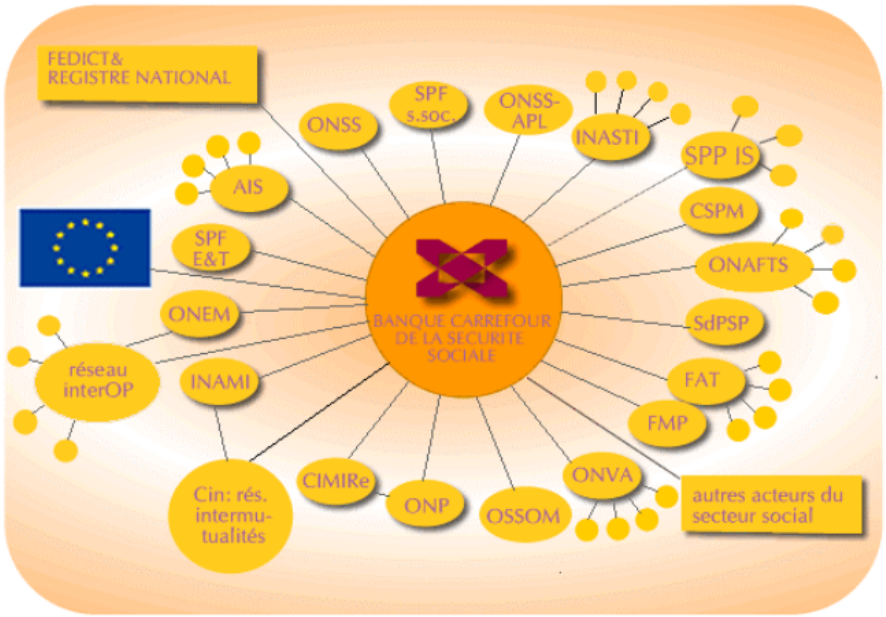

FIG. 1.1 – Banque-Carrefour de la sécurité sociale

Le schéma de la structure du réseau distingue deux niveaux (Fig. 1.1) :

1. le **réseau primaire** : organismes coordinateurs de la sécurité sociale[6] ;
2. le **réseau secondaire** : les institutions coopérantes de sécurité sociale[7].

Les institutions de sécurité sociale sont **tenues de communiquer à la Banque-Carrefour de sécurité sociale toutes les données dont celle-ci a besoin** pour sa mission. C'est une obligation pour ces organismes d'enregistrer et de tenir à jour les données dont la conservation leur a été confiée.

La Banque-Carrefour de sécurité sociale est reliée à des banques de données externes, et principalement au Registre National. Aucune institution de sécurité sociale n'a plus accès au direct au Registre National, mais les

[5] travailleurs salariés, travailleurs indépendants, secteur public

[6] Collège inter-mutualiste national, caisse de secours et de prévoyance, fonds des accidents du travail, fonds des maladies professionnelles, INAMI, INASTI, ONSS, SPF Emploi, etc.

[7] Organismes assureurs, caisses d'allocations familiales, compagnies d'assurances, organismes d'allocations de chômage, réseau des CPAS, etc.

données de celui-ci sont répercutées à l'intervention de la Banque-Carrefour de sécurité sociale.

Toute communication de données par une institution de sécurité sociale doit transiter par la Banque-Carrefour de sécurité sociale. Exceptions lorsque la communication a pour destinataires :
- les personnes auxquelles les données se rapportent (ou leurs mandataires légaux) ;
- les personnes ayant besoin des données pour remplir leurs obligations légales en matière de sécurité sociale ;
- les organismes de droit étranger pour l'application de conventions internationales ;
- les institutions de sécurité sociale (arrêtés royaux).

1.5.3.4 Mesures de protection de la vie privée

La loi prévoit diverses mesures de protection pour la vie privée qui ont pour objet commun les « données sociales à caractère personnel ». Les **données à caractères personnel** sont « toutes les données nécessaires à l'application de la sécurité sociale, concernant une personne identifiée ou identifiable ». Il faut entendre par cette expression **toutes** les données à caractère personnel, en possession des institutions.

Diverses mesures de protection ont également pour objet commun les « banques de données sociales ».

Banques de données sociale : « banque de données où des données sociales sont conservées par les institutions de sécurité sociale ou pour leur compte ».

1. **Mesures d'autocontrôle**

   Principe de finalité et de spécialité : les personnes qui demandent des informations à caractère personnel dans l'application de la sécurité sociale ne peuvent disposer que des informations :
   - dont elles ont besoin ;
   - que le temps nécessaire pour l'application ;
   - en gardant le caractère confidentiel de ces informations.

   Devoir de discrétion : toute personne qui, en raison de ses fonctions, collecte, traite ou communique des données sociales à caractère personnel, ou a connaissance de telles données, doit en respecter le caractère confidentiel, sauf si la loi ne l'y oblige.

   Les obligations de finalité ou de confidentialité s'étendent à toute personne qui détient des données relevant de la sécurité sociale (*e.g.*, le personnel des secrétariats sociaux, ou les membres des services du personnel des entreprises et des administrations publiques).
   Les données médicales sont sujettes à une protection renforcée. Elle doivent être traitées, échangées et conservées sous la surveillance et la responsabilité d'un médecin.

   Donnée médicale : toute donnée « dont on peut déduire une information sur l'état antérieur, actuel ou futur de la santé physique d'une personne (excepté des données purement administratives ou comptables relatives aux traitements et aux soins médicaux).
2. **Contrôle individuel**
3. **Contrôle institutionnel**
   (a) Comité de surveillance : C'est un comité d'experts des différentes branches concernées (droit, informatique, médecine). C'est un organe de contrôle[8] spécifique à la sécurité sociale coexistant avec la Commission pour la protection de la vie privée et collaborant avec cette dernière.
   (b) Inspecteurs sociaux : Ce sont des fonctionnaires qui sont chargés de la « surveillance pénale » du respect de la loi relative à Banque-Carrefour de la sécurité sociale. Ils ont des pouvoirs d'investigation très étendus, avec la seule restriction de la nécessité d'une autorisation du pouvoir judiciaire si la visite doit se dérouler dans des locaux habités.

[8] indépendant de l'ordre judiciaire

(c) Commission de la protection de la vie privée : La Commission veille à ce que les données à caractère personnel ne soient pas utilisées d'une manière contraire à la loi. Elle a aussi pour mission de répondre aux demandes d'informations et de traiter les plaintes qui lui sont adressées.

(d) Dispositions pénales : Les sanctions pénales pour ceux qui enfreignent le principe de finalité, le devoir de confidentialité ou qui s'abstiennent de prendre des mesures appropriées pour leur respect.

Chapitre 2

Evolution du droit sous l'influence de l'informatique

L'informatique apparaissant comme un phénomène de masse au fur et à mesure que le temps s'écoulait, son influence sur le droit devint de plus en plus profonde.

Quel que soit le domaine dans lequel on souhaite appliquer le droit, l'informatique en fait partie intégrante. L'informatique étant un domaine vaste, il est complexe de définir la multiplicité des obligations des diverses parties impliquées. Par ailleurs, la quantité importante des intervenants du domaine rend difficile la définition des tâches et des responsabilités de chacun.

Quoi qu'il en soit, la question ultime du domaine est, et reste, la suivante : « Comment réprimer justement ceux-qui tentent d'utiliser l'informatique à des fins illicites ? ». La question cible essentiellement l'appropriation illégitime des valeurs informatiques d'autrui.

La suite du cours montre que rares sont les cas où un nouveau droit a été élaboré du fait que le législateur y soit amené par un besoin pressant. Ce qui pourrait s'expliquer par la plastique des règles/notions/concepts de notre droit. Celui-ci est, en effet, à contenu vague et évolutif (cf. « bonnes moeurs », « faute » et « ordre public »).

Le contenu des concepts a évolué dans la loi sans que les concepts eux-même n'aient subi une quelconque modification. Le juge applique, ainsi, toujours la même règle à laquelle l'évolution des esprits a donné un contenu différent !

Notons que c'est au législateur qu'il appartient de modifier la loi et non au juge. Ce dernier se doit, en effet, de respecter et d'appliquer la loi en vigueur et ce, quelles que soient les évolutions qui surviendraient (base du système constitutionnel belge).

Chapitre 3

Informatique et propriété industrielle

3.1 Généralités

Propriété industrielle :

- droits exclusifs à l'usage de signes distinctifs qui servent à identifier une entreprise, un établissement ou un produit (**marques**) ;
- droits à un certain monopole d'exploitation d'une **invention**[1] ;
- droit exclusif de reproduire les dessins ou les formes qui différencient un objet d'autres objets similaires (dessins et **modèles**) ;
- droit exclusif de tirer profit l'**œuvre** protégée par le droit de l'auteur.

3.2 Brevets d'invention

Les inventions exploitées dans le commerce et l'industrie peuvent être protégées par des brevets. Les droits associés à un brevet sont limités dans le temps et supposent la délivrance préalable d'un brevet administratif dit « d'invention ». La durée est de 5 ans (sans contrôle d'antériorité) ou 20 ans (avec contrôle d'antériorité).

La Convention de Munich harmonise la délivrance des brevets européens (adoptée 1984 en Belgique).

Un élément est brevetable s'il est « nouveau » par rapport à l'existant (non compris dans l'état de la technique) et s'il ne découle pas directement de l'état de la technique. Cet élément doit avoir « une action sur la matière ».

Les programmes et logiciels d'ordinateur sont exclus de la brevetabilité :

- une invention brevetable suppose qu'elle soit susceptible d'application industrielle immédiate ; un logiciel rentre dans la catégorie des « méthodes mathématiques », des « idées pures » et des « solutions abstraites » ;
- la technique de délivrance des brevets est mal adaptées aux logiciels : description, rapports de recherche, revendications).

Une invention comportant comme élément constitutif un système de traitement de l'information peut être brevetée pour autant que cette invention considérée « in globo » satisfasse aux conditions de brevetabilité. « Les machines, les procédés de fabrication ou de commande, commandés par un programme d'ordinateur, devraient normalement être considérés comme des objets susceptibles d'être brevetés ».

[1] par un **brevet**

3.3 Droits d'auteur

Il s'agit de l'ensemble des droits accordés au créateur d'une oeuvre de l'esprit. Ils lui permettent d'être le seul à pouvoir tirer profit de son oeuvre (monopole économique) et à en assurer le respect.

Différences avec les autres droits de la propriété industrielle :

- la protection du droit d'auteur existe dès que l'oeuvre est mise en forme ou ébauchée ;
- la durée de protection est beaucoup plus importante (70 ans après la mort) ;
- les droits d'auteur ne disparaissent pas lorsqu'un monopole d'exploitation a été conféré ;
- le droit d'auteur ne suppose pas la « nouveauté » mais simplement « l'originalité ».

Conditions pour qu'une oeuvre bénéficie de protection par les droits d'auteur :

1. l'oeuvre doit être exprimée dans une certaine forme (orale, peinte, écrite, codée, ...)[2] ;
2. l'oeuvre doit être originale (marquée de la personnalité de son auteur).

Seul le créateur ou le concessionnaire des droits du créateur a le droit de communiquer une oeuvre au public (**doit de représentation**). Le **doit de reproduction** stipule que toute reproduction/traduction nécessite obligatoirement le consentement de l'auteur (sauf si à caractère privé). La reproduction est autorisée s'il s'agit de citations dans un but polémique, critique ou d'enseignement.

3.3.1 Quid de la protection des logiciels par le droit d'auteur ?

Le logiciel peut apparaître comme une oeuvre de l'esprit. L'existence de supports matériels permet de songer à faire protéger le logiciel par la loi du droit d'auteur, pour autant qu'il soit original et formulé de manière suffisamment précise.

Les tribunaux belges ont admis le principe de la protection des logiciels par le droit d'auteur comme une chose évidente, allant de soi et ne nécessitant pas de longs débats. Cependant, il faut constater que les quelques rares décisions publiées n'ont pas abordé les questions essentielles, telles que le degré d'originalité exigé d'un logiciel ni l'objet et l'étendue exacte de la protection conférée. Les caractéristiques de l'originalité seraient présentes à partir du moment où la composition du programme exige plus qu'une « simple compilation de données connues ».

« Un programme d'ordinateur est protégé s'il est original, en ce sens, qu'il est une création intellectuelle propre à son auteur. Aucun autre critère ne s'applique s'il peut bénéficier d'une protection par le droit d'auteur ».

La protection prévue par la loi belge vise les programmes, sous quelque forme et quelque support que ce soient, en compris ceux qui sont incorporés au matériel et toutes les étapes de leur conception et de leur réalisation. A contrario, les idées et principes à la base de tout élément d'un programme ne sont pas protégés par le droit d'auteur (y compris ses interfaces).

Dans le cas d'un programme créé par un employé dans le cadre de l'exercice des ses fonctions, l'employeur est présumé cessionnaire des droits patrimoniaux relatifs à celui-ci.

Dans le cas d'un programme créé dans le cadre d'un contrat de commande, les droits peuvent être cédés au commanditaire à condition que la cession sont expressément prévue dans le contrat.

Contrairement aux autres auteurs, le programmeur ne dispose pas du droit de divulgation[3]. Egalement, il ne sera en mesure de faire respecter le droit à l'intégrité[4] de son oeuvre que s'il établit un préjudice à son honneur ou à sa réputation. Les droits moraux du programmeur sont cessibles et il peut valablement y renoncer.

[2] Le droit d'auteur ne protège que la forme d'expression, pas le contenu

[3] « L'auteur a seul le droit de divulguer son oeuvre ».

[4] « Le droit à l'intégrité de l'oeuvre permet d'empêcher toute modification ou déformation de celle-ci et toute atteinte à son endroit ».

Les droits patrimoniaux du programmeur (monopole d'exploitation) comprennent :

- la reproduction en tout ou partie, par quelque moyen et sous quelque forme que ce soient ;
- la traduction, l'adaptation, l'arrangement et toute autre transformation qui ne préjudice pas les droits de la personne qui transforme le programme ;
- toute forme de diffusion au public (vente, location, prêt, ...).

3.3.1.0.1 La limitation du « first sale ». Dès que le titulaire du droit d'auteur a vendu une copie de son programme à un tiers, son droit de distribution s'épuise (il ne peut plus se réserver le droit d'autoriser ou d'interdire son exploitation commerciale). Il ne conserve que le droit de contrôler les locations/copies du programme.

3.3.1.0.2 Exceptions des droits patrimoniaux :

1. la reproduction, traduction, adaptation, arrangement, transformation ne sont pas soumis à l'autorisation préalable du titulaire du droit lorsque ces actes sont nécessaires pour permettre d'utiliser le programme d'une manière conforme à sa destination ;
2. la reproduction sous forme d'une copie de sauvegarde ne peut être interdite à une personne ayant reçu le droit d'utiliser le programme ;
3. l'autorisation du titulaire du droit n'est pas exigée pour une personne ayant reçu le droit d'utilisation s'il désire observer, étudier ou tester son fonctionnement afin de déterminer les idées et les principes qui sont à la base de l'un de ses éléments ;
4. l'autorisation n'est pas requise pour une reproduction/traduction d'un programme dans un but d'interopérabilité (accompli par une personne jouissant du droit d'utilisation, informations nécessaires à l'interopérabilité disponibles, traduction limitée aux parties du programme d'origine nécessaires à l'interopérabilité, ne peut porter préjudice au titulaire du droit).

La loi belge ne résout pas la question d'une éventuelle exception pour courtes citations ou copie privée d'un programme.

La durée est celle du droit d'auteur général, en l'occurrence, 70 ans après la mort de l'auteur. Les sanctions applicables sont celles prévues par la loi générale.

3.4 Oeuvres fabriquées ou produites par ordinateur

Les oeuvres fabriquées à l'aide de l'informatique sont aussi affectées par le droit d'auteur : musique, images, dessins, représentations visuelles, vidéos, images de jeux vidéos.

Si l'oeuvre créée ne contient rien d'autre que ce qui a été programmé par le concepteur du logiciel, le droit d'auteur repose sur ce concepteur. A contrario, si l'oeuvre créée peut être considérée comme indépendante du logiciel, la paternité de l'oeuvre repose dans le chef de l'utilisateur (le logiciel est utilisé comme un simple outil au service de l'originalité).

Dans certains cas, la création comporte des éléments empruntés au système d'aide à la création (e.g., plans d'architecture). On parle alors de copropriété intellectuelle.

3.5 Banques de données

3.5.1 Protection des données contenues dans la banque

Le stockage de données[5] dans la banque est assimilable à une reproduction de celles-ci. Dès lors, l'exploitant de la banque données doit avoir l'autorisation de l'auteur des données pour les stocker (et les communiquer aux consommateurs de la banque). L'exploitant doit également obtenir l'approbation préalable de l'auteur pour effectuer des compilations, des résumés (adaptations) ou des transformations en langage informatique.

La simple indexation d'une article (mots clés ou autre) n'est pas considérée comme portant atteinte aux droits de l'auteur (France), sous réserve que soient mentionnés le nom de l'auteur et la source, et que les informations rassemblées ne dispensent pas le lecteur de recourir à la lecture de l'oeuvre elle-même.

3.5.2 Protection de la banque de données en elle-même

L'auteur d'une banque de données jouit d'un droit d'auteur exclusif sur celle-ci (« les bases de données [...] constituent une création intellectuelle propre à l'auteur »).

La loi belge a entendu protéger d'une manière spécifique les banques de données qui ont nécessité un investissement qualitativement ou quantitativement substantiel pour l'obtention, la vérification ou la présentation de leur contenu (directive européenne de 1996).

Le droit d'auteur du producteur d'une base données est étendu par des protections au sujet :

- de l'extraction et/ou de réutilisation de la totalité ou d'une partie substantielle de ses données ;
- des l'extractions et/ou réutilisations répétées/systématiques/contraires à une utilisation normale de parties non substantielles de ses données (opérations susceptibles de causer un préjudice aux intérêts légitimes du producteur).

3.6 Protection de la propriété intellectuelle par les contrats

Le droit des brevets et le droit d'auteur n'apportent que peu de protection aux firmes informatiques. Dans la pratique, les firmes se prémunissent par des dispositif techniques et des clauses contractuelles.

La plupart des conventions en matière de logiciels sont intitulées « concessions de droit d'usage » ou « licences d'utilisation », plutôt que « ventes ». Le but étant d'éviter de transférer un droit privatif à l'utilisateur sur le logiciel « vendu ».

3.7 Protection des topographies des produits semi-conducteurs

La mise au point de la topographie des puces nécessite un investissement humain et financier considérable. La copie de ces produits et leur reproduction est à l'inverse très facile et beaucoup moins onéreuse.

Souvent, ces produits ne recèlent pas un degré de nouveauté tel qu'ils soient brevetables. Le logiciel intégré manque souvent de l'originalité nécessaire pour être protégé par le droit d'auteur.

Une protection spécifique existe. Une directive de la CEE la définit. Elle vise à protéger les circuits intégrés et les les produits semi-conducteurs selon certains principes de base communs, les modalités de protection étant

[5] Ou d'une partie de celles-ci.

laissées aux états.

La directive octroie des droits exclusifs au créateur d'une topographie : le droit d'autoriser ou d'interdire la reproduction d'une topographie, le droit d'autoriser ou d'interdire son exploitation commerciale.

Ces droits exclusifs ne s'appliquent pas à la reproduction aux fins d'analyse, d'évaluation ou d'enseignement des procédés, systèmes ou techniques incorporées au produit.

Une topographie n'est protégée que si elle est le produit d'un effort intellectuel propre du créateur et n'est pas généralement connue dans l'industrie du semi-conducteur.

La durée des droits exclusifs n'excède pas dix ans à partir de la première commercialisation ou à partir de la demande d'enregistrement de la topographie. La directive laisse aux Etats membres la liberté d'organiser ou non un système d'enregistrement ou de dépôt auprès d'un organisme spécialisé.

3.7.1 Détails pour la législation Belge

En Belgique, France, Pays-Bas, Allemagne, Royaume-Uni, le choix de la protection spécifique a été retenu (1990).

Le protection est accordée aux personnes physiques qui créent les topographies ou à leur employeur si elle est créée dans le cadre d'une relation de travail. En cas de travail sur commande, le commanditaire est considéré être le créateur.

Les droits exclusifs accordés sont relatifs à la reproduction et à l'exploitation commerciale. Le droit exclusif de commercialisation ne s'étend pas à une topographie après qu'elle ait été mise sur le marché.

La loi belge exclut toute formalité à l'obtention ou le maintient de la protection. La protection a une durée de dix ans après la première exploitation commerciale (15 ans après la création de la puce si pas d'exploitation commerciale).

Les sanctions pratiquées en cas de non respect sont l'indemnité en réparation du préjudice causé, la confiscation des produits contrefaits. Si un produit contrefait a déjà été commercialisé, le juge peut allouer au bénéficiaire une somme égale à la valeur des semi-conducteurs déjà vendus.

Chapitre 4

Contrats informatiques

4.1 Généralités

Les contrats du domaine de l'informatique couvrent un large panel de demandes :

- travail préliminaire à la conception ;
- fourniture de biens ;
- conception et réalisation d'un logiciel ;
- transfert de droits intellectuels ;
- formation du personnel de l'entreprise ;
- connexion entre différentes banques de données ;
- assistance/Maintenance.

Ces prestations peuvent faire l'objet de contrats distincts que ce soit avec un unique cocontractant ou plusieurs.

Le choix entre l'unicité ou la pluralité des contrats a une importance majeure. En effet, dans le cas d'un contrat unique, le défaut d'exécution d'une prestation autorise au client de demander la dissolution du contrat dans sa totalité. Alors que dans le cas de plusieurs contrats, la rupture des contrats se fait indépendamment les uns des autres et se fait, le plus souvent, au détriment du client.

4.2 Qualification des contrats informatiques

Les règles de droit applicables aux contrats informatiques sont difficilement décelables pour le juriste : multiplicité des activités offertes, multiplicité des intervenants, caractère « immatériel » du résultat.

Les contrats informatiques sont de deux natures essentiellement : *contrats de vente* et *contrats d'entreprise*. Les premiers appellent à la fourniture d'une chose (e.g., hardware), alors que les deuxièmes visent essentiellement à mettre en avant le travail effectué par l'homme (prestation de conseil, élaboration d'un logiciel spécifique, ...).

Rappelons toutefois qu'il ne faut pas considérer ces deux branches comme étant strictement disjointes. En effet, il se peut que, dans des cas exceptionnels, il faille accepter un caractère mixte au contrat.

4.2.0.0.3 Fourniture de biens : est typiquement un contrat de type *contrat de vente*. Il faut que les prestations du fournisseurs comportent une garantie contre les vices cachés.

4.2.0.0.4 Logiciel de base/logiciel système : fait l'objet, avec la vente de la machine cible (dans la plupart des cas), d'un contrat de vente. Juridiquement, on n'impose pas de garantie contre les vices cachés d'un programme. En effet, celui-ci étant toujours soumis à une marge d'erreurs irréductible (mises à jour et corrigées au fur et à mesure).

4.2.0.0.5 Logiciel d'application spécifique : fait l'objet d'un *contrat d'entreprise*, en ce sens, qu'il est conçu spécifiquement pour les besoins particuliers d'un client et nécessite, de fait, une prestation principalement intellectuelle de la part du concepteur.

Le cas particulier des **Progiciels**[1] fait polémique. En effet, certains pensent qu'il doit s'agir d'un contrat de vente de part le fait qu'il se confond avec la mise à disposition d'un bien particulier sans besoin d'une application intellectuelle. D'autres pensent, au contraire, qu'il doit s'agir d'un contrat d'entreprise en ce sens que la correction d'erreur, fruit d'un effort intellectuel, ne peut correspondre avec la notion de vente.

4.2.0.0.6 Système « clé en main » : combine études et conseils, prestations de développement/maintenance, ... et donc est associé à un contrat d'entreprise. Encore une fois, il est nécessaire d'introduire une garantie quant aux vices cachés portant sur le matériel fourni.

4.3 Négociation et exécution des contrats informatiques

4.3.1 Période pré-contractuelle

Les parties n'ayant pas émis leur volonté de s'engager, elles ne sont tenues à rien et les risques de rupture ne donnent, en principe, lieu à aucune indemnisation.

Dans la période pré-contractuelle, la jurisprudence impose une obligation d'information et de renseignement à charge des deux parties et une obligation de conseil à charge du fournisseur uniquement.

L'utilisateur doit clairement définir ses besoins, ses souhaits, les objectifs afin que le fournisseur puisse mener à bien le projet. Il peut, en outre, se faire aider en ayant recours à un conseil spécialisé. Le fournisseur doit prêter la main à l'utilisateur lors de la définition des objectifs pour éviter les problèmes ultérieurs. L'utilisateur doit également s'informer auprès du fournisseur au sujet du matériel et des garanties fournies par ce dernier.

Attention à la « clause des quatre-coins » qui annule tous les pourparlers antérieurs.

4.3.2 Période contractuelle

Le fournisseur se doit de :

- livrer au client un objet ou une prestation conforme à la commande, dans les délais prévus (difficile à évaluer) ;
- garantir le bon fonctionnement du système livré (englobant la notion de garantie sur les vices cachés) ;
- collaborer avec le client face à ses demandes (faculté d'adaptation) ;
- conseiller l'utilisateur quant à l'utilisation du système fourni.

L'utilisateur quant à lui se doit de :

- permettre au fournisseur d'opérer la livraison commandée (mise à disposition de locaux dans les mesures de sécurité préconisées) ;

[1] Logiciel standard, produit de série pré-constitué destiné à une clientèle d'acheteurs ou d'utilisateurs ayant des besoins similaires.

– collaborer avec le fournisseur pour lui permettre d'exécuter son obligation (ouvert au dialogue et à la communication) ;
– payer le prix convenu dans les délais fixés.

4.4 Clause des 4 coins

Le client reconnaît avoir pris connaissance du présent contrat et de toute annexe y relative en toutes leurs dispositions écrites et imprimées et déclare en accepter les termes et conditions. Il reconnaît, en outre, que ces documents constituent l'intégralité de l'accord intervenu entre les parties, remplaçant ou annulant toutes propositions ou engagements écrits ou verbaux les précédant et toutes autres communications entre les parties ayant trait au présent contrat.