Les établissements de crédit, l'éthique et les nouvelles technologies

FRANÇOIS SCHWERER
Administrateur du Centre Montesquieu

Introduite à l'origine dans les textes normatifs français, par le biais des règles de fonctionnement des marchés financiers, la prise en compte des préoccupations éthiques intéresse de plus en plus les banques. L'évolution de l'appréciation des risques et l'irruption des nouvelles technologies dans le quotidien des établissements conduisent à un renforcement considérable de cette prise en compte de cette dimension éthique dans toutes les règles internes de fonctionnement comme dans toutes les relations entre la banque et les tiers.

Selon l'ancien bâtonnier de Paris, Dominique de la Garanderie, la multiplication des codes d'éthique à laquelle nous assistons aujourd'hui «est une conséquence directe de l'insécurité juridique induite par la mondialisation, qui place l'entreprise face à une multiplicité de systèmes juridiques nationaux en perpétuelle évolution, comme de la difficulté à identifier certains délits relevant de l'inobservation d'une obligation morale (délit d'initié, prise illégale d'intérêts...)» [1]. D'un autre point de vue, nous pouvons admettre, avec Pascal Diener, que l'éthique des affaires est un investissement, puisque «c'est la poursuite méthodique d'un intérêt bien compris qui rapporte à moyen et long terme. Conjuguer éthique et stratégie dans les entreprises les plus performantes du monde devient la condition d'une réussite durable» [2].

L'irruption de l'éthique dans la vie des affaires a commencé aux Etats-Unis avec l'adoption en 1977 du Foreign Corrupt Practices Act qui recommandait aux entreprises d'adopter un programme de prévention et de détection des délits en sept points :

- établissement de principes et procédures devant guider un comportement éthique ;
- nomination, dans chaque établissement, d'un responsable éthique ;
- mise en avant de l'intégrité et de l'exemplarité du responsable de l'éthique ;
- communication de ces principes et procédures à tous les membres du personnel ;
- mise en place de mécanismes de contrôle ;
- établissement de sanctions en cas de violation des règles établies ;
- prise de mesures pour éviter les récidives en cas de délit.

Depuis cette époque les Américains n'ont eu de cesse d'imposer au monde leurs normes éthiques, et en 1997, le Council on Economic Priorities Accreditation Agency a promu la norme SA (Social Accountability) 8000. Celle-ci développe en huit chapitres les règles à respecter au regard du travail des enfants [3], du travail forcé, de l'hygiène et la sécurité, de la liberté syndicale, de la lutte contre la discrimination, des pratiques disciplinaires, du temps de travail et des rémunérations. Elle se conclut par des prescriptions relatives au système de management permettant de faire vivre la norme.

L'Europe n'est pas restée en marge de cette évolution, et le «code de conduite» européen du 25 juillet 1977 édicte des règles qui se veulent des principes généraux auxquels tous les systèmes juridiques européens doivent se conformer :

- toute opération sur les marchés implique le respect non seulement de la lettre mais encore de l'esprit de toutes les normes juridiques en vigueur ;
- le public doit disposer d'une information loyale, accessible à tous en même temps de façon que personne ne puisse être privilégié ;
- les actionnaires doivent pouvoir jouir d'une égalité de traitement ;
- les membres des organes sociaux doivent s'abstenir d'entraver le bon fonctionnement du marché des titres ;
- les intervenants sur les marchés financiers doivent toujours avoir un comportement loyal, même si cela les prive d'un avantage financier quelconque ;
- les intermédiaires financiers s'efforcent d'éviter tout conflit d'intérêt.

C'est dans ce contexte qu'évoluent aujourd'hui les banques françaises.

La déontologie bancaire et financière régulée en France

En ce qui concerne les établissements de crédit, la prise en compte de l'éthique a suivi plusieurs étapes. En premier lieu, elle a concerné la régulation financière, qui est l'œuvre tant de la Commission des opérations de bourse (Cob), en vertu de la loi n° 89-531 du 2 août 1989 qui a modifié l'ordonnance n° 67-833 du 28 septembre 1967 que du Conseil des marchés financiers (CMF). Ce dernier a édicté des «*règles de bonne conduite applicables aux prestataires habilités*».

Elle s'est intéressée ensuite à la régulation bancaire proprement dite, laquelle est partagée entre le Comité de la réglementation bancaire et financière qui édicte les règles et la Commission bancaire qui «est chargée de contrôler le respect par les établissements de crédit des dispositions législatives et réglementaires qui leur sont applicables et de sanctionner les manquements constatés […]. Elle veille au respect des règles de bonne conduite de la profession» [4].

Les premières règles de comportement édictées par la Cob ont mis en avant trois principaux types de comportement qu'il convient d'éviter, car fautifs :

- le délit d'initié qui suppose que l'information privilégiée soit précise, particulière, certaine et de nature à influencer le cours du titre dès sa publication ;
- le délit de fausse information, qu'il s'agisse d'une information inexacte, imprécise ou trompeuse (à la différence de la loi pénale, la Cob ne rend pas nécessaire, pour réprimer le délit, de démontrer l'existence d'un lien entre la diffusion de la nouvelle dans le public et la volonté d'agir sur le cours) ;
- et le délit de manipulation des cours qui correspond à une manœuvre faite sciemment et ayant pour conséquence d'induire autrui en erreur.

Ces règles ne concernaient essentiellement que les comportements vis-à-vis des marchés, elles n'intéressaient pas les relations entre la banque et son client investisseur. Dans ce domaine, il est bon de voir l'évolution internationale de ces exigences en examinant la façon dont nos voisins helvétiques réfléchissent à ces questions ; c'est ainsi que, tirant les conclusions de l'affaire Abacha[5], la Commission fédérale des banques suisses a envisagé une nouvelle réglementation qui imposerait notamment aux membres de la direction des établissements actifs dans la gestion de fortune de connaître les clients les plus importants. Elle a même envisagé de rendre obligatoire pour les banques qui rompent une relation avec un client, parce qu'il est douteux, d'en avertir les autres banques. Mais pour l'instant, elle semble en être restée au stade des réflexions.

Plus immédiatement intéressante, car directement applicable aux banques françaises présentes sur la toile, la décision n° 99/07 du CMF, «relative aux prescriptions et recommandations pour les prestataires de services d'investissement offrant un service de réception transmission ou d'exécution d'ordres de bourse comportant une réception des ordres via internet». Cette décision est, d'une part, rédigée en termes très généraux qui pourraient la rendre transposable, par analogie, à de nombreuses opérations financières réalisées via internet (comme par exemple les virements), et d'autre part, porteuse de nouveautés juridiques importantes.

Ce texte met l'accent sur la transparence et la précision des informations que le prestataire doit porter à la connaissance de ses clients potentiels. Puis il définit les dispositions qui doivent être respectées «avant que ne soient rendus les premiers services». En particulier, l'identification du client, la convention d'ouverture de compte, la convention de services et le consentement du client forment un bloc qui est préalable à toute prestation. Mais dès lors que ce bloc est respecté, la responsabilité des opérations change de tête ; elle passe au «maître du système». Ce sera désormais à lui de prouver que l'information qu'il émet est bonne, et non au client qui la reçoit de prouver qu'elle est mauvaise. Les articles 9 à 12 précisent ainsi sur quoi porte notamment cette responsabilité : «*le prestataire s'assure que le client reçoit l'information prévue…*» ; «*le prestataire doit disposer d'un système automatisé de vérification du compte…*» ; «*… le système doit assurer le blocage…*» ; etc. Ce renversement de la charge de la preuve aboutit à un véritable transfert du risque de fonctionnement du système puisque l'article 12 précise que «*le prestataire assume la responsabilité de la bonne exécution de l'ordre*». C'est donc que l'ordre, une fois émis, est bien reçu et exécuté. Pour reprendre une formule-choc de Maître Bensoussan, «*les électrons voyagent aux risques et périls du prestataire et non plus aux risques et périls de l'émetteur*». Enfin, cette décision conduit le prestataire à assumer la charge de la sécurité et de la preuve. En particulier, «*en cas de dysfonctionnement du système de réception d'ordres, le prestataire habilité fait ses meilleurs efforts* [6] *pour informer les utilisateurs de la nature et de la durée prévisible du dysfonctionnement*». De même, le prestataire est tenu de maintenir un système ayant toujours une capacité suffisante, compte tenu de sa clientèle et de ses perspectives de développement. Enfin, «*le prestataire habilité s'assure qu'en regard des normes courantes de sécurité* [7] *des systèmes informatiques, le système informatisé de réception d'ordres mis en place est correctement sécurisé*». Compte tenu de ces obligations, le prestataire doit normalement faire certifier juridiquement son chemin de preuve.

Plus général, car visant directement toutes les activités, mais moins strictement opérationnel car n'étant pas un texte créant des règles immédiatement obligatoires, le Livre blanc de la Commission bancaire et de la Banque de France : «Internet, quelles conséquences prudentielles ?» Les recommandations qui y figurent «revêtent un caractère de bonnes pratiques, destinées à maîtriser les risques encourus par le recours à internet comme canal de distribution des services bancaires et financiers» [8].

Les premières recommandations qu'on y trouve s'adressent aux dirigeants des établissements de crédit et concernent le contrôle interne, la lutte contre le blanchiment et la sécurité.

Il s'agit, pour ces dirigeants de :

- formaliser dans un document validé par les organes exécutifs la stratégie commerciale internet de l'établissement en précisant en particulier les risques encourus ; «*A ce titre, l'établissement devrait formaliser sa stratégie commerciale sur internet, dans un document validé par les*

organes exécutifs et délibérants, qui développerait en particulier le plan de développement de l'activité, en termes de services offerts, de clientèle, de volume d'activité et de rentabilité, en tenant compte de manière exhaustive des facteurs de risques techniques et commerciaux […]. *A tout le moins, trois types de risques de crise devraient être pris en compte : le risque commercial de forte chute du produit net bancaire, le risque d'atteinte à l'image et à la réputation de l'établissement suite à des problèmes techniques, le risque technologique d'inadaptation du système face à la croissance de l'activité*» [9] ;

• élaborer un document relatif à la maîtrise des risques, déclinés en risques de contrepartie, en risques juridiques [10] et techniques, qui fournit à la direction générale une vision globale des risques encourus ;

• fournir au responsable du contrôle interne une compétence explicite et exhaustive sur toutes les questions relatives à la sécurité ;

• évaluer les moyens nécessaires pour assurer la continuité de l'entreprise et sa crédibilité vis-à-vis des clients et partenaires, tout particulièrement en situation de crise ; «*Il est raisonnable de compléter la réflexion par l'étude de scénarios de crise, sur la base d'hypothèses extrêmes, impliquant des moyens importants pour rétablir la continuité de l'entreprise et sa crédibilité vis-à-vis des clients et partenaires. Les hypothèses pourraient être :*

– une attaque majeure du système en vue de provoquer son indisponibilité et ruiner la crédibilité technique de l'établissement ;

– un défaut de conception entraînant une dégradation inacceptable des performances du système face à une pointe de charge, provoquant la fuite de la clientèle et nécessitant des travaux importants pour rétablir le niveau de service promis aux clients ;

– une campagne systématique de dénigrement menée par des concurrents sur la base de problèmes techniques, réels ou imaginaires» [11] ;

• maîtriser les prestations externalisées par l'établissement, en prévoyant des clauses d'audit dans ses contrats ; «*Sur le fondement de l'article 14 du règlement n° 97-02 relatif au contrôle interne des établissements de crédit* […] *l'établissement devrait démontrer qu'il maîtrise tous les aspects du système d'information utilisé, y compris lorsque celui-ci est confié à un prestataire extérieur, que ce soit pour le développement comme pour l'exploitation technique. L'établissement devrait avoir accès à toute l'information sur les spécifications fonctionnelles et techniques du système, et déterminer librement le paramétrage* […]. *Le libre accès des autorités de tutelle ou instances de contrôle aux installations externes devrait être garanti par une clause contractuelle. Les relations avec les prestataires externes devraient être formalisées dans des conventions claires et précises, en application de ces principes*» [12] ;

• s'assurer du respect des règles d'identification satisfaisant le degré d'exigence de la loi du 12 juillet 1990, lorsque la relation de «face à face» est impossible [13] ;

• s'assurer que les renseignements qui sont exigés lors des ordres de transferts émis par le client sont complets et conservés afin de détecter les opérations douteuses et de s'assurer de la traçabilité des opérations ; «*La surveillance des opérations sur internet en raison de la distanciation des liens avec le client doit conduire les établissements à faire preuve d'une vigilance renforcée ; aussi apparaît-il d'autant plus nécessaire que les contrôles ne soient pas uniquement automatisés mais qu'il existe toujours des gestionnaires de compte qui centralisent toutes les informations sur les opérations effectuées sur ce compte*» [14] ;

• pouvoir bloquer, le cas échéant, la réalisation automatique de certaines opérations afin de se donner le temps d'examiner leurs caractéristiques ou d'obtenir un complément d'information ;

• élaborer dans chaque établissement une politique de sécurité internet ;

• utiliser des techniques permettant la non-répudiation pour les transactions jugées sensibles par l'établissement ;

• suivre attentivement l'évolution des textes juridiques relatifs à la signature électronique et au formalisme des contrats électroniques ainsi que la mise en place des prestataires de services de certification ;

• établir une étude juridique destinée à mesurer précisément les risques encourus s'agissant des prestations transfrontières ;

• associer les directions juridiques et les directions techniques et informatiques pour renforcer le besoin de sécurité des transactions.

S'ajoutent à ces recommandations d'autres mesures qui concernent le fonctionnement interne de l'établissement, ainsi que des recommandations relevant de la discipline de place qui dépassent le cadre de cette sensibilisation à l'influence des nouvelles technologies et à la prise en compte de la dimension éthique dans les établissements de crédit.

L'évolution de la prise en compte de la dimension éthique sur les marchés bancaires et financiers

Compte tenu du fait que les marchés financiers ont été les premiers visés par des impératifs déontologiques il est bon d'en examiner l'évolution de la dimension éthique. L'article 19 de la loi n° 88-70 du 22 janvier 1988, adoptée après les travaux du groupe Brac de la Perrière avait déjà disposé que les établissements de crédit doivent prévoir dans leur règlement intérieur «*les conditions dans lesquelles les salariés peuvent effectuer des opérations de bourse pour leur propre compte ; les conditions dans lesquelles ils doivent dès lors en informer leur employeur ; les obligations qui s'imposent à eux en vue d'éviter la circulation indue d'informations confidentielles*». Puis la loi de modernisation des activités financières (loi n° 96-597 du 2 juillet 199615) avait rendu obligatoire la nomination d'un déontologue auprès de chaque prestataire de service d'investissement.

Ce fut ensuite l'ancien article 2-2-6 du règlement général de fonctionnement du CBV (Conseil de la bourse des valeurs) qui disposait que «*chaque société de bourse désigne en son sein un responsable du contrôle rendant compte directement au directeur général de la société […]. Le responsable du contrôle veille au respect par les personnes placées sous l'autorité de la société ou agissant pour son compte de leurs obligations professionnelles et des règles de déontologie qui leur sont applicables. A ce titre, il est l'interlocuteur privilégié pour les questions d'ordre déontologique et le destinataire des informations que les règlements auxquels elles sont soumises prévoient qu'elles communiquent*».

Enfin c'est le titre III du règlement général du CMF (Conseil des marchés financiers), adopté en 1998, qui rend obligatoire la présence d'un déontologue dans toutes les entreprises qui sont prestataires de services d'investissement, hors les sociétés de gestion qui relèvent des règles de déontologie édictées par la Cob. Dans les sociétés importantes, le déontologue ne peut pas assurer d'autre mission. Dans tous les cas il «*agit de façon indépendante par rapport à l'ensemble des structures à l'égard desquelles il exerce ses missions*» [16].

Puisque les intermédiaires financiers doivent exercer leur activité «*avec diligence, loyauté, équité, dans le respect de la primauté des intérêts du client et de l'intégrité des marchés*», les intérêts que doit d'abord protéger le déontologue ne sont donc pas ceux de l'établissement mais ceux des clients, d'une part, et de la place d'autre part. C'est pourquoi une des principales responsabilités du déontologue en la matière est d'élever une véritable «Muraille de Chine» entre les diverses activités de façon à limiter le plus possible la circulation indue des informations.

C'est bien toujours dans le même esprit que, le 16 juillet 1992, la Commission bancaire avait approuvé un Code de déontologie des marchés interbancaires de gré à gré qui a été modifié en 1996 pour tenir compte des dispositions de la loi du 2 juillet 1996 relative à la modernisation des activités financières. Ce code repose sur un principe fondamental : «*les participants aux marchés ont un droit absolu à ce que les ordres qu'ils donnent et les transactions qu'ils effectuent soient connus seulement de leur(s) intermédiaire(s) et de leur(s) contrepartie(s). Dans le cas d'opérations conclues par l'intermédiaire d'un courtier, celui-ci ne doit divulguer que les informations strictement nécessaires à la réalisation d'une transaction*».

Pour permettre le développement de cette dimension éthique, le CMF attribue au déontologue trois types de mission : une mission de communication interne, un devoir de surveillance et un pouvoir de décision.

Ainsi, Françoise Bonfante qui, après avoir été chargée de l'information à la Cob, est devenue déontologue chez UBS Warburg à Paris, explique : «*ma première mission, c'est d'assurer la veille réglementaire et la pédagogie de l'entreprise. Cela représente environ la moitié de mon temps car la réglementation est en constante évolution. Ma deuxième mission consiste à fournir aide et assistance, pour des questions particulières ou pour la rédaction de nouvelles procédures. La troisième concerne les contrôles et les sanctions*» [17].

A la Société Générale, le déontologue travaille en étroite collaboration avec le service juridique, l'audit interne et l'inspection générale (notamment en ce qui concerne la lutte contre le blanchiment). Du fait de sa présence sur de nombreux marchés internationaux et de son activité financière très développée, la Société Générale a mis en place un service chargé de la déontologie très important ; elle s'efforce de respecter le ratio appliqué par les anglo-saxons d'un contrôleur pour 100 opérateurs. G. Arbillot considère que le rôle premier des déontologues est «*de minimiser tous les risques d'image tout en facilitant au maximum le travail des opérateurs*» [18].

Fin janvier 2001, le Comité de Bâle a présenté l'avant-projet des nouvelles normes en matière de fonds propres que devront bientôt respecter tous les établissements de crédit. Parmi les grandes nouveautés proposées, il y a en particulier la prise en compte des «risques opérationnels». Celle-ci aura inéluctablement une influence sur la dimension déontologique dans les banques.

La méthode de prise en compte du risque opérationnel pourra être développée selon trois approches différentes : une approche standard «simple», une approche par ligne de métiers et une approche par «mesure interne». La méthode retenue résultera de l'organisation interne et des moyens mis en œuvre ce qui supposera une décision au plus haut niveau de l'entreprise. A titre d'exemple, le rôle et la mission exacte du «déontologue», ou du «*compliance officer*», sa position dans la hiérarchie, l'étendue de ses pouvoirs, seront des éléments qui pourront influer sur la prise en compte du risque, dans le cas notamment des approches par ligne de métiers et par mesure interne. De même la gestion centralisée ou décentralisée des risques opérationnels sera prise en compte.

Du fait de leur nature et de leur nouveauté les risques opérationnels se prêtent mal aujourd'hui à une mesure purement quantitative ; ils devront faire l'objet, au moins dans un premier temps, d'une approche qualitative alors qu'aucune méthode universellement admise ne sera disponible. Cette analyse devra notamment intégrer la mesure du degré d'adéquation de l'organisation interne avec l'objectif visé ainsi qu'avec le niveau des risques acceptés par le Conseil d'administration.

Dans ce nouveau cadre, ce sera au conseil d'administration qu'il appartiendra de définir le profil de risque qu'il entendra assumer et au «*risk manager*» de faire en sorte que l'entreprise bancaire respecte, dans tous les domaines, le niveau de risque ainsi fixé. Le rôle de ce «*risk manager*» ne se confondra donc pas avec celui du «*compliance officer*», mais viendra le compléter. Si le second aura une vision plus juridique et organisationnelle de la banque, le premier devra avoir une approche plus concrète et opérationnelle («*Le risk manager est responsable de tout, y compris de la femme de ménage*»).Les deux devront cependant avoir des rapports étroits.

La «déontologie choisie» ou les codes internes

A côté de cette «déontologie régulée», la tendance est à un développement de la «déontologie choisie» qui résulte de divers codes qui, lorsqu'ils édictent des dispositions impératives, font partie intégrante du règlement intérieur et, comme tels, doivent être soumis aux règles de forme que le Code du travail impose à tout règlement intérieur. Ces codes qui ne s'arrêtent pas aux simples règles relatives aux opérations de bourse réalisées pour compte propre par les membres du personnel, ni aux opérations de lutte contre le blanchiment, peuvent aussi intégrer des domaines aussi divers qu'une charte destinée aux informaticiens ou des règles de passation des contrats pour travaux immobiliers, par exemple.

Tous doivent mettre l'accent sur tout ce qui peut faire courir un risque d'image à l'établissement, et tous doivent «*être réactualisés en permanence en fonction de l'évolution de la réglementation, des métiers, des événements qui marquent l'établissement ou les marchés*» [19].

L'importance de ces codes et chartes, qui viennent compléter les lois et les interprétations jurisprudentielles, est grande mais, en même temps, diversement appréciée selon les systèmes juridiques. Ainsi, si «*l'on considère que la responsabilité des personnes morales peut être engagée par les bénéficiaires de délégations de pouvoirs, l'impact de la mise en place de chartes d'éthique sur la responsabilité des personnes morales nous semble être pratiquement négligeable. En effet, en ce qui concerne tout d'abord les délits non intentionnels qui peuvent être constitués à la suite d'un simple accident, l'existence d'une charte ou code prohibant ce type de délit ne nous semble pas pouvoir exonérer la personne morale de sa responsabilité pénale, sauf à ce qu'il puisse être soutenu que le responsable du délit aurait agi hors de ses fonctions ou pour son propre compte sur la base des éléments figurant dans la charte d'éthique. Il en est de même en ce qui concerne les délits intentionnels. En revanche, si on se fonde sur la théorie de l'autonomie de la responsabilité des personnes morales, la mise en place de charte d'éthique pourrait avoir pour effet d'alléger la responsabilité des personnes morales. En effet, selon cette seconde théorie, la personne morale doit avoir commis une faute personnelle pour que sa responsabilité pénale puisse être engagée*» [20].

Dans notre étude relative à la place de l'éthique et des nouvelles technologies dans les établissements de crédit, nous devons maintenant faire une place particulière à la «netiquette».

On appelle ainsi les règles déontologiques applicables sur les réseaux informatiques ouverts. Mais, avant d'en examiner quelques points, commençons par rappeler le principe fondamental du rôle de l'informatique au regard du droit français : «*L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles et publiques*» [21].

Dans le détail, il faut rappeler que la loi Informatique et libertés repose sur cinq principes fondamentaux :

- **le principe de finalité :** les données personnelles ne peuvent donner lieu qu'aux traitements qui ont justifié leur collecte ;
- **le principe de proportionnalité :** les données collectées doivent être strictement limitées à celles nécessaires au traitement annoncé et au but poursuivi ;
- **le principe de loyauté :** les données personnelles ne doivent pas être collectées à l'insu des personnes concernées ni cédées à un tiers sans leur consentement ;
- **le principe de sécurité :** le responsable d'un traitement doit assurer la confidentialité de ses fichiers, les mettre à jour et corriger toute erreur dès qu'il en a connaissance ;
- **le principe du respect des droits de la personne :** toute personne fichée doit pouvoir accéder aux informations la concernant, obtenir les rectifications des informations erronées, voire exiger leur effacement.

C'est en vertu de ces principes fondamentaux que la CNIL paraît considérer que rien n'est plus attentatoire aux libertés individuelles que la conservation et l'exploitation, notamment par les banques, de données périmées conservées dans les fichiers. C'est aussi en vertu de ces mêmes principes fondamentaux que l'avant-projet de loi relatif à la société de l'information, tel qu'il a été présenté le 6 février 2001, établit un véritable droit de réponse sur internet : «*Toute personne nommée ou désignée dans un service de communication en ligne dispose d'un droit de réponse sans préjudice de toute demande de correction ou de suppression du message pendant la période au cours de laquelle le message est encore accessible au public.*»

«*La demande d'exercice du droit de réponse doit être présentée au plus tard dans un délai de huit jours suivant celui de la cessation de la mise à disposition du public du message contenant la mise en cause qui la fonde*».

Au fond, il ne s'agit que de l'application dans le domaine juridique d'une obligation de loyauté qui peut encore être illustrée par référence à la décision du tribunal de commerce de Paris en date du 25 janvier 2001. Dans cette affaire, le tribunal a condamné une société qui avait mis en place, entre son site et celui d'une autre, un lien profond. Pour cela il s'est fondé sur les dispositions de l'article L. 122-4 du Code de la propriété intellectuelle qui condamne le fait de représenter une œuvre sans le consentement de son auteur. Il a précisé que «*le bon usage des possibilités offertes par le réseau*» exige de prévenir le propriétaire du site cible. Au cas d'espèce, le lien profond masquait totalement le nom du site cible, ce qui a amené le tribunal à préciser que «*s'il est admis que l'établissement de liens hypertextes simples est censé avoir été implicitement autorisé par tout opérateur de site Web, il n'en va pas de même pour ce qui concerne les liens dits "profonds" et qui renvoient directement aux pages secondaires d'un site cible sans passer par sa page d'accueil*». En l'absence de cette autorisation du titulaire du site cible, le juge a considéré comme déloyal et parasitaire [22] l'établissement d'un hyper lien car cela a pour conséquence :

- de détourner le contenu ou l'image du site cible ;
- de faire apparaître ledit site comme étant le sien, sans mentionner la source ;
- de ne pas signaler à l'internaute, de façon claire et non équivoque, qu'il a été dirigé vers un site extérieur au premier site connecté.

Ce faisant le tribunal a ainsi proposé un véritable code de bonne conduite.

Mais ces moyens modernes de communication sont aussi utilisés au sein même des établissements pour leurs besoins internes. Or, l'intranet fait courir à chaque entreprise des risques particuliers car il peut venir bousculer les circuits hiérarchiques, favoriser les contrôles (y compris les contrôles occultes), limiter le champ de «la vie privée résiduelle» et même bousculer, voire bloquer complètement la vie de l'entreprise.

L'intranet

D'un point de vue technique, il faut d'abord insister sur un point important, celui des sauvegardes automatiques dont chacun finit par perdre conscience. Celles-ci sont automatiquement archivées, conservant ainsi en mémoire les états intermédiaires d'une réflexion ou d'une négociation. Y compris de documents qui peuvent mettre l'accent sur des questions que l'entreprise ne souhaiterait pas forcément voir citées dans un procès éventuel.

La mise en place d'un intranet doit être examinée au regard de cinq séries de textes :

– la loi relative aux fichiers, à l'informatique et aux libertés,

– le droit d'auteur,
– le droit du travail,
– la protection de la vie privée,
– et la sécurité.

En ce qui concerne la loi relative aux fichiers, à l'informatique et aux libertés il convient de commencer par signaler que tout traitement nominatif réalisé dans le cadre d'un intranet (courrier électronique, liste de diffusion, accès sélectifs...) doit faire l'objet d'une déclaration à la CNIL. Le non-respect de cette obligation rend le traitement illicite et peut donc entraîner la mise en cause de la responsabilité du chef d'entreprise : responsabilité pénale d'abord, mais aussi responsabilité civile si le traitement incriminé cause un préjudice à quelqu'un. L'absence de déclaration peut aussi avoir un autre effet gravement dommageable, celui de rendre illicite et donc inopérante l'utilisation d'informations issues de ces traitements comme mode de preuve (que ce soit au regard du commerce électronique ou du droit du travail, en particulier). Dans un arrêt de la chambre sociale de la Cour de cassation du 20 novembre 1991 a été fixé le principe suivant lequel «*si l'employeur avait le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu, constituait un mode de preuve illicite*».

Dans le prolongement de cette loi, pour les entreprises qui auraient des implantations à l'étranger et qui mettraient en place un intranet transfrontière, elles doivent respecter les règles communautaires de protection de la vie privée. Aux termes de ces dispositions, la circulation des données informatisées au sein de l'Espace européen est libre, mais elle est interdite vers les pays qui n'ont pas été reconnus par la Commission comme offrant une protection suffisante. Or, au 31 décembre 2000, la Commission européenne n'avait inscrit que deux pays sur la liste de ceux assurant cette protection suffisante : la Suisse et la Hongrie. Cependant la Commission européenne a signé un accord avec les Etats-Unis, dit *Safe Harbour Principles* ou accord «sphère de sécurité», aux termes duquel des données peuvent librement circuler entre l'Europe et les entreprises américaines qui se sont volontairement faites homologuées auprès du ministère américain du commerce comme respectant le minimum de protection. Il est possible encore de transférer des données à condition d'avoir l'accord express et éclairé de chacune des personnes qui pourraient être concernées par un tel transfert. Dernière possibilité, que l'entreprise passe une convention avec le gestionnaire du système destinataire aux termes de laquelle ce dernier s'engage à assurer le même niveau de protection.

Au regard du droit du travail c'est l'article L. 432-2 qui est le texte fondamental. En vertu de cet article : «*le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel. Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences quant aux points mentionnés ci-dessus.*

«*Lorsque l'employeur envisage de mettre en œuvre des mutations technologiques importantes et rapides, il doit établir un plan d'adaptation. Ce plan est transmis, pour information et consultation, au comité d'entreprise en même temps que les autres éléments d'information relatifs à l'introduction de nouvelles technologies. En outre, le comité d'entreprise est régulièrement informé et périodiquement consulté sur la mise en œuvre de ce plan*».

Il convient encore de se souvenir, en ce qui concerne les informations relatives aux membres du personnel, que ceux-ci disposent de tous les droits que la loi relative aux fichiers, à l'informatique et aux libertés reconnaît aux personnes fichées : droit de savoir lors de la collecte des données quelles sont les questions à caractère obligatoire et celles à caractère facultatif, droit de connaître les conséquences d'une absence de réponse, droit de savoir quels sont les destinataires des informations, droit d'accès et de rectification.

Par ailleurs l'article 29 de la loi relative aux fichiers, à l'informatique et aux libertés, impose la sécurité des traitements : «Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées, ou communiquées à des tiers non autorisés». Cette sécurité impose le respect de la confidentialité des informations transmises et le respect du secret bancaire. La seule façon de respecter ces obligations est l'usage de la cryptographie. En ce qui concerne l'usage des nouvelles technologies, la CNIL s'appuie sur cette obligation pour demander communication des contrats passés avec les hébergeurs des sites de l'entreprise.

En ce qui concerne le droit d'auteur, il convient de rappeler que toutes les créations immatérielles appartiennent à leur auteur, fut-il salarié d'une entreprise et la création réalisée pendant le temps de travail. Deux exceptions seulement : les logiciels, d'une part, et les œuvres collectives d'autre part.

Dès lors la mise en place d'un intranet devrait respecter cinq étapes :

- dépôt du nom de l'Intranet en tant que marque ;
- élaboration d'une charte, d'un guide et des procédures ;
- définition des droits de chacun (contrat écrit préalable obligatoire) ;
- déclaration à la CNIL ;
- consultation des institutions représentatives du personnel.

Il faut pour terminer sur ce sujet se poser la question de savoir comment encadrer cet usage d'un intranet. La seule façon de faire est l'élaboration d'une charte qui précise les droits de chacun (contrôle des connexions, contrôle des accès à l'entrée comme à la sortie, droit de s'inscrire sur des listes de diffusion externe, droit de se constituer ses propres listes de diffusion, droit d'adresser ou non un message à tous les collaborateurs de l'entreprise, à une catégorie d'entre eux, droit à une correspondance privée, droit au reroutage des messages personnels, droit à l'ouverture des «mels» – ou «courriels» – reçus en l'absence du salarié, participation à des forums ou à des «*papotoires*» [23], etc.). La question qui se pose alors est celle

de savoir si la charte doit être annexée au règlement intérieur (décidé par l'employeur, mais relativement rigide) ou doit rester indépendante (plus souple, mais doit être approuvée par chaque salarié avant d'entrer en application ce qui suppose la mise en place d'un «contrat-clic», c'est-à-dire l'utilisation du double clic pour reconnaître avoir pris connaissance... Rappelons ici qu'en vertu de l'article L. 122-35 du Code du travail, le règlement intérieur «*ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*». ■

Achevé de rédiger le 5 septembre 2001.

[1] «Ethique et commerce international», *CJFE/CFCE*, n° 2/2000, p. 247.
[2] «Ethique et droit des affaires», *Dalloz*, 1993, ch. p. 18.
[3] «*En 1992, le sénateur américain Harkin Bill lance un projet de loi visant à interdire l'importation, aux Etats-Unis, de produits fabriqués par les enfants […]. Si on avait écouté [les enfants bengalis], on aurait découvert qu'il s'agissait en majorité de fillettes dont le risque majeur (de leur point de vue) est l'agression sexuelle, le viol et la grossesse. Faute d'écoles procurant la protection, elles cherchent à accompagner au plus près leur mère et leurs grandes sœurs, et profiter ainsi de la protection que représentent les entreprises où elles travaillent […]. S'il fallait résumer d'un mot le message des enfants travailleurs, d'un mot choisi et répété sans cesse par les enfants eux-mêmes, ce serait celui de dignité. Reconnaissance de la dignité de chaque enfant et de chaque travailleur. Au moment où les phénomènes de mondialisation et la net-économie ébranlent nos habitudes de vie et de pensée, les enfants travailleurs nous invitent à garder le cap sur l'essentiel : la dignité de chaque être humain, participant à la marche de l'humanité, créée pour le travail et non pour la servitude*» (M. Bonnet, «Que penser du travail des enfants ?», Etudes, avril 2001).
[4] Loi n° 84-46 du 24 janvier 1984, art. 37.
[5] Rapport de la *CFB* du 30 août 2000.
[6] Obligation de résultat !
[7] Norme AFNOR 42-013.
[8] *Livre blanc* présenté le 30 janvier 2001, p. 15.
[9] *Livre blanc*, p. 90.
[10] En ce qui concerne les risques juridiques, le Livre blanc explique que les établissements de crédit «*doivent se conformer, pays par pays, aux règles relatives à l'exercice de l'activité envisagée – notamment l'obtention d'un agrément –, aux règles relatives à la capacité des clients à effectuer des opérations bancaires et financières (conditions de majorité ou de capacité juridique, conditions d'accès au type de service proposé), aux conditions de forme de la prestation de services envisagée, notamment les conditions déclaratives ou les obligations de vérification (consultation de fichiers d'incidents par exemple) à l'ouverture d'un compte, aux régimes spécifiques de protection des clients (droit de la consommation, règles applicables à l'information des investisseurs…), et notamment aux règles d'ordre public qui s'imposent aux parties, au régime fiscal, aux règles de preuve, etc.*» (*Livre blanc*, p. 74). «*Préalablement à tout exercice de son activité dans un nouveau pays ou avec des clients couverts par le droit de ce pays, l'établissement procède ou fait procéder à une étude sur le cadre des activités juridiques en ligne. Cette étude sert de base à la rédaction des conventions avec les clients, ainsi qu'à la rédaction des procédures relatives aux contrôles à l'ouverture de relations*» (*Livre blanc*, p. 98).
[11] Livre blanc, p. 94/95.
[12] Livre blanc, p. 109.
[13] Tout établissement de crédit «*doit s'assurer en particulier du caractère certain du consentement [de son client] à l'opération, même transmis de manière dématérialisée*» (*Livre blanc* p. 74). «*Dans le cas où la reconnaissance physique apparaît impossible à mettre en œuvre, les organismes financiers qui proposent des ouvertures de comptes à distance à leurs clients doivent procéder à des mesures additionnelles de vérification au nombre desquelles la production de pièces justificatives supplémentaires pour s'assurer de l'identité du client. Ces mesures additionnelles de vérification doivent permettre de connaître avec certitude l'identité du client*» (*Livre blanc*, p. 128).
[14] *Livre blanc*, p. 131.
[15] L'article 58-1° de cette loi dispose aussi que les prestataires de services d'investissement doivent «*se comporter avec loyauté et agir avec équité au mieux des intérêts de leurs clients et de l'intégrité du marché*».
[16] *Règlement CMF*, article 3-1-3.
[17] *Les Echos*, 28 novembre 2000.
[18] *Les Echos*, 28 novembre 2000.
[19] E. Coulomb, «Déontologie : les incorruptibles», *Banque* n° 555, janvier 1995, p. 66.
[20] S. Le Damany et C. Joly-Baumgartner, «Chartes d'éthique, codes de déontologie et responsabilité pénale des entreprises et de leurs dirigeants», *CJFE/CFCE*, n° 2/2000, p. 331.
[21] Article 1er de la loi n° 78/17 du 6 janvier 1978, relative à l'informatique aux fichiers et aux libertés.
[22] Le Président du tribunal a précisé que la création de tels liens hypertextes serait considérée comme une action déloyale ou parasitaire même si le site établissant les liens n'avait pas la même activité que le site cible et qu'il n'entrait donc pas en concurrence avec lui.
[23] En anglais «chat».