**6.1 La responsabilité juridique**

|  |  |  |
| --- | --- | --- |
| **Responsabilité pénale** | **Responsabilité civile** | **Responsabilité administrative** |
| * Sanctions individu * Par emprisonnement * amende | **Responsabilité contractuelle**   * Elle résulte d’un acte juridique, autrement dit une manifestation volontaire de droit. * Elle a pour origine l’inexécution et pour sanction des dommages et intérêts. | Elle consiste à engager la responsabilité de l’Etat. |
|  | **Responsabilité délictuelle**   * Elle résulte d’un fait juridique, soit une manifestation involontaire de droit. * Elle est également sanctionnée par des dommages et intérêts. |  |

En Droit Français, on distingue deux grandes responsabilités. :

* La première est la responsabilité pénale. L’objet de la responsabilité pénale est la sanction de l’individu en vue de la protection de la société. Cette sanction se manifeste généralement par une peine d’emprisonnement, et/ou une amende.
* La seconde est la responsabilité civile, dont l’objet est la réparation d’un dommage. En matière de responsabilité civile, il convient de distinguer **la responsabilité contractuelle** et la **responsabilité délictuelle**. La responsabilité contractuelle sanctionne l’inexécution d’un contrat qui résulte d’un acte juridique (l’acte juridique est une manifestation volontaire de Droit). La responsabilité délictuelle résulte quant à elle d’un fait juridique (Soit une manifestation involontaire de Droit).

Afin d’engager la responsabilité civile, il convient de réunir trois conditions en pratique cumulatives:

* Un dommage
* Un fait dommageable
* Un lien de causalité

1. **Le dommage**

Il existe deux terminologies en matière de dommage. On parle de dommage subi ou bien de préjudice subi. Le dommage est l’atteinte qu’une victime peut avoir lorsqu’un fait dommageable est soumis à son encontre. En Droit français, on distingue deux types de dommages :

* Le dommage patrimonial, soit celui qui se chiffre aisément. Il est principalement à caractère matériel ;
* Le dommage extrapatrimonial, soit celui qui se chiffre difficilement. Le prix de la douleur suite par exemple à au décès d’un enfant ne tient pas de l’évidence. Le préjudice sexuel est un autre exemple.

On distingue également le préjudice matériel, le préjudice moral, ou encore le préjudice physique. Pour que le dommage ou le préjudice soit indemnisé, il doit revêtir un certain nombre de caractères afin d’être validé par le juge.

**Cinq caractéristiques** doivent être respectées pour établir le dommage :

* Il doit être **certain**, c’est-à-dire en principe non-hypothétique. La seule exception est la perte de chance, invocable dans deux cas : un avenir rendu inaccessible par le fait d’un acte relevant de la responsabilité délictuelle, ou le non-respect d’un accord conclu lors de pourparlers ;
* Il doit être **direct**, ce qui signifie que seule la victime du dommage peut prétendre à réparation. Il y a deux exceptions : la victime par ricochet et les victimes collectives. La victime par ricochet est une victime collatérale du dommage (cf. exemple de l’enfant mort). Les victimes collectives ont été introduites par la loi du 17 mars 2014 qui introduit entre autres l’action de groupe, celle-ci permettant une action collective pour un même fait dommageable. Le caractère collectif permet également à certaines associations ou corps de métier de réclamer des dommages et intérêts ;
* Il doit avoir un **intérêt légitime**, ce qui signifie que le demandeur doit pouvoir prétendre à des dommages et intérêts ;
* Le dommage est compensé par **une seule réparation** ;
* Enfin, il y a la **prévisibilité**, qui se pose beaucoup en matière contractuelle. Elle dicte que l’on doit être en mesure de prévoir les conséquences de l’inexécution contractuelle.

1. **Le fait dommageable**

Le fait dommageable est souvent appelé la faute, et n’a pas nécessairement un caractère prémédité. Pour que la responsabilité soit engagée, encore faut-il qu’à l’origine il se soit passé quelque chose. Sans faits, pas de responsabilité. La question étant, quand sommes-nous responsables, et surtout qu’est-ce qui nous rend responsables de quelque chose qui s’est produit ? Il est à noter que l’on peut être responsable du fait de quelqu’un d’autre.

Pour qu’il y ait responsabilité, encore faut-il qu’il se soit passé quelque chose, en effet, le fait qui engage la responsabilité doit entraîner un dommage, et c’est pourquoi on parle de fait dommageable et non pas de faute.

En principe, c’est lorsque l’on n’a pas respecté l’une de ces obligations qu’on devient responsable. Ceci parait assez simple à saisir en matière contractuelle, car on va rechercher si nos obligations contractuelles ont bien été respectées, si on a commis une faute, ou encore une inexécution contractuelle.

Précédemment à la réforme du code civil, il existait deux obligations contractuelles : l’obligation de moyen et l’obligation de résultat. Depuis la réforme du Code Civil, cette distinction tend à disparaitre. En effet, l’article 1341 du Code Civil dispose que le créancier a Droit à l’exécution de l’obligation ; il peut y contraindre le débiteur dans les conditions prévues par la loi.

En tout état de cause, il faut savoir qu’aujourd’hui, on a une tendance à une plus grande indemnisation parce qu’on ne prend pas en compte uniquement la notion de faute. Le manquement à une obligation peut aussi être indemnisé par des dommages et intérêts. Le juge peut également prendre en considération le risque que l’on peut faire courir à une partie (cf. principe de précaution : sanctionner un fait qui pourrait amener des conséquences néfastes pour une des parties dans le futur).

Le juge prend aussi en compte, la négligence, la maladresse ou encore l’imprudence.

En matière **délictuelle** en revanche, pour engager la responsabilité, on va rechercher un fait dommageable qui a été commis par nos soins. On parle alors de responsabilité du fait personnel. (Art. 1242 du code civil)

On peut également être responsable d’une personne dont on répond. Il existe deux types de sous-responsabilités d’une personne dont on répond : la responsabilité du commettant du fait de son préposé ou encore la responsabilité des parents du fait des enfants.

Troisièmement, il y a la responsabilité du fait des choses. La loi dispose que l’on est responsable du fait des choses dont à la garde, la direction et le contrôle.

1. **Le lien de causalité**

Le lien de causalité se définit comme le lien entre le fait dommageable et le dommage. En conséquence, une problématique se pose : le cas où l’on a un dommage mais plusieurs faits ayant contribué à la réalisation de ce dommage. Il existe deux théories à ce sujet : celle de la causalité adéquate et celle de l’équivalence des conditions.

La **causalité adéquate** correspond au fait sans lequel le dommage ne serait pas produit et qui permet d’identifier celui ou celle dont la responsabilité est engagée.

L’équivalence des conditions est lorsqu’on prend en compte tous les faits qui ont participé à la réalisation du dommage.

1. **Autres principes**

Il y a le principe de non cumul des responsabilités, qui signifie que l’on ne peut pas engager simultanément une responsabilité contractuelle et une responsabilité délictuelle.

Ensuite, les causes d’exonération de responsabilité. Dans certaines situations, même si le fait est avéré juridiquement, la responsabilité ne sera pas engagée. Il existe trois cas :

* La force majeure, soit un évènement imprévisible, irrésistible et extérieur à l’auteur.
* Le fait d’un tiers, lorsqu’un tiers est intervenu en plus dans l’accident
* Fait de la victime (on ne peut réclamer des dommages pour un fait dont on est responsable – « nul ne peut se prévaloir de sa propre turpitude »)

**6.2 Responsabilité des prestataires externes**

Le développement d’internet a corollairement permis l’expansion de la liberté d’expression. En effet, internet est devenu un espace d’échange, ou chacun peut émettre de son avis et donner ses opinions sur des sujets tant politiques qu’économique sou sociétaux. Cependant, même si cette liberté d’expression est permise et consacrée par le droit fondamental, elle connait ses limites à partir du moment où elle entrave le Droit des autres. En effet, l’auteur d’une information illégale peut voir sa responsabilité pénale et civile engagée. Se pose donc la question des prestataires techniques. En effet, le prestataire technique a pour mission de donner accès à cette information, mais pour autant il n’en est pas l’auteur. En conséquence, ces prestataires techniques invoquent le fait qu’il faut leur appliquer une responsabilité particulière car ils ne peuvent maitriser la volatilité de l’information. Historiquement, il s’est posé la question de calquer le régime de responsabilité en cascade de la presse aux prestataires externes.

(En matière de presse, le directeur de la publication est responsable de ce qui a été émis apr. l’auteur.)

Cependant, il a été difficile de transposer cette responsabilité en cascade car il est difficile d’imposer une obligation de surveillance pour les prestataires externes. C’est ainsi que la loi pour la confiance en l’économie numérique (**LCEN), en 2004, dans son article VI**, a posé un régime spécifique de responsabilité pour les prestataires techniques qui ont la qualification juridique d’hébergeur, et un principe de non responsabilité pour les fournisseurs d’accès internet.

1. **La qualification juridique d’hébergeur et une responsabilité allégée**
2. **La définition d’un hébergeur**

Au sens de la loi LCEN, l’article 6-1-2 dispose que « les hébergeurs sont des personnes physiques ou morales, qui assurent, même à titre gratuit, pour mise à disposition du public, par des services de communication au public en ligne, le stockage de signaux, d’écrits, d’images, de sons ou de message de toute nature fournis pas des destinataires de ces service. »

L’hébergeur est donc un prestataire technique et informatique, qui n’est pas le créateur des contenus qu’il héberge, mais il fournit le contenu et le rend accessible au public. La jurisprudence s’est posé la question de savoir la différence entre un hébergeur et un éditeur.

La jurisprudence de la CJUE, dans un arrêt du 23 Mars 2010, a posé une différence entre un éditeur et un hébergeur. Elle dispose que l’hébergeur est dit neutre dans les contenus qu’il décide de communiquer au public, à la différence d’un éditeur, qui lui a un rôle actif vis-à-vis des contenus qu’il pose et qu’il sélectionne afin de les mettre en valeur. A titre d’exemple, Facebook fournit les moyens techniques de diffuser des informations sur internet, et chaque utilisateur poste ensuite le contenu qu’il souhaite de la manière dont il le souhaite. Facebook est donc qualifié juridiquement d’hébergeur et peut donc bénéficier d’une responsabilité allégée. Il en va de même pour Dailymotion, ainsi que posé par l’arrêt de la chambre civile du 17/02/2011 de la cour de cassation.

En revanche, des sites comme eBay ou Priceminister assurent un contrôle systématique des annonces mises en lignes, ils autorisent la recherche de mots-clés pertinents, et organisent notamment l’anonymat des vendeurs. Ce pourquoi la CJUE, dans un arrêt du 12 juillet 2011, les a qualifiés d’éditeurs.

1. **La responsabilité allégée**

La responsabilité de l’hébergeur ne sera engagée que si trois conditions **cumulatives** sont respectées :

* Il doit avoir la faculté technique d’intervenir ;
* Il doit avoir eu connaissance de l’activité ou de l’information illicite ;
* **Il doit avoir choisi volontairement le fait de ne rien faire.**

L’engagement se fait au titre des articles 1241 et 1242 du Code Civil (responsabilité délictuelle).

1. **La qualification juridique du fournisseur d’accès et le principe d’irresponsabilité**
2. **La définition d’un fournisseur d’accès**

Un fournisseur d’accès internet est la société qui fournit à l’utilisateur des services de communication publique en ligne. Juridiquement, il est donc assimilé à un simple transporteur de données, sans possibilité de contrôler ce qui transite par le biais de son service. La loi ne prévoit donc pas d’obligation de surveillance de la part des fournisseurs d’accès internet.

La loi prévoit tout de même qu’il doit informer ses utilisateurs, qu’il existe des moyens de restreindre l’accès à certains services comme le contrôle parental.

1. **Le principe de non responsabilité**

La LCEN pose un principe de non responsabilité des fournisseurs d’accès internet, à condition que ces derniers respectent une totale neutralité dans les informations diffusées. En conséquence, la neutralité est l’unique condition de l’irresponsabilité des fournisseurs d’accès internet.

1. **Les obligations des prestataires externes**
2. **Une obligation d’identification des prestataires externes**

Ainsi que précédemment mentionné, il n’existe pas d’obligation de surveillance par les prestataires externes. Cependant, il existe un corollaire à la responsabilité allégée des hébergeurs ou à la responsabilité des fournisseurs d’accès internet. A ce titre, l’article 6.2 de la LCEN dispose d’une obligation d’identification.

Autrement dit, les prestataires techniques se voient imposer des obligations visant à permettre l’identification des auteurs de contenu illicite, et à défaut, ils peuvent voir leur responsabilité engagée. Les prestataires techniques ont l’obligation de conserver ces données, pendant un an, et sont responsables par la loi s’ils ne les ont pas conservées, et en conséquence ne peuvent communiquer ces informations à toute autorité compétente.

La loi a prévu un délit pénal afin de limiter les dénonciations abusives auprès des hébergeurs et des fournisseurs d’accès internet alors même que l’information n’était pas illicite.

1. **Une obligation contractuelle**

Comme le dispose l’article 11-147du Code Civil, le prestataire externe doit respecter l’obligation contractuelle comme elle existe chez son co-contractant. De plus, les hébergeurs ont une obligation contractuelle d’assurer le stockage des données, et également de permettre un accès en continu au réseau sous peine de voir leur responsabilité engagée.

**6.3 Responsabilité de l’administrateur réseau**

Tout dirigeant d’entreprise a des intérêts antinomiques mais légitimes à gérer au sein de sa structure. En effet, l’employeur souhaite protéger les intérêts de son entreprise en protégeant la fuite des informations stratégiques, en prévenant l’apparition de virus, ou encore en empêchant la circulation des contenus illicites au sein de son réseau. Cela passe donc par la sécurisation de son réseau.

A l’inverse, nombre de salariés revendiquent le droit à une vie privée sur le lieu de travail, qui se matérialise notamment à travers une connexion internet à des fins personnelles. Afin d’encadrer et de limiter un usage excessif d’internet sur le lieu de travail, l’employeur dispose, au titre de son pouvoir de direction, d’un droit de contrôle sur son salarié (arrêt de la chambre sociale du 14 Mars 2000, « Dujardin contre la société Instinct »). Néanmoins ce pouvoir ne doit pas pour autant méconnaitre le respect à la vie privée ainsi que le secret des correspondances.

La CNIL a, dans plusieurs rapports, reconnu un droit à la vie privée pour le salarié, tout en soulignant qu’il était irréaliste d’interdire toute utilisation d’internet à des fins personnelles.

L’administrateur réseau est au carrefour de ces deux perspectives. En effet, il est à la fois en charge d’assurer la sécurité du réseau à la demande d’une autorité hiérarchique, et de la sécurité des données aussi bien professionnelles que personnelles des salariés.

1. **Le rôle de l’administrateur réseau**
2. **Les missions de l’administrateur réseau**

L’administrateur réseau doit veiller à l’utilisation optimale du réseau et assurer la sécurité des données en entreprise. Il est en charge de la mise en place du système d’information, et il doit prévenir au mieux toute intrusion au sein de celui-ci.

Les directives communautaires, comme la Loi Informatique et Libertés, confèrent une obligation d’assurer la sécurité des traitements informatiques. L’article 29 de la Loi Informatique et Libertés dispose  qu’il est engagé vis-à-vis des personnes concernées a « prendre toute précaution utile afin de préserver la sécurité des informations, et notamment d’empêcher qu’elle ne soit déformée, endommagée, ou communiquée à des tiers non autorisés. La loi semble donc imposer une obligation de moyen à l’administrateur réseau.

Cependant, la directive communautaire 95/46/CE, dans son Article 17, semble poser une obligation de moyen renforcée. En effet, cet article 17 dispose que « le responsable de la sécurité doit mettre en œuvre les mesures techniques et d’organisation 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 toute autre forme de traitement illicite. »

La directive du 12 juillet 2002 ne solutionne toujours pas cette question de l’obligation, puisqu’elle invite l’administrateur réseau à « prendre les mesures appropriées pour assurer la sécurité de leur service », et d’autre part à « un devoir d’information des risques encourus par l’utilisateur. »

1. **Le statut de l’administrateur réseau**

Afin de garantir au mieux la sécurité du réseau, l’administrateur doit pouvoir accéder à toutes les données contenues dans les messageries, ainsi que les fichiers utilisateurs. Autrement dit, la jurisprudence prévoit qu’il puisse accéder à l’intégralité des informations, mêmes privées, afin de pouvoir réaliser au mieux ses obligations.

C’est la cour d’appel, dans l’arrêt ESPCI du 17 décembre 2001, qui a énoncé : « il est dans les fonctions de l’administrateur réseaux d’assurer le fonctionnement normal de ceux-ci, ainsi que leur sécurité, ce qui entraine entre autres qu’ils aient accès aux messageries et à leurs contenu, ne serait-ce pour débloquer ou éviter des démarches hostiles ».

En conséquence, l’administrateur réseau dispose de pouvoirs étendus afin de permettre une bonne utilisation du réseau. Il peut donc avoir accès aux informations des utilisateurs, à savoir leur messagerie, leur connexion internet, la durée de visite des sites internet, contrôler les débits, identifier la durée des connexions, répertorier les sites les plus fréquemment utilisées ou leurs tentatives de connexion, contrôler les pièces jointes, ainsi que leur volume.

Il peut avoir l’ensemble des informations émises, reçues et créées par le salarié. La CNIL, notamment dans son rapport du 5 février 2002, confère un statut particulier à l’administrateur réseau et lui permet d’avoir un accès illimité à l’ensemble des informations relatives au salarié. Ce statut particulier n’est pas contraire à la Loi Informatique et libertés du 6 janvier 1978.

Toutefois, ce statut atypique est évidemment encadré par la loi et par le secret professionnel.

1. **Un contrôle encadré et limité**
2. **L’obligation de confidentialité**

Cette obligation de confidentialité est posée par l’arrêt Nikon du 21/10/2002. Cet arrêt a reconnu expressément une vie privée au salarié. Il dispose : « que même au temps et lieu de travail, le salarié a droit au respect de l’intimité de sa vie privée, que celle-ci implique en particulier le secret de ses correspondances, que l’employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l’employeur aurait interdit une utilisation non professionnelle de l’ordinateur. >>

Ce respect à la vie privée se fonde à travers l’article 8 de la convention Européenne de sauvegarde des droits de l’homme et du citoyen, de l’article 9 du code civil, de l’article 1 de la Loi Informatique et Libertés du 6 janvier 1978, ou encore de l’article 226-15 du Code Pénal.

En vertu de la vie privée, l’administrateur réseau est donc soumis au secret professionnel et ne peut divulguer les données personnelles auxquelles il a accès. Cette obligation de confidentialité couvre aussi bien la messagerie personnelle, que les fichiers personnels relevant de la vie privée.

Si la jurisprudence reconnait la possibilité à l’administrateur réseau de lire le contenu des messages, il n’est en revanche pas autorisé à les divulguer à son supérieur hiérarchique. Se pose donc la question, pour un administrateur réseau, de savoir comment réagir lorsqu’une situation porte préjudice à l’entreprise. L’arrêt Nikon ou encore l’arrêt ESPCI ne précisent à aucun moment comment prendre les sécurités qui s’imposent lorsque l’administrateur réseau découvre une situation préjudiciable pour l’entreprise.

La mission de l’administrateur réseau est donc très délicate, car il devra mettre fin aux comportements frauduleux, sans pour autant en informer son supérieur hiérarchique, qui a pourtant toute autorité de décision. A ce titre, la cour d’appel a déjà sanctionné un administrateur réseau pour avoir informé ses supérieurs sur le contenu des messages auxquels il avait accès. Cet arrêt précise que la divulgation d’un message ne se rattache pas aux objectifs de sécurité de l’administrateur réseau, et doit être sanctionné sur le fondement de l’article 432-9 du Code Pénal.

Cependant, la cour d’appel d’Aix en Provence du 17 décembre 2002 est venue tempérer ce principe de non divulgation.

1. **Le contrôle doit être loyal, transparent et proportionné**
2. **Un contrôle transparent**

La démarche de contrôle d’un administrateur réseau doit se faire dans une logique de transparence vis-à-vis des salariés. En effet, les salariés doivent avoir été informés par l’employeur de la mise en place d’un dispositif de contrôle, soit à travers leur contrat de travail, soit à travers une charte informatique (cf. article L.121-8-1 du Code du travail, qui prévoit notamment qu’aucune information ne peut être collectée à l’insu du salarié).

Les comités d’entreprise, ou encore les délégués du personnel, doivent être informés de ce contrôle. Lorsque ce contrôle est automatisé, il doit faire l’objet d’une déclaration à la CNIL. La CNIL préconise de plutôt faire des statistiques des sites référencés que des contrôles nominatifs ou individualisés.

1. **Un contrôle loyal**

Le contrôle de l’administrateur réseau doit se faire de manière impartiale et sincère. Autrement dit, l’administrateur réseau doit agir dans le cadre de ses fonctions et son action ne peut pas découler d’une initiative personnelle ou encore d’un ordre hiérarchique, mais d’une nécessité justifiée uniquement par des impératifs de sécurité.

1. **Un contrôle proportionné**

Le contrôle de l’administrateur réseau doit être proportionné au but recherché. Il appartient à l’administrateur réseau d’utiliser uniquement les moyens permettant de remplir la sécurisation du réseau, sans pour autant aller au-delà. Son action doit donc s’inscrire dans une logique cohérente. Par exemple, si afin de vérifier l’optimisation du réseau, cela ne passe que par le contrôle de la volumétrie des messages, l’administrateur réseau ne devra pas aller chercher le contenu des mails pour vérifier si le réseau est optimal.

1. **La mise en place d’une charte informatique**

La mise en place d’une charte informatique à un intérêt fondamental dans l’entreprise à plusieurs titres, car elle permet d’informer le salarié des contrôles qui peuvent avoir lieu, et des usages pratiqués ou non dans l’entreprise. Généralement, ces chartes sont annexées au règlement intérieur, et il est demandé au salarié d’accepter contractuellement cette charte, soit par le biais de son contrat de travail, soit par le biais d’un avenant contractuel.

Pour autant, cette charte informatique ne règle pas les questions du rôle de l’administrateur réseau, et à juste titre cette charte devra être soumise au comité d’entreprise s’il en existe un et/ou au comité d’hygiène et de sécurité, et cette charte devra être communiquée notamment à l’inspecteur du travail.

**6.4 La responsabilité des concepteurs de solutions logicielles**

1. **Le processus lié au développement du logiciel**

La création d’un logiciel répond généralement à un processus spécifique qui s’élabore de la manière suivante :

1. Rédaction d’un cahier des charges qui décrit les attentes et le besoin du client
2. Elaboration d’un calendrier avec des délais précis d’avancement assortis de pénalités en cas de non-respect de ces délais
3. Une analyse par l’entreprise des besoins du client et de la faisabilité technique, de l’identification des contraintes ou encore de la prévision des moyens matériels et humains par l’entreprise
4. Réalisation de la documentation relative à l’utilisation du logiciel
5. La construction de l’architecture du logiciel et l’écriture du code source
6. La livraison du logiciel développé au client et les indications d‘utilisation de ce dernier avec l’explication du gain économique espéré
7. **Les obligations juridiques liées à la conception d’un logiciel**

La règlementation informatique et libertés fait peser la responsabilité juridique aussi bien pénale que civile sur le responsable de traitement, c’est-à-dire celui qui détermine les finalités et les moyens du logiciel. Par conséquent, les concepteurs de logiciels, qu’ils commercialisent ensuite auprès des responsables de traitement, n’encourent aucune responsabilité sur le fondement de la règlementation informatique et libertés.

1. **L’obligation d’information : une responsabilité antérieure à la livraison**

Dès la phase de négociation, le concepteur de solutions logicielles doit fournir à son client toutes les informations nécessaires au bon fonctionnement du projet informatique. Cette obligation d’information a pour objectif de rééquilibrer la relation contractuelle entre le professionnel qui créée le logiciel et la société cliente qui peut être profane en la matière.

Cette obligation d’information se décompose généralement en trois points distincts :

* L’obligation de renseignement, soit une information sur les qualités et le service proposé ;
* L’obligation de mise en garde, qui oblige le concepteur de solutions logicielles à informer le client de toutes les perturbations que la mise en place de ce logiciel peut engendrer (ralentissements, pertes de données…), tant pendant le démarrage du logiciel que pendant la période de rodage, et il doit également informer le client de toute perturbation que ce logiciel pourrait entrainer avec les logiciels déjà existants au sein de l’entreprise ;
* L’obligation de conseil, soit le devoir d’informer le client et de le conseiller sur les choix à effectuer en fonction des spécifications du logiciel, étant précisé que le cahier des charges est là pour spécifier les besoins du client, et que le concepteur de solutions logicielles doit révéler les insuffisances ou les erreurs de l’analyse fournie par le client.

Cette obligation d’information est une obligation de moyen (soit le devoir tout mettre en place pour aboutir au résultat attendu, quitte à échouer malgré tout). Cette obligation d’information, qu’on va imposer au concepteur de solutions logicielles, va être analysée vis-à-vis du client avec lequel il interagit. La chambre commerciale de la cour de cassation, dans un arrêt du 14 Mars 2000, a disposé des termes suivants :

« Attendu qu’ayant révélé que l’acquisition du progiciel avait été précédée d’une visite de la société A. au cabinet B. ainsi qu’une démonstration en présence de plusieurs membres du personnel, l’arrêt retient que B., utilisateur de longue date de programmes informatiques pour les besoins de sa profession était à même d’évaluer si les performances du logiciel qu’il avait choisi de commander étaient adaptées à ses besoins ; et qu’en l’état de ces constatations et appréciations, la cour a légalement justifié sa décision. >>

L’arrêt de la chambre commerciale du 6 Mai 2003 dispose que le concepteur de solutions logicielles n’est pas dispensé de l’obligation alors même que son client était doté d’un service informatique interne actif et compétent, dès lors, que ces informaticiens ne disposaient pas de toutes les compétences nécessaires s’agissant de l’installation de logiciels spécifiques.