INTERNET ET LES RESEAUX NUMERIQUES

Collection Etudes du Conseil d'Etat

Sommaire

Synthèse

Un débat international

La philosophie générale

Les principales recommandations

Protéger les données personnelles et la vie privée

Favoriser les échanges par une confiance accrue des acteurs

Valoriser les contenus par la protection de la propriété intellectuelle

Lutter contre les contenus et comportements illicites

Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications

Conclusion

Première partie

Protéger les données personnelles et la vie privée

Un besoin nouveau de protection

Les traitements visibles

Les traitements invisibles

Conclusion

Les exemples étrangers : autorégulation et liberté de circulation de l'information

Les États de l'Union européenne

Les États hors Union européenne

Les organisations internationales

Conclusion

Les solutions nouvelles : un accord international et une nécessaire combinaison du droit et des mesures d'autorégulation

La nécessité d'un accord international

Le recours aux procédés d'autorégulation

Évolution du rôle de la CNIL

Conclusion

Deuxième partie

Favoriser les échanges par une confiance accrue des acteurs

Chapitre 1

Transactions électroniques et protection du consommateur

Assurer en France la transparence et la sécurité juridique des transactions électroniques

Lever les ambiguïtés relatives au régime de la publicité sur Internet

Clarifier la qualification juridique d'une transaction sur Internet : vente à distance avec ou sans démarchage ?

S'assurer que les consommateurs ont été bien informés et ont manifesté clairement leur consentement

Renforcer l'identification des professionnels sur Internet

Encourager les professionnels à la mise en place d'instruments garantissant un respect effectif des droits du consommateur

Mettre en place un cadre juridique international adapté aux transactions électroniques et à la protection du consommateur

L'insuffisance du cadre juridique international actuel

La nécessité d'une convention internationale relative aux transactions électroniques et à la protection du consommateur

Chapitre 2

La reconnaissance de la valeur juridique du document et de la signature électroniques

La nécessité de reconnaître la valeur juridique du documentet de la signature électroniques n'est qu'imparfaitement rendue possible par le droit civil

La prise en compte du document électronique varie en fonction des régimes de preuve et suppose de bien distinguer deux objectifs : recevabilité et force probante

Le droit civil ne permet qu'une prise en compte imparfaite du document électronique

La nécessité d'une réforme législative est largement reconnue

Reconnaître la valeur probatoire du message électronique et favoriser la mise en place d'une offre de services de certification

Reconnaître la valeur probatoire du message électronique authentifié par une signature électronique fiable

Favoriser la mise en place d'une offre de services de certification

Chapitre 3

Les enjeux de la cryptologie sur Internet

La libéralisation de la cryptologie est réelle mais encore partielle

Moyens de cryptologie assurant des fonctions de signature et d'authentification, sans fonction de confidentialité

Moyens de cryptologie assurant des fonctions de confidentialité des messages ou des fichiers

La mise en œuvre du nouveau cadre légal se heurte à certaines difficultés

Certains aménagements du cadre légal de la cryptologie pourraient être envisagés à terme

Chapitre 4

L'adaptation de la fiscalité au commerce électronique

La détermination de l'assiette est rendue difficile par la dématérialisation des transactions

Le prélèvement de la TVA face à la dématérialisation des transactions

L'impôt sur les sociétés et le problème de l'interprétation du concept d'établissement stable

Le recouvrement des impôts et taxes se heurte à de sérieuses difficultés

Les caractéristiques d'Internet rendent difficiles l'identification des transactions et le recouvrement des impôts et taxes

Évaluer la possibilité d'associer des tiers

Chapitre 5

Noms de domaine et droit des marques

Les modalités actuelles d’attribution des noms de domaine sont peu satisfaisantes pour les titulaires de marques et pour les États

Présentation du système des noms de domaine (DNS)

Les difficultés liées au développement incontrôlé des domaines génériques internationaux

Les réformes proposées par le " Comité international ad hoc " (IAHC) puis par le Gouvernement américain

Propositions pour rationaliser l’attribution des noms de domaine tout en protégeant les titulaires de marques

L’organisme de régulation du système des noms de domaine

Les bureaux d’enregistrement et la procédure d’attribution des noms de domaine

L’articulation de l’architecture des noms de domaine avec les principes du droit des marques

La détermination de la loi applicable et le règlement des litiges

L’assouplissement souhaitable de la " charte de nommage " du domaine français (" .fr ")

Troisième partie

Valoriser les contenus par la protection de la propriété intellectuelle

L’adaptation du régime de la propriété intellectuelle aux enjeux d’Internet et des réseaux numériques

L’état de la réflexion internationale

Conserver les principes fixés par la législation française en matière de propriété littéraire et artistique

Faire évoluer le régime de la titularité des droits, notamment à l’égard des auteurs salariés

Adapter, dans un cadre international, le régime des exceptions au droit d’auteur

Harmoniser les règles relatives aux conflits de lois et de juridictions, notamment en matière d’atteintes aux droits de propriété intellectuelle

La lutte contre la contrefaçon

La responsabilisation des acteurs et l’identification des œuvres

L’amélioration des procédures judiciaires

La coopération internationale

Quatrième partie

Lutter contre les contenus et comportements illicites

Préciser la loi applicable et la compétence du juge français

En matière pénale

En matière civile

Conclusion

Clarifier les responsabilités des acteurs

L'inadéquation de la responsabilité en cascade au monde des réseaux

Les enseignements de la jurisprudence et des exemples étrangers

La proposition en matière pénale

La responsabilité civile

Faciliter l'action de la police et de la justice

Renforcer l'identification des acteurs

Augmenter les pouvoirs et les compétences du juge

Adapter la procédure à la fugacité des réseaux

Créer une cellule interministérielle pour la criminalité de haute technologie

Renforcer la coopération internationale

Conclusion

Susciter et renforcer l'autorégulation des acteurs

Des initiatives internationales convergentes

Des initiatives françaises peu conclusives

La création d'un organisme de corégulation de l'Internet et des réseaux

Cinquième partie

Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications

Le phénomène de convergence ne doit pas remettre en cause la distinction entre communication

au public et correspondance privée

L'analyse du Livre vert de la Commission européenne sur le phénomène de convergence

La réalité du phénomène de convergence et son impact sur la réglementation appellent un constat nuancé

Des adaptations de la réglementation sont rendues nécessaires par la convergence technologique et le développement des services en ligne

Adapter à moyen terme la réglementation de la communication

Définir un cadre juridique pour les services en ligne

Annexes

Annexe 1

Résumé des propositions

Annexe 2

Présentation d'Internet

Annexe 3

Glossaire

Annexe 4

Composition du groupe d'étude

Annexe 5

Liste des personnes auditionnées ou consultées

Synthèse

Internet : le " réseau des réseaux ", un " nouveau média ", une " conversation mondiale sans fin " . Les qualificatifs ne manquent pas pour tenter de décrire ce phénomène majeur de la fin du XXe siècle qui bouleverse les modes de fonctionnement traditionnels des sociétés contemporaines.

Internet et les réseaux numériques, c'est avant tout un **nouvel espace** d'expression humaine, un espace international qui transcende les frontières, un espace décentralisé qu'aucun opérateur ni aucun État ne maîtrise entièrement, un espace hétérogène où chacun peut agir, s'exprimer et travailler, un espace épris de liberté.

Cet espace n'est pas naturellement celui du droit. Celui-ci, d'application territoriale, s'appuie sur des comportements, des catégories homogènes et stables, tous éléments qui font défaut dans le cas d'Internet. Cet antagonisme avec le droit aurait même, selon certains, favorisé l'essor initial

du réseau, libre de toutes contraintes hormis celles fixées par la communauté des chercheurs qui sont à l'origine de sa création.

Cette situation ne peut cependant plus perdurer. Le succès et la généralisation progressive d'Internet, qui est désormais un espace grand public et marchand reliant plus de 100 millions d'utilisateurs, conduit à s'interroger sur la fixation des règles de cet espace : qui les fixe, selon quelles modalités et avec quelle efficacité ? Les réponses ne peuvent plus seulement être celles d'un petit nombre de spécialistes. Elles doivent être discutées entre l'ensemble des acteurs publics et privés et faire l'objet d'un débat démocratique.

C'est dans ce contexte que, par une lettre du 22 septembre 1997, le Premier ministre a demandé au Conseil d'État d'analyser les questions juridiques liées au développement d'Internet et de mettre en lumière les adaptations nécessaires de notre droit.

Un débat international

Ce débat est international, et le temps de la réflexion est compté. En effet, des négociations internationales très importantes sont d'ores et déjà en cours, et pour certaines sur le point d'aboutir. Ces négociations, conduites dans une large mesure à l'initiative d'intérêts publics et privés nord-américains, risquent de structurer les usages et les comportements sur les réseaux numériques. Il sera trop tard demain pour défendre une conception différente des droits de la personne ou du consommateur. Il faut dès lors participer de façon active à ce débat mondial sous peine de le voir s'organiser selon une logique strictement économique.

Car tel est bien l'enjeu : faire en sorte que le monde qui naît sous nos yeux, porteur d'enrichissement, de croissance et d'échanges entre les peuples accompagne le dynamisme des entreprises mais dans le respect de la personne humaine. À la globalisation économique doivent correspondre des choix politiques et éthiques, illustrant le type de société, de rapports entre acteurs et finalement d'échelle de valeurs que nous souhaitons voir adoptés dans le monde virtuel. Il ne s'agit certes pas de militer pour une approche " romantique " de l'Internet autour d'un idéalisme humaniste européen, mais de prouver, une nouvelle fois, la capacité de notre Vieux Monde à imaginer celui de demain, compte tenu de sa diversité culturelle et de son attachement à la défense des droits de l'homme.

La philosophie générale

La démarche du Conseil d'État s'est voulue pragmatique, s'appuyant sur les nombreux travaux déjà réalisés sur des sujets proches et sur l'expérience concrète des professionnels qui ont été consultés. Le souci a toujours été de privilégier le conseil au Gouvernement, à la fois juridique et stratégique, sur les sujets les plus importants et les plus urgents, plutôt que de proposer un ouvrage académique et exhaustif sur les enjeux juridiques de l'Internet. Le travail s'est déroulé d'octobre 1997 à juin 1998, enrichi par les contributions tant des administrations et des acteurs français que de leurs homologues étrangers.

La philosophie générale de ce rapport pourrait être résumée dans l'objectif de **faire des réseaux numériques un espace de " civilité mondiale "**, la civilité étant " l'art de vivre bien ensemble ".

Avant d'entrer dans le détail de chacun des sujets étudiés, quatre observations générales méritent d'être soulignées.

Tout d'abord, contrairement à ce l'on entend parfois, **l'ensemble de la législation existante s'applique aux acteurs d'Internet**, notamment les règles de protection du consommateur et celles qui garantissent le respect de l'ordre public. **Il n'existe pas et il n'est nul besoin d'un**

droit spécifique de l'Internet et des réseaux : ceux-ci sont des espaces dans lesquels tout type d'activité peut être pratiqué et toutes les règles régissant un domaine particulier (publicité, fiscalité, propriété intellectuelle...) ont vocation à s'appliquer.

Les réseaux numériques transfrontières induisent une modification substantielle des modes de régulation habituels des pouvoirs publics : d'une part, **la réglementation d'origine étatique doit désormais se combiner avec l'autorégulation des acteurs**, c'est-à-dire l'intervention de ceux-ci pour décliner les principes de la règle de droit dans des environnements non prévus par celle-ci, et pour agir de façon préventive contre la commission d'infractions. D'autre part, **compte tenu des limites inhérentes à toute initiative purement nationale, la coopération internationale des États est nécessaire pour faire respecter l'intérêt public** dans un espace largement dominé par l'initiative privée. En d'autres termes, Internet et les réseaux introduisent une double interdépendance, entre acteurs publics et privés, entre États eux-mêmes, ce qui rend toute politique en la matière très complexe à élaborer et à mettre en œuvre.

Le Gouvernement doit définir des orientations stratégiques communes assurant la cohérence des positions françaises dans les diverses négociations internationales concernant Internet et les réseaux numériques (OCDE, CNUDCI, OMC, OMPI, Conseil de l'Europe...). Le dispositif actuel de coordination sur ce sujet paraît insuffisant au regard des enjeux en cause et de la multiplicité des enceintes de négociation, que ce soit pour la définition des orientations générales ou le suivi au quotidien des travaux internationaux. Il convient donc de mettre en place au plus vite une cellule interministérielle, assurée d'une forte légitimité administrative et capable de faire travailler, de concert, administrations et acteurs privés. L'objectif premier d'une telle cellule sera de promouvoir un consensus européen, indispensable pour peser véritablement sur l'issue des négociations internationales.

Enfin, le monde des réseaux étant en perpétuelle évolution, **les fonctions de veille et d'observation sont essentielles.** Aucune solution ne pouvant être énoncée une fois pour toutes, il est nécessaire, en matière juridique, de suivre l'évolution des réseaux numériques afin d'identifier les sujets de préoccupation et de formuler des réponses. Ainsi, sans qu'il soit besoin nécessairement de créer une structure permanente, des " rendez-vous " périodiques seraient utiles pour examiner la situation avec l'ensemble des acteurs concernés.

Au-delà de ces réflexions générales, cinq sujets ont fait l'objet d'une étude approfondie, compte tenu de leur importance et de leur urgence :

– la protection des données personnelles et de la vie privée sur les réseaux, qui est l'un des sujets les plus sensibles aux yeux des utilisateurs ;

– la sécurisation et l'adaptation des règles de la transaction électronique, qui conditionnent le développement du commerce et de l'initiative privée sur Internet ;

– la valorisation de la propriété intellectuelle, nécessaire à l'apparition de nouveaux contenus sur le réseau ;

– la lutte contre les contenus et les comportements illicites, afin de faire des réseaux des espaces de " civilité " ;

– l'adaptation de la réglementation de la communication et des services en ligne aux phénomènes de convergence entre l'informatique, l'audiovisuel et les télécommunications.

Les principales recommandations

Les principales conclusions des travaux du Conseil d'État dans chacun des domaines étudiés sont

les suivantes.

Protéger les données personnelles et la vie privée

La protection des données personnelles est menacée par de nouveaux risques dans l'environnement des réseaux numériques : collectes de données à l'insu de l'utilisateur, procédés de captation d'informations permettant la création de bases de données comportementales, achats ou trocs de données personnelles,... Il n'y a pas de vide juridique : le cadre légal s'applique. Néanmoins, la dimension internationale de l'Internet et l'extrême variété des pratiques des acteurs nécessitent un changement profond des modes de régulation. L'approche réglementaire doit se combiner avec les diverses pratiques d'autorégulation des acteurs et la Commission nationale de l'informatique et des libertés (CNIL) doit avoir pour nouvelle mission d'assurer le suivi de celles-ci : information et conseil sur les dispositifs techniques, labellisation des codes de déontologie et de conduite, des contrats... **C'est ce partage des missions d'encadrement entre acteurs publics et privés qui garantira une protection efficace et légitime.**

En outre, il importe de trouver un équilibre entre la préservation de l'anonymat des individus sur les réseaux et la nécessité de pouvoir retrouver leur identité lorsqu'ils commettent des infractions. Des obligations de conservation des données de connexion doivent dès lors être imposées aux intermédiaires techniques afin de faciliter les enquêtes judiciaires par une meilleure " traçabilité " des utilisateurs des réseaux.

Enfin, il est nécessaire de **définir au plan international des principes minimaux communs** qui pourraient faire l'objet d'une convention internationale. L'opportunité de négocier celle-ci est offerte aujourd'hui à l'occasion de la transposition de la directive du 24 octobre 1995 relative aux données personnelles et notamment son article 25 qui exige un " niveau de protection adéquat " pour les transferts de données personnelles à destination des pays tiers.

Au-delà des seuls traitements de données personnelles, il apparaît que les pratiques ou contenus des réseaux sont de nature à mettre en question la notion même d'identité : faut-il reconnaître l'existence d'une personne virtuelle dotée de droits distincts de ceux de la personne physique ? La réflexion, juste esquissée dans le cadre du groupe de travail, devrait se poursuivre et être élargie à des apports philosophiques, sociologiques ou politiques.

Favoriser les échanges par une confiance accrue des acteurs

Le commerce électronique sur Internet, dont les volumes sont aujourd'hui encore modestes, de l'ordre de six milliards de francs pour l'Europe en 1997, rencontre un succès croissant auprès des consommateurs. Ceux-ci ont en effet la possibilité de mettre en concurrence des vendeurs répartis sur l'ensemble de la planète. Cette nouvelle forme de commerce demeure néanmoins largement dominée par les transactions inter-entreprises. Elle reste en outre marginale par rapport aux ventes à distance faites par les procédés classiques (téléphone et minitel). Le commerce électronique ne connaîtra un véritable essor auprès des particuliers que si le cadre juridique des transactions électroniques est clarifié et adapté, afin de renforcer la confiance des consommateurs.

La première priorité consiste à assurer un **cadre juridique sécurisant pour les consommateurs**, offrant un niveau de protection comparable à celui des ventes à distance " classiques " en Europe.

Dans l'ensemble, le dispositif actuel de protection du consommateur est applicable à l'Internet. En France, cependant, des ambiguïtés doivent être levées concernant le régime juridique de la publicité et la nature de la transaction électronique (vente à distance avec ou sans opération de démarchage). Des adaptations du cadre juridique sont en outre nécessaires pour clarifier le champ d'application de certaines législations spécifiques, notamment la publicité sur l'alcool et

l'obligation d'emploi de la langue française, pour mieux identifier les parties, et pour assurer une information transparente des consommateurs, qui doivent être mis à même de manifester clairement leur consentement. Il apparaît enfin indispensable d'associer les professionnels à l'évolution de ces règles et de favoriser la mise en place rapide de codes de déontologie et de contrats types.

Au plan international, deux approches doivent par ailleurs être combinées. La première orientation consiste à définir un socle minimal de principes fondamentaux pour la protection du consommateur que pourraient partager tous les pays. Les transactions sur Internet s'effectueront pour partie avec des commerçants non européens, d'où la nécessité de négocier une convention internationale relative aux transactions électroniques, s'inspirant des principes retenus par la directive européenne du 20 mai 1997 sur les ventes à distance. La seconde orientation concerne l'adaptation des règles de conflit de lois relatives à une transaction électronique. Il est probable que le droit applicable aux transactions commerciales relèvera encore largement d'une base nationale dans les années à venir. Il importe dès lors d'adapter les règles de conflit de lois existantes, notamment celles résultant de la convention de Rome du 19 juin 1980, qui sont très favorables au vendeur. Il faudra tenir compte de la destination des messages, par le jeu d'un faisceau d'indices, afin de préserver un juste équilibre entre l'impératif de protection des consommateurs et la nécessité de ne pas imposer de contraintes irréalistes aux entreprises.

Tout aussi importante est la reconnaissance de la valeur juridique des outils d'une transaction dans le monde virtuel d'Internet. **La signature et le message électroniques** doivent d'abord assurer avec certitude l'identification des signataires et l'authentification du message. Ils doivent en outre pouvoir, au même titre que l'écrit ou la signature manuscrits, constituer la preuve d'une transaction en cas de contestation. Il est proposé, à cette fin, de reconnaître dans le code civil la valeur probatoire d'un message électronique répondant à deux exigences : authentification par une signature électronique fiable et conservation durable du message sous le contrôle du signataire. La certification du message par un organisme dûment accrédité pourrait même faire présumer que ces deux exigences légales sont satisfaites. Il faut donc favoriser la mise en place rapide d'une offre de services de certification, profession dont l'exercice doit demeurer libre, et définir les modalités de l'accréditation facultative des organismes de certification. Une fois ces principes acquis en France et dans l'Union européenne, il conviendra d'instaurer un principe de reconnaissance mutuelle des services de certification au plan international.

La confidentialité des échanges, assurée par le chiffrement des messages, est également essentielle pour rassurer les acteurs. Le cadre légal de la cryptologie doit s'efforcer de trouver un juste équilibre entre les besoins des acteurs et les préoccupations de sécurité publique. Ceci suppose une **libéralisation des instruments de cryptologie**, mais aussi la mise en place d'un dispositif de recouvrement des clés de chiffrement adéquat et, si possible, harmonisé au plan international. L'accueil réservé au nouveau dispositif légal issu de la loi du 26 juillet 1996 et de ses décrets d'application et la nécessité d'évaluer le nouveau dispositif ont conduit le Gouvernement à annoncer une vaste consultation sur ce sujet à la fin de l'année 1998, notamment en ce qui concerne le système des " tiers de séquestre ", organismes agréés chargés de conserver les clés de chiffrement des messages cryptés. Certains assouplissements de la réglementation pourraient être envisagés, visant notamment à permettre à des organismes professionnels, à des fournisseurs d'accès et à des administrateurs de réseau de jouer le rôle de " tiers de séquestre ". À plus long terme, le maintien du système des " tiers de séquestre " ne sera cependant possible que si d'autres États, notamment au sein de l'Union européenne, retiennent un dispositif analogue. Un dispositif de recouvrement des clés de chiffrement devra, en tout état de cause, être maintenu.

La fiscalité est au carrefour de divers intérêts : la souveraineté des États, la compétitivité des

acteurs et la sécurité du consommateur. Sans pouvoir procéder dans les délais impartis pour la remise de ce rapport à l'étude approfondie que nécessite l'examen complet de cette question, il apparaît d'ores et déjà que **des adaptations importantes des règles fiscales seront requises.** C'est en particulier le cas pour la TVA, dont le prélèvement est très affecté par le développement de transactions portant sur des biens immatériels ou " dématérialisés ". Des indications sont données sur les principales voies à explorer en vue d'adapter la fiscalité au commerce électronique : qualification juridique des biens " dématérialisés " ; harmonisation des règles de territorialité pour la TVA en retenant le lieu de consommation du service pour la taxation des services offerts par un prestataire établi à l'extérieur de l'Union européenne ; clarification du concept d'établissement stable, et évaluation des possibilités d'associer des intermédiaires au recouvrement des impôts et taxes ou au moins à l'identification des parties.

Enfin, **l'architecture des noms de domaine**, véritable " colonne vertébrale " de l'Internet, qui permet d'identifier les sites, doit être améliorée dans le cadre d'une réflexion internationale en veillant à une **meilleure articulation avec le droit des marques**. Il importe en particulier de veiller à ce que le futur organisme de régulation du système des noms de domaine bénéficie d'un " mandat " international, qui fixerait les principes généraux applicables aux noms de domaine. Il est urgent, sur ce point, que l'Union européenne réagisse aux propositions formulées unilatéralement par le Gouvernement américain dans son *Livre blanc*. Quant aux modalités d'organisation du système des noms de domaine, on peut notamment suggérer la création d'une vingtaine de domaines génériques (gTLD) correspondant aux principaux secteurs de l'activité économique afin de faciliter la coexistence de marques homonymes. Il paraît impératif de prévoir, en cas de litige relatif à une marque, un mécanisme de médiation et d'arbitrage, qui soit obligatoire pour le titulaire du nom de domaine et dont la sentence s'impose au bureau d'enregistrement. Enfin, en ce qui concerne le domaine français (" .fr "), un assouplissement de la " charte de nommage " paraît indispensable pour restaurer l'attractivité du " .fr " auprès des entreprises françaises.

Valoriser les contenus par la protection de la propriété intellectuelle

Le régime juridique actuel de la propriété intellectuelle (*i.e*. littéraire et artistique, et industrielle) ne paraît pas devoir être remis en cause par le développement des réseaux. Quatre problèmes doivent toutefois être résolus. Les deux premiers sont communs à l'ensemble de la propriété intellectuelle, alors que les deux autres sont spécifiques à la propriété littéraire et artistique.

Le problème le plus aigu est celui de la **contrefaçon** : il appartient aux titulaires de droits de mettre en œuvre des moyens communs pour y remédier, avec l'appui des pouvoirs publics. En matière littéraire et artistique, les mécanismes techniques de protection et d'identification des œuvres devraient sensiblement restreindre la contrefaçon. Il conviendra également d'inciter, notamment par le jeu de la responsabilité civile et pénale, les fournisseurs d'accès et d'hébergement à bloquer préventivement l'accès aux contenus contrefaisants lorsqu'ils sont saisis à cet effet par les titulaires de droits. Enfin, l'amélioration des procédures judiciaires d'urgence et d'exequatur permettra de compléter la protection des titulaires de droits.

La deuxième difficulté est celle de la **détermination de la loi applicable et du tribunal compétent** en cas d'atteinte à un droit de propriété intellectuelle (notamment en cas de contrefaçon). Il est proposé de retenir la solution vers laquelle s'oriente la jurisprudence actuellement, c'est-à-dire la loi et le tribunal du (ou des) pays de réception, pour la part du préjudice subi dans chacun d'entre eux. Cependant, pour éviter la multiplication des procès, il faudrait donner au titulaire de droits lésé la faculté de saisir un tribunal, autre que celui du lieu du pays d'émission, qui serait reconnu compétent pour réparer l'intégralité du préjudice subi au plan mondial (ou, à tout le moins, européen). Serait compétent le tribunal qui présente le lien le plus étroit avec le préjudice, en présumant qu'il s'agit de celui dans lequel la victime a sa résidence

habituelle. Ce tribunal devrait néanmoins faire une application distributive des lois des différents pays de réception pour la part du préjudice subi dans chacun d'entre eux.

En troisième lieu, des adaptations apparaissent nécessaires en ce qui concerne les **exceptions au droit d'auteur** et tout particulièrement la copie privée : le principe légal selon lequel celle-ci est présumée autorisée pourrait être conservé, tout en permettant aux titulaires de droits de l'interdire par une mention expresse sur leur site. Les titulaires de droits seraient néanmoins incités à ne pas s'opposer à la copie privée, car ils bénéficieraient du mécanisme légal de " rémunération pour copie privée ". Celle-ci serait financée par la redevance existante, qui serait étendue à tous les supports d'enregistrement. Un mécanisme analogue pourrait être envisagé concernant les " copies techniques " faites par les fournisseurs d'accès sur leurs serveurs informatiques.

Enfin, une **réflexion sur les droits d'auteur de l'employeur** sur les œuvres de ses salariés paraît s'imposer, compte tenu notamment de l'essor des œuvres " multimédia " sur l'Internet. Au-delà des aménagements à apporter à la législation, il faudra réfléchir à la définition même de l'auteur, notamment dans le cadre salarié.

De manière plus générale, les propositions en matière de propriété littéraire et artistique visent à trouver un équilibre entre les aspirations légitimes des auteurs, dont les droits doivent être préservés dans l'environnement des réseaux, l'intérêt économique des entreprises, notamment à l'égard de leurs auteurs salariés, et enfin la préoccupation tout aussi justifiée de ceux qui veulent maintenir une certaine liberté d'accès à la culture et à l'information, et qui souhaitent tirer parti des potentialités offertes par l'Internet à cet égard.

Lutter contre les contenus et comportements illicites

La lutte contre les " déviations " du cyberespace est indispensable pour en faire un espace de civilité ouvert et accueillant. Elle nécessite de veiller au respect des règles de droit, contrôlées *a posteriori* par le juge, et de développer des mécanismes d'autorégulation par les acteurs eux-mêmes, destinés à assurer une certaine autodiscipline sur les réseaux numériques.

Il faut tout d'abord **déterminer la loi applicable et le tribunal compétent** : en matière pénale, les règles sont claires et permettent d'appliquer la loi française dans la plupart des cas. En matière civile, il convient de s'en tenir pour l'instant aux règles du droit international privé existantes même si les risques de plurilocalisation des conflits et donc les difficultés de mise en œuvre des solutions jurisprudentielles sont accrus.

Les **responsabilités des acteurs** devraient en outre être clarifiées : la responsabilité pénale " en cascade " serait limitée à l'activité éditoriale (édition de contenus), les autres fonctions et notamment celles d'intermédiation technique, relevant du droit commun. En matière civile, le juge devrait raisonner au cas par cas, en faisant une distinction entre les professionnels et les autres. Pour les premiers, un devoir de vigilance semble devoir être retenu.

Enfin, **l'action de la police et de la justice** devra être facilitée afin de s'assurer de l'application effective des règles de droit. Pour cela, un renforcement de l'identification des acteurs est nécessaire et justifie de mentionner des informations minimales sur le site et d'obliger les fournisseurs d'accès à conserver les données de connexion et à les communiquer, comme l'identification de leurs abonnés, en tant que de besoin, aux autorités de police.

En outre, le juge pourra désormais interdire l'accès ou l'hébergement d'un site, prononcer pour les infractions les plus graves des peines complémentaires comme l'interdiction d'avoir une page personnelle, ordonner la publication en ligne des décisions de justice... Une adaptation de la prescription de courte durée prévue par la loi de 1881 sur la presse pourra de surcroît être

envisagée afin de faciliter les incriminations. Il ne paraît pas souhaitable de spécialiser des magistrats ou des tribunaux pour les affaires concernant Internet. En revanche, il est indispensable de consentir un effort substantiel en termes de formation et de moyens pour permettre aux tribunaux de traiter ces affaires. À ce titre, la création d'une cellule interministérielle compétente pour la criminalité de haute technologie serait utile : cette cellule constituerait un pôle d'expertise de haut niveau commun à tous les services concernés et animerait en outre des échanges d'informations sur l'ensemble de ces questions.

Sur le plan international, il apparaît souhaitable de renforcer les échanges d'information dans le cadre d'Interpol et d'Europol. La coopération judiciaire doit être allégée et des formes spécifiques aux réseaux probablement imaginées. Dès à présent, la transmission de commissions rogatoires directement de juge à juge devrait être la règle au sein des États membres du Conseil de l'Europe. Il apparaît cependant que les progrès des discussions internationales sont lents et que les réticences des États demeurent grandes face à tout ce qu'ils identifient comme des abandons de souveraineté. Il faut donc qu'une volonté politique fasse progresser rapidement cette coopération, notamment en Europe, sous peine de rendre inefficace sur les réseaux l'arsenal répressif dont disposent aujourd'hui les États.

Enfin, la France doit développer son expérience en matière d'**autorégulation**. Celle-ci ne remplace pas le droit mais se combine avec la régulation étatique pour la mettre en œuvre dans des environnements non prévus par celle-ci. La création d'un organisme de corégulation d'Internet, de droit privé, rassemblant l'ensemble des acteurs concernés, serait un moyen de réfléchir aux nouveaux procédés d'autorégulation, de définir des positions communes et de mettre en place des solutions efficaces reposant sur un large consensus.

Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications

Internet est souvent présenté comme l'archétype d'un phénomène nouveau : la convergence entre les mondes jusqu'alors séparés des réseaux informatiques, de l'audiovisuel et des télécommunications. Internet n'est, en effet, ni un réseau à proprement parler, ni un service : il est accessible par tous les réseaux et offre l'accès à des services et des contenus transnationaux d'une grande variété.

Jusqu'à une période récente, chaque type de réseau était exclusivement ou principalement dédié à un service : par exemple, le câble aux services audiovisuels, le réseau téléphonique à la téléphonie vocale et du minitel, etc. Désormais, sous l'effet des phénomènes de convergence technologique, les réseaux ne sont plus dédiés à des services particuliers et permettent de véhiculer tous types de contenus et de services (programmes audiovisuels, téléphonie vocale, services commerciaux interactifs,...). Dès lors, la distinction traditionnelle entre d'un côté la régulation des services et des réseaux audiovisuels et, de l'autre, la régulation des services et des réseaux de télécommunications perd sa pertinence. **Une distinction nouvelle doit désormais être opérée entre deux types de réglementations : celle des réseaux de télécommunication et celle des contenus et des services.**

Les réseaux de télécommunication, qui sont de simples infrastructures de transport, devront être régis par une réglementation transversale, indépendante des contenus véhiculés (sauf pour les fréquences hertziennes qui demeurent une ressource rare).

Le régime juridique des contenus et des services devra également évoluer. Il ne devra plus dépendre des réseaux empruntés, mais uniquement de l'objet du service.

Les services déjà existants doivent continuer à se voir appliquer les différentes législations sectorielles les concernant, dont certaines devront d'ailleurs être adaptées. Il faudra en particulier veiller à ce que des services équivalents ou substituables soient soumis à des contraintes réglementaires comparables, afin d'éviter toute distorsion de concurrence entre eux : par exemple, la téléphonie vocale ne doit plus être traitée différemment selon qu'elle est offerte sur le réseau téléphonique classique ou via Internet. Pour les services nouveaux, spécifiques à Internet, tels que forums de discussion et messagerie électronique, on pourrait instituer certaines règles, en vue notamment de responsabiliser les fournisseurs de ces services.

Par ailleurs, **l'ensemble des services doivent respecter la distinction fondamentale entre la " communication audiovisuelle " et la " correspondance privée "**. Celle-ci n'est en effet pas remise en cause par l'émergence des services " mixtes " : ceux-ci, par exemple les services de vente à distance, relèvent à la fois de la " communication audiovisuelle " (publicité et catalogue en ligne) et de la " correspondance privée " (prise de commande). Il est tout à fait possible, dans ce cas, de faire une application combinée des deux législations (loi sur la communication audiovisuelle et code des postes et télécommunications). Il serait néanmoins opportun de remplacer, dans la loi, le concept de " communication audiovisuelle " par celui plus explicite de " communication au public ".

Enfin, il faudra prévoir **un socle minimal de principes communs à tous les services de communication au public**, en particulier : la protection des mineurs, le respect de la dignité humaine, de la vie privée et des données personnelles, le respect de la propriété intellectuelle, et l'identification de la publicité comme telle.

Conclusion

À l'issue de cette analyse, il apparaît que les questions juridiques suscitées par le développement d'Internet et des réseaux numériques ne sont pas de nature à remettre en cause les fondements mêmes de notre droit. Au contraire, elles confirment la pertinence de la plupart des concepts généraux, parfaitement transposables à ce nouvel environnement, même si certaines adaptations sont nécessaires.

Certains sujets ont été identifiés mais nécessitent des études complémentaires. Il s'agit de la fiscalité, de la réflexion sur la notion d'auteur ou sur les droits de la personne virtuelle, des conséquences réglementaires de la convergence et notamment des mécanismes de soutien aux industries de programmes. Ces travaux doivent approfondir notre connaissance d'Internet et des réseaux numériques et aider à la mise en place d'un espace de " civilité mondiale ".

Cet objectif constitue l'enjeu majeur de ce monde en construction. Il implique un bouleversement profond de nos modes de réflexion et de fonctionnement : à une approche centralisée et verticale doivent se substituer des orientations transversales et décentralisées. Plus encore, cet objectif nécessite une coopération sans précédent entre les États et les acteurs privés, au plan national comme au plan international.

Le droit, instrument privilégié de la construction de ce nouvel espace, doit prendre acte de la complexité de cet environnement et adapter ses modes d'élaboration et d'application. Le rôle de l'État doit lui aussi évoluer, passant de celui de gardien de l'application d'une réglementation territoriale à celui de garant de l'intérêt général et d'un équilibre " acceptable " entre acteurs, dans un environnement largement dominé par l'initiative privée.

Protéger les données personnelles et la vie privée

Le concept de vie privée s'est développé vers la fin du XIXe siècle.

La Déclaration universelle des droits de l'homme du 10 décembre 1948 dispose en son article 12 : " Nul ne fera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteinte à son honneur ou à sa réputation. "

De même, la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950, affirme, en son article 8, le droit au respect de la vie privée et familiale, du domicile et de la correspondance.

Dans le droit interne français, la loi 70-643 du 17 juillet 1970 a introduit dans le code civil un article 9 dont le premier alinéa est rédigé ainsi : " Chacun a droit au respect de sa vie privée. " Solidement établi par les textes mais jamais défini, le respect de la vie privée a fait l'objet d'une abondante jurisprudence qui a précisé et élargi le contenu de cette notion : le Conseil constitutionnel lui a ainsi reconnu une valeur constitutionnelle par son rattachement au principe de la liberté individuelle, qui est une liberté constitutionnellement garantie (DC 94-352).

Les données personnelles apparaissent comme une partie de ce principe qui englobe tout ce qui se rattache à l'identité personnelle, familiale d'une personne ainsi qu'à son image.

Les réseaux sont-ils de nature à mettre en péril cette vie privée ?

Il apparaît que certaines pratiques des réseaux et notamment celles visant à la constitution de bases de données comportementales, suscitent des craintes de la part des utilisateurs. C'est d'ailleurs la raison principale, comme le montrent tous les sondages, de leurs réticences à l'égard d'Internet.

Au-delà de cette réaction un peu émotionnelle, il est clair que des questions éthiques voire philosophiques qu'avait déjà suscitées l'outil informatique prennent une actualité nouvelle avec les réseaux numériques : les données personnelles sont-elles des biens commercialisables à l'image des biens de consommation ? Quelles garanties l'individu doit-il établir dans ce monde virtuel, à l'image de ses droits et libertés réelles ? Qui peut avoir accès à ces données... ? Les réponses à ces interrogations complexes ne peuvent se faire de façon univoque : elles doivent associer acteurs publics et privés, droit et solutions techniques, sur un plan national et international.

La France, pionnière en matière de données personnelles avec la loi du 6 janvier 1978, doit participer à ce débat en offrant des solutions originales ; son expérience et sa tradition humaniste légitiment son intervention mais elle doit aussi adapter sa " culture " et ses moyens d'intervention. Les propositions qui seront faites en ce sens se fondent sur l'analyse faite par le rapport de M. Guy Braibant du 3 mars 1998 (" Données personnelles et société de l'information ").

Un besoin nouveau de protection

La France a, dès le milieu des années soixante-dix, réalisé les risques que l'informatique faisait peser sur les données personnelles et plus généralement sur les libertés de la personne humaine et a réagi en adoptant la loi du 6 janvier 1978 dite " Informatique et Libertés ". Des travaux internationaux ont par la suite été entrepris, dans le cadre de l'OCDE par l'adoption des lignes

directrices pour la protection des données en 1980, par le Conseil de l'Europe à travers la convention 108 du 28 janvier 1981 et par les Nations unies en 1990. Comme le souligne le rapport de M. Braibant, " il s'agit là de la première étape, celle de la macro-informatique ; la deuxième, ouverte il y a une quinzaine d'années est celle de la micro et de la directive européenne de 1995 ; la troisième vient de commencer : c'est celle des réseaux mondiaux et d'Internet ".

Ce dispositif textuel français s'applique à l'Internet et aux réseaux dans le cas d'un " élément de traitement " réalisé sur le territoire : la Commission nationale de l'informatique et des libertés (CNIL) l'a proclamé dès qu'elle a été appelée à connaître de cas touchant Internet et la plupart des autorités chargées de la protection des données personnelles dans les autres pays de l'Union européenne ont adopté la même position. Il apparaît donc, à l'image de nombreux autres domaines, qu'Internet n'a pas fait naître un quelconque " vide juridique " même si des compléments doivent être apportés à l'occasion de la transposition en droit interne de la directive européenne du 24 octobre 1995 relative aux données personnelles.

En effet, les réseaux par rapport à la situation que la loi de 1978 avait voulu maîtriser et que le développement de la micro-informatique avait déjà transformée, apportent un enrichissement formidable des possibilités de faire et de mal faire, grâce notamment à l'interactivité, et surtout à la possibilité d'une circulation internationale des informations.

Deux nouveaux types d'atteintes apparaissent selon les différents services proposés à l'utilisateur : soit des renseignements collectés sur les individus à travers des traitements " visibles ", soit une collecte d'informations réalisée à l'insu de ceux-ci.

L'enjeu est aujourd'hui particulièrement préoccupant du fait du développement du commerce électronique qui se fonde notamment sur un " marché " des données personnelles : celles-ci sont en effet des outils formidables de marketing permettant au commerçant de fidéliser son client en lui proposant un service " sur mesure " déduit de l'analyse de son comportement sur le réseau. Or un client fidélisé coûte cinq fois moins cher qu'un nouveau client à trouver ! Les données sont réunies en bases de données exploitées par des techniques nouvelles d'investigation (programmes intelligents de type " data mining ") et sont à la base de la technologie " push " . Faire commerce des données personnelles devient donc une activité lucrative, soit en tant que telle en vendant ces données à des tiers, soit en en faisant un élément de différenciation commerciale, attractif pour le client.

Les traitements visibles

Divers éléments d'information sur les utilisateurs sont recueillis en clair sur le réseau ; il s'agit soit des pratiques observées dans les forums de discussion, soit de l'exploitation des messages électroniques, soit des annuaires.

Les forums

Il convient à titre préliminaire de relever que la contribution à des espaces de discussion mis en œuvre par des sites Web ou sur le réseau Usenet (" newsgroups " ou " chats ") est volontaire et porte le plus souvent sur des thèmes déterminés.

Il ne semble pas que les tribunaux judiciaires français aient à ce jour eu à connaître de litiges portant sur la collecte et l'utilisation commerciale des données personnelles traitées dans le cadre de ces espaces, la CNIL ayant, pour sa part, été saisie de peu de plaintes à ce sujet.

Différents procédés de captation des informations traitées sont possibles : il peut s'agir de logiciels de recherche d'adresses électroniques, qui peuvent même opérer à l'insu des personnes,

destinés à alimenter des bases de données commerciales ; de moteurs de recherche tels que " DejaNews ", qui indexent l'ensemble des informations figurant dans les " newsgroups " et permettent ainsi à quiconque d'obtenir l'adresse électronique et l'ensemble des sujets auxquels une personne inscrite dans la base a contribué. Dejanews permet de retrouver un message datant de plusieurs années alors que ces messages sont normalement émis dans une perspective éphémère.

Dans le cadre d'une déclaration ordinaire relative à un site comportant un espace de discussion, la CNIL a recommandé, d'une part, qu'une mention informe les personnes accédant à cet espace de l'interdiction d'utiliser les informations accessibles pour d'autres finalités que celles qui ont justifié la diffusion et notamment pour enrichir des bases de données commerciales (rapport d'activité pour 1996, p. 92), d'autre part, que les utilisateurs de ces espaces soient clairement informés que leurs coordonnées et leurs contributions peuvent être captées à partir de quelque endroit du monde que ce soit. Il s'est donc agi pour la CNIL :

– d'appliquer le principe de finalité aux espaces de discussion (en particulier l'interdiction d'utilisation commerciale des données accessibles) ;

– d'informer les utilisateurs des risques de captation (principe d'autoresponsabilité).

Cette prise de position est cependant sans effet sur les forums accessibles de France mais localisés à l'étranger qui représentent l'essentiel aujourd'hui de cette nouvelle activité de communication.

La responsabilité des espaces de discussion mis en œuvre dans le cadre de sites Web pèse sur le responsable du site, qu'il s'agisse de l'application des règles de protection des données personnelles, de la conformité des espaces de discussion et des contributions aux règles d'ordre public ou à la ligne éditoriale fixée, le cas échéant, par le responsable du site.

La CNIL et ses homologues européennes recommandent de manière générale que les personnes puissent visiter un site Internet ou participer à un espace de discussion sans avoir à s'identifier (voir communication de la CNIL sur le commerce électronique du 24 octobre 1997).

Il ne s'agit bien évidemment pas pour la Commission de préconiser un usage des espaces de discussion qui conduise à ce que le réseau des réseaux devienne le sanctuaire de la délinquance et du crime organisé (rapport d'activité pour 1996 p. 66) ; il convient au demeurant d'observer que l'identité déclarée par les personnes peut être tout à fait fantaisiste ou usurpée, *a fortiori* lorsqu'elles se prêtent à des activités délictueuses ou criminelles. Dans le souci que la préconisation de l'anonymat ne puisse favoriser les abus, la CNIL a admis qu'un modérateur (animateur de site) puisse intervenir préalablement à la diffusion sur Internet d'une contribution manifestement illicite ou portée sous une identité manifestement usurpée ou encore contraire à la ligne éditoriale du site.

Elle s'est notamment prononcée en ce sens lors de l'examen de plusieurs demandes d'avis dont elle était saisie en 1997, relatives aux sites Internet du Premier ministre (avis no 97-009 du 4 février 1997) et aux sites ministériels (avis no 97-032 du 6 mai), la question se posant de savoir si la fonction du modérateur suffit à prévenir les risques d'atteinte à l'ordre public.

Cependant, là encore, ces recommandations pour utiles qu'elles soient, ne concernent que les forums " modérés " qui ne sont qu'une petite partie de cette activité sur le réseau. La plupart d'entre-eux sont au contraire gérés de façon automatique et les messages dupliqués sur l'ensemble des serveurs de la planète hébergeant lesdits forums.

La messagerie électronique

Les transferts de données personnelles par voie de courrier électronique soulèvent deux questions : le respect du secret des correspondance et la sécurité des traitements.

? *Le secret des correspondances*

Il importe en effet de préciser dans un environnement dérèglementé, avec une multitude d'opérateurs, comment est assuré le principe fondamental du droit des postes et télécommunications qui est celui du secret des correspondances. La question est simple : qui peut avoir accès aux messages envoyés par un utilisateur ?

La loi no 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications dispose : " Le secret des correspondances émises par voie de télécommunications est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci. "

Une télécommunication est elle-même définie (article 32 du code des postes et télécommunications) comme " toute transmission, émission ou réception de signes, signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil optique, radioélectricité ou autres systèmes électromagnétiques ".

Cette rédaction extrêmement générale rend le champ d'application de la loi de 1991 très large et il englobe sans nul doute les messages électroniques sous réserve qu'ils aient un caractère privé ; les messages mis à disposition du public relèvent en effet de la loi sur l'audiovisuel du 30 septembre 1986 et non de la réglementation des télécommunications.

La difficulté réside évidemment dans l'analyse des différents services offerts qui apparaissent souvent de nature mixte entre la correspondance privée et la communication audiovisuelle (voir *infra* cinquième partie).

Cependant, malgré ces incertitudes sur le caractère public ou privé des services Internet, le principe du secret des correspondances pour les messages électroniques est clair et donc la protection, par ce biais, des données personnelles qui pourraient y figurer. Il ne peut donc être porté atteinte à cette confidentialité que dans le cadre légal fixé par la loi de 1991 sur les interceptions administratives ou judiciaires.

Quelles sont les conséquences de cette obligation de respect du secret des correspondances sur le réseau ?

Le secret des correspondances doit tout d'abord être respecté par les fournisseurs d'accès eux-mêmes en tant que fournisseur d'un service de télécommunications (article L 32-3 du CPT). La plupart des acteurs le reconnaissent et le code de déontologie de l'AFA (Association des fournisseurs d'accès à des services en ligne et à Internet) d'avril 1998 en témoigne : " Les membres de l'AFA respectent le secret de la correspondance privée. Les courriers sont habituellement effacés par les serveurs sur lesquels ils sont enregistrés avant livraison à l'ordinateur de l'utilisateur, dès réception par ce dernier ou après un temps déterminé. " Dans la pratique, il apparaît que les courriers électroniques sont gardés entre un à deux jours après réception par l'utilisateur.

Le code ajoute : " Les membres de l'AFA s'interdisent de communiquer les informations nominatives concernant leurs utilisateurs en dehors des cas autorisés par la loi. "

Une affaire récente aux États-Unis a illustré les risques liés au dévoilement intempestif de ce type de renseignements par un fournisseur d'accès : celui-ci, sollicité de manière informelle par

le Département de la Défense, a spontanément communiqué des informations sur les messages d'un utilisateur appartenant au ministère de la Défense et soupçonné par ses chefs d'être homosexuel.

En conclusion, le secret des correspondances garantit à l'utilisateur que ses données personnelles y figurant seront protégées au même titre que le courrier postal.

? *La sécurité des traitements*

L'autre aspect de la vie privée dans les messages électroniques concerne la sécurité de ces données lorsqu'elles circulent sur le réseau et la crainte qu'elles ne soient altérées ou piratées par des tiers. L'article 29 de la loi du 6 janvier 1978, les articles 16 et 17 de la directive 95/46 du 24 octobre 1995 font peser une obligation de confidentialité et de sécurité des traitements de données personnelles sur le responsable du fichier, c'est-à-dire en l'espèce sur l'expéditeur du message.

L'articles 4.1 de la directive du 15 décembre 1997 concernant le traitement des données personnelles et la protection de la vie privée dans le secteur des télécommunications, pour sa part, fait obligation aux prestataires de services de télécommunications et au fournisseur du réseau public de télécommunications, de prendre toutes mesures d'ordre technique et organisationnel appropriées afin de garantir respectivement la sécurité des services et du réseau. L'article 4.2 précise que le prestataire d'un service de télécommunications accessible au public doit informer les abonnés des risques particuliers de violation de la sécurité du réseau qui pourraient exister et des moyens d'y remédier.

En tout état de cause, la garantie de la sécurité des traitements de données personnelles véhiculées par la voie du courrier électronique est essentiellement d'ordre technique : c'est le chiffrement des données qui circulent sur le réseau.

À cet égard, la libéralisation du régime français de la cryptologie intervenue dans le cadre de la loi du 26 juillet 1996 sur la réglementation des télécommunications et de ses décrets d'application permet une utilisation plus large de ces techniques et donc un renforcement des garanties offertes à l'utilisateur, notamment l'assurance de l'intégrité du message transmis et de sa confidentialité. Une expertise plus complète du dispositif français est faite dans la deuxième partie du rapport relative au commerce électronique.

Concernant les messages électroniques, il apparaît donc que le dispositif national est de nature à prendre en compte les nouveaux usages au moins sur le territoire national. Cependant, comme pour les forums, ce dispositif ne couvre pas les serveurs de messagerie localisés à l'étranger.

Il ne prend pas non plus en compte les nouvelles pratiques ou produits de type ICQ (" I seek you " : je vous recherche) qui permettent de savoir si un internaute est connecté ou pas ; ce logiciel téléchargeable permet de retrouver tous les membres d'une liste dès qu'ils se connectent sur le Net ; 4 millions d'internautes l'utiliseraient !

Que penser, enfin, de services comme " Do it yourself " qui propose pour 19,95 dollars six mois de recherche tous azimuts sur le Net concernant un ami, un concurrent...

L'on voit bien que la dimension internationale et l'extrême variété de produits sans cesse renouvelés rend l'encadrement réglementaire national un peu théorique malgré les recommandations du régulateur et livre l'internaute aux pratiques hétérogènes des acteurs.

Les annuaires

Il s'agit de sites, dédiés en tout ou partie à la diffusion sur Internet d'annuaires de membres,

d'élèves, d'abonnés ou de personnels, qui étaient, le plus souvent, d'ores et déjà édités sur d'autres supports, papier ou télématique.

S'agissant plus précisément des annuaires téléphoniques, la doctrine de la CNIL a été rappelée dans l'avis qu'elle a rendu le 4 février 1997 sur le projet de décret relatif à l'annuaire universel. Le retard de la promulgation de ce décret a conduit la Commission à exprimer sa position à l'attention de tous les acteurs du secteur de l'édition de listes d'abonnés, par délibération no 97-60 du 8 juillet 1997 portant recommandation relative aux annuaires en matière de télécommunications.

Dans cette délibération, la Commission recommande que les abonnés soient clairement et préalablement informés par les éditeurs d'annuaires sur Internet des caractéristiques du réseau Internet que sont la libre captation des informations diffusées et la difficulté, voire l'impossibilité, de contrôler l'utilisation qui pourrait être faite de ces données par des tiers.

La Commission recommande par conséquent que les abonnés puissent s'opposer gratuitement et sans avoir à indiquer de motif à la diffusion sur un réseau international ouvert de données les concernant. Ce droit d'opposition doit pouvoir s'exercer préalablement à la diffusion des données sur Internet ainsi qu'ultérieurement à tout moment.

Cette recommandation a été depuis lors suivie par France Télécom et un éditeur privé d'annuaires qui diffusent, l'un et l'autre, sur Internet l'annuaire téléphonique. France Télécom, par l'intermédiaire de la " Lettre de France Télécom " annexée à la facture de janvier février 1998, l'éditeur privé, par publipostage d'une brochure, ont informé les abonnés de ce droit d'opposition spécifique et des modalités de son exercice gratuit (appels à un numéro gratuit propre à chaque éditeur). En outre, l'acte réglementaire de France Télécom relatif à la gestion des annuaires édités par l'opérateur, vise expressément l'information, l'existence et les modalités d'exercice de ce droit d'opposition.

Les positions prises par la Commission (l'information et le droit d'opposition préalables des personnes à la diffusion sur Internet de données les concernant) trouvent leur fondement dans le fait qu'un réseau de type Internet offre des possibilités uniques de captation des informations diffusées et rend difficile, voire impossible, de contrôler l'utilisation qui pourrait en être faite par des tiers.

Les moteurs de recherche tel que (Yahoo, Alta Vista...) sont, en effet, des moyens extrêmement puissants de recherche d'informations et, en indexant l'ensemble des données diffusées, ils rendent tout internaute, quelle que soit sa localisation sur la planète, destinataire potentiel de ces informations ; ceci est un enrichissement formidable des outils de connaissance mais aussi une source renouvelée d'utilisations contestables, la plupart des pays de " traitement " n'offrant pas le niveau " adéquat " de protection exigé par l'article 25 de la directive du 24 octobre 1995.

La collecte d'informations en ligne

Il s'agit dans la plupart des cas de formulaires que l'internaute doit remplir requérant l'adresse électronique, l'identité, les références postales ou téléphoniques ainsi que des informations socio-économiques relatives au visiteur (profession, revenu,...). La question est de savoir pour quelles utilisations ces données sont collectées et si l'utilisateur est toujours au courant de celles-ci.

Une étude récente réalisée par l'EPIC , groupe de pression en faveur de la vie privée aux États-Unis, sur les cent sites les plus visités du Web, a montré que plus de la moitié d'entre eux avaient constitué des profils d'utilisateurs.

Le problème pourrait être aisément réglé dans le cadre européen où les principes de la directive s'imposent aux formulaires de collecte. En revanche, il reste non résolu pour une collecte de caractère mondial réalisée dans un pays n'offrant pas de protection et téléchargée vers l'Union européenne.

Les internautes ont cependant trouvé une parade, un peu amère pour les tenants du marketing direct : une étude du GVUC (Graphic, Visualization & Usability Center) affirme que 40 % d'entre eux auraient l'habitude de livrer de fausses informations quand ils sont questionnés en ligne !

Les traitements invisibles

Au-delà des données nominatives circulant sur le réseau, il en est d'autres que l'utilisateur ordinaire ne peut directement appréhender, alors que leur valeur informationnelle et les risques qu'elles représentent pour la vie privée des personnes sont importants.

Les données de connexion ou " fichier log "

Ces données sont liées aux techniques utilisées sur Internet pour établir la communication entre ordinateurs distants (le protocole TCP/IP) et à l'utilisation faite du réseau par l'individu ; elles concernent d'une part les adresses des machines du réseau, dites adresses IP, et en particulier celles de l'émetteur d'un message et de son destinataire, adresses auxquelles sont associées la date et l'heure de la connexion, des informations techniques caractérisant le type d'usage (accès au Web, messagerie...) d'autre part, la requête (page du site que l'utilisateur veut visiter...) ou le message proprement dit. Ces données sont collectées automatiquement par les fournisseurs d'accès et consignées dans un fichier dénommé " fichier log ".

Ces éléments sont des outils d'identification et de " traçabilité " des individus extrêmement puissants qu'il convient d'analyser.

? *Quelques éléments techniques*

L'adresse IP n'est pas l'adresse d'une personne physique mais " l'adresse réseau " de la machine d'un utilisateur connecté au réseau Internet.

Selon le choix technique et contractuel effectué par l'utilisateur ou l'organisme qui lui fournit l'accès à Internet (par exemple entreprise ou université), l'adresse IP de la machine de l'utilisateur sera permanente (on parle alors d'adresse fixe) ou sera attribuée par le fournisseur d'accès, à la volée, pour la durée de la connexion (on parle alors d'adresse IP dynamique).

L'adresse IP étant l'identification, parfois temporaire, d'une machine, on pourrait s'interroger sur son rapport avec la protection des données. Les incidences de l'attribution d'une adresse IP sont cependant tout à fait considérables.

L'adresse IP affectée à la machine de l'utilisateur, qu'elle soit permanente ou dynamique, est en effet significative pour le responsable du réseau et pour son fournisseur d'accès, qui sont en mesure, à tout moment, de faire le lien entre l'utilisateur et cette adresse, ainsi qu'avec toutes les informations relatives à la nature de la communication (messagerie, consultation de sites, etc), la date et l'heure de la connexion, l'adresse du site Internet consulté ou de la page du site demandée.

En effet, le fournisseur d'accès peut conserver toutes les données de connexion correspondantes à une adresse IP et associer à chaque adresse IP, même dynamique, l'ensemble des données personnelles relatives à l'internaute, qui est son client.

Ainsi les données conservées par le fournisseur d'accès (données de connexion associées à l'adresse IP) peuvent permettre de suivre, pas à pas, l'activité d'un internaute (les sites visités, la date et l'heure, les documents téléchargés, la participation à un espace de discussion, les messages électroniques expédiés ou reçus) aussi longtemps que ces données sont conservées.

Les fichiers " logs " détenus par les fournisseurs d'accès constituent, dès lors, un gisement de données indirectement nominatives – association de l'identité d'un client et des autres données personnelles figurant dans le fichier de gestion de clientèle du fournisseur d'accès et détail de ses " navigations " et de ses utilisations d'Internet – qui soulève d'importants problèmes de protection des données personnelles.

? *Quelles sont les garanties qui devraient être attachées à ce type de données ?*

Il n'existe pas de jurisprudence sur la nature des données de connexion à un site Internet, en particulier sur le point de savoir si ces données sont " indirectement nominatives " au sens de l'article 4 de la loi du 6 janvier 1978. La réponse ne fait cependant aucun doute dans la mesure où le fournisseur d'accès peut associer le nom d'un client à une adresse IP.

La CNIL, faisant application des principes de finalité légitime et de proportionnalité (article 5 de la convention 108 du Conseil de l'Europe repris dans la directive européenne de 1995) a reconnu, dans le domaine non marchand, deux finalités distinctes et légitimes pour le traitement de ces données : la sécurité afin d'éviter les pénétrations frauduleuses du site et l'élaboration de statistiques agrégées sur les consultations du site. La question est de savoir si d'autres finalités peuvent justifier la conservation de ces données. L'enjeu commercial est évidemment important.

Les fournisseurs d'accès recherchent en effet la rentabilité économique qui résulte non seulement des revenus qu'ils tirent des abonnements souscrits, mais également des revenus provenant de la publicité.

Or, Internet permet de passer de la prospection de masse à la prospection ciblée dite " one to one ", c'est-à-dire directement adaptée au profil comportemental d'une personne.

L'analyse des services, des sites et informations consultés par tel internaute permet de connaître, beaucoup mieux que par le biais d'une enquête directe, les habitudes, goûts et centre d'intérêts de celui-ci : la technique offre là de nouveaux moyens d'établissement de bases de données comportementales.

L'application, dans ce domaine, des principes de la protection des données tels qu'ils sont prévus par les textes actuels et, sur ce point, repris par la directive européenne, a conduit la CNIL à l'élaboration d'une doctrine fondée, d'une part, sur le principe de la collecte loyale des données, d'autre part, sur le droit d'opposition des personnes.

Les personnes doivent être informées de la finalité du traitement de ces données et de leur droit de s'opposer à l'enregistrement de certaines catégories de services consultés (en particulier ceux qui sont susceptibles de faire apparaître, outre leur profil de consommateur potentiel, leurs mœurs, leurs opinions politiques ou religieuses, c'est-à-dire les données sensibles visées par l'article 31 de la loi du 6 janvier 1978).

Cette approche n'épuise cependant pas le sujet dans la mesure notamment où certains fournisseurs d'accès offrent un accès gratuit à Internet ou un service de messagerie électronique en contrepartie de l'autorisation donnée par l'internaute d'analyser à des fins de prospection personnelle les données de connexion qui se rapportent à sa " navigation " sur Internet ; cette pratique manifeste aisément les limites des solutions qui reposent sur le choix individuel de la

personne.

Faut-il poursuivre dans cette direction et laisser faire le marché ? Pour certains, une telle évolution serait de nature à faire dépendre la protection de la vie privée du revenu des utilisateurs et pourrait ruiner à terme l'économie globale du réseau : la défiance des consommateurs envers ce nouveau média pourrait, en effet, croître si son accès à moindre coût était subordonné à l'abandon de leurs droits.

Cette problématique est, à un moindre degré, comparable à celle qui s'était développée il y a quelques années sur la vente d'organes humains : certains pays européens défendaient que l'autonomie de la volonté des individus justifiait que chacun ait le droit de vendre ses organes. Peut-on, de même, vendre sa propre vie privée ?

La CNIL recommande, si l'on souhaitait inverser cette tendance, d'interdire par voie législative un contrat qui pourrait être considéré comme contraire à l'ordre public. Cette appréciation juridique, qui est déjà une réalité aujourd'hui sans nécessité d'élaborer un nouveau texte, ne résoudrait, en tout état de cause, qu'imparfaitement la question : celle-ci est posée au plan international et une interdiction purement nationale aurait une portée limitée.

Une autre forme d'exploitation commerciale de ces données consiste à céder à des tiers des informations résultant du rapprochement du fichier de clientèle (nom, adresse, téléphone, etc) et des données de connexion qualifiant les habitudes et le comportement de la personne concernée. Cette question pose celle de la confidentialité de ces données.

Sur ce point, il convient de relever que l'accès à tel ou tel service de communication audiovisuelle, catégorie dans laquelle peuvent être classés les services diffusés à partir d'un site Internet , est couvert par le secret. En effet, l'article 3 de la loi no 86-1067 du 30 septembre 1986 relative à la liberté de communication dispose que " le secret des choix faits par les personnes parmi les services de télécommunications et parmi les programmes offerts par ceux-ci ne peut être levé sans leur accord ".

Les choix du consommateur au cours de sa navigation sur les sites Web, notamment synthétisés par les fichiers logs, relèvent donc de l'article 3 de la loi de 1986 et ne peuvent dès lors être dévoilés sans l'accord de l'intéressé.

En outre, la directive européenne du 24 octobre 1995 consacre explicitement un élément de doctrine depuis longtemps dégagé par la CNIL : le droit de s'opposer sans motif, sauf dérogations en nombre limité, à la cession de ses données à des tiers. Le droit actuel permet donc de garantir en Europe du moins, pour cette dernière forme d'exploitation commerciale des données de connexion, le respect des données personnelles.

Les " cookies "

Un " cookie " est un petit fichier émis par un serveur consulté par un utilisateur et enregistré sur le disque dur de celui-ci. Il est identifié par l'adresse Internet du site ou de la page. Il comporte, en général, une date de validité – sa durée de conservation – et peut contenir l'information qu'aura souhaité y inclure le site visité.

Il permet au responsable du site de mémoriser les précédentes consultations du site par l'internaute afin, soit de faciliter l'ergonomie de la visite (en évitant, par exemple, de remplir à chaque visite le même formulaire d'identification), soit d'adapter les pages du site au " profil " de l'internaute tel qu'il est précisément déduit des " traces " conservées lors des visites précédentes.

La plupart des logiciels de navigation qui incluent cette fonction sont programmés de manière à ne permettre la lecture d'un cookie que par le serveur ou site qui l'a envoyé. Les versions les plus courantes des logiciels de navigation sur le marché permettent la conservation de deux cents cookies sur le poste de l'utilisateur, un nouveau cookie étant, au-delà de ce nombre, mémorisé à la place du plus ancien cookie reçu.

Mise en œuvre de manière cachée, cette technique a été considérée par la communauté des internautes comme constituant un " pistage " inadmissible des utilisateurs.

La CNIL, pour sa part, lors de débats publics, ainsi qu'à l'occasion de l'instruction du dossier relatif au service en ligne de Microsoft et de sa prise de position sur le commerce électronique, a indiqué que la mise en œuvre de cette technique à l'insu des internautes soulevait des difficultés tant au regard du principe de la collecte loyale des informations que de celui du droit d'accès, dans la mesure où, même dans l'hypothèse où il en aurait connaissance, l'internaute n'est pas en mesure de comprendre la signification des informations enregistrées dans le cookie.

Les éditeurs de logiciels de navigation ont, peu à peu, modifié leur approche au fur et à mesure de la sortie de nouvelles versions. Ils ont, en effet, à partir de 1996, permis aux utilisateurs d'être avertis de l'envoi d'un cookie et d'en accepter ou d'en refuser l'enregistrement. Cette procédure a eu une conséquence : les utilisateurs étaient constamment sollicités pour faire connaître, à chaque fois qu'un cookie leur était envoyé, leur choix d'accepter ou de refuser celui-ci, ce qui entravait considérablement leur navigation.

En outre, pour les deux logiciels de navigation les plus connus commercialisés depuis l'été 1997, les utilisateurs se voient offrir le choix de refuser *a priori* l'enregistrement de tout cookie ce qui, rappelons-le, est lourd de conséquences en termes de facilité de navigation.

En tout état de cause, le maintien de l'utilisation de cette technique devrait passer par l'application des principes habituels de la protection des données : il ne devrait pas être possible d'inscrire une information sur le disque dur d'un utilisateur sans qu'il en soit averti, sans qu'il puisse s'y opposer et sans qu'il puisse en connaître la teneur de manière intelligible.

C'est d'ailleurs ce que certains serveurs effectuent en intégrant cette technique à celle de l'envoi de formulaires comme ceux relatifs à la facturation des biens commandés, permettant ainsi à l'utilisateur de prendre connaissance de l'ensemble des éléments nécessaires à la décision de conserver ou non le cookie.

Concernant les cookies, la réaction des internautes et l'action pédagogique des autorités de protection des données personnelles ont permis, finalement, d'améliorer considérablement la situation. Le rapport prochain du Centre national de la consommation (CNC) devra, à l'image de son étude sur l'offre de connexion, permettre de dresser un bilan exhaustif de ces pratiques.

Conclusion

Il ressort de cette analyse sur les risques nouveaux liés aux pratiques et spécificités des réseaux :

– que le régulateur qu'est la CNIL a très tôt analysé ces nouvelles pratiques et formulé des avis ;

– que les seules réponses nationales sont clairement insuffisantes ;

– que face à l'extrême dispersion et variété des pratiques des acteurs, il est nécessaire d'associer ceux-ci à la protection des données personnelles, de façon positive et volontaire, sous peine de voir l'arsenal réglementaire " dépassé " par la réalité.

Les exemples étrangers :

autorégulation et liberté de circulation de l'information

Le développement commercial d'Internet a été l'occasion, depuis 1994, dans tous les pays développés et dans plusieurs organisations internationales, d'une intense activité sur le thème de la protection de la vie privée et des données personnelles.

Dans les États de l'Union européenne, les questions ont été traitées jusqu'à ce jour en tant qu'application des lois générales de protection des données, sauf en Allemagne où ont été adoptées des dispositions législatives particulières dans le cadre de la loi sur le multimédia du 1er août 1997.

Dans les États non dotés de législation générale d'application dans le secteur privé, le problème a pris la forme de débats publics importants dans lesquels l'industrie, les gouvernements et les associations de défense des libertés se sont engagés. Ces débats portent tout à la fois sur des pratiques particulières, telle que celle des " cookies ", la nature du système de protection dans son ensemble (législation, autorégulation professionnelle, recours à des procédés techniques), le contenu des principes de protection (principes de finalité et de proportionnalité, de transparence, droit d'accès, recours, autorité indépendante de contrôle...). C'est le cas notamment aux États-Unis, au Canada et en l'Australie.

Au plan international, dès la première conférence ministérielle du G7 sur la société de l'information, tenue à Bruxelles les 25 et 26 février 1995, la protection de la vie privée et des données personnelles a été reconnue comme une exigence. Ainsi les partenaires se sont engagés à " intensifier leurs efforts en vue de trouver des solutions technologiques et politiques créatives [...], qui supposent la définition de dispositions nationales et régionales, le respect de celles-ci et la coopération internationale ".

En l'absence d'une enceinte internationale spécifique de négociation, les organisations internationales impliquées de longue date dans le sujet en ont traité depuis lors, le Conseil de l'Europe en liaison avec la convention 108 et l'Organisation de coopération et développement économique (OCDE) en liaison avec les lignes directrices adoptées en 1980. D'autres ont émergé à la faveur de ce mouvement, l'Organisation internationale de normalisation (ISO) à la suite d'une initiative canadienne, et l'Organisation mondiale du commerce (OMC) à la suite de l'initiative de l'Union européenne, dans le prolongement des accords du GATS, qui prévoient une possibilité de dérogation à la libre circulation des services fondée sur la protection des données (article XIV).

Il convient de noter que cette activité internationale est essentiellement rythmée par la position prise par l'Union européenne depuis l'adoption de la directive du 24 octobre 1995 et par les réponses formulées jusqu'à présent par les États-Unis.

L'Union européenne, dotée de principes ancrés dans les droits de l'homme, contraignants, éprouvés et harmonisés, a en effet posé, dans la directive du 24 octobre 1995, le principe du " niveau de protection adéquats " des pays tiers vers lesquels le transfert de données personnelles est autorisé. Ce principe, au-delà de ceux contenus dans la convention du Conseil de l'Europe, prend un relief particulier dans le cadre d'Internet.

Les États-Unis, quant à eux, berceau du développement de l'Internet et de ses technologies, connaissent quelques lois sectorielles en vigueur au plan fédéral couvrant certains aspects de la protection des données mais se sont prononcés de manière plus générale pour l'autorégulation. Ainsi le président Clinton a-il incité les entreprises, le 1er juillet 1997, dans le cadre de sa communication " Framework for Global Electronic Commerce ", à développer des pratiques loyales en matière de traitement de données personnelles ; un bilan de cette politique est attendu

pour juillet 1998.

Dès lors, compte tenu de ces divergences d'appréciations, le débat international progresse à pas lents et tente de ménager les diverses voies ; ainsi la conférence internationale ministérielle de Bonn des 6-8 juillet 1997 organisée par le gouvernement allemand et la Commission européenne sur les réseaux globaux de l'information a-t-elle notamment précisé, en matière de protection des données, que " les ministres conviennent de conjuguer leurs efforts pour établir des principes universels de libre circulation de l'information tout en sauvegardant le droit fondamental à la vie privée et à la protection des données... "

Au-delà des effets d'annonce politique, au titre de la politique commerciale commune à l'égard des pays tiers et sur le fondement de la réglementation en matière de flux de données vers les pays tiers prévue dans la directive 95/46 précitée, la Commission européenne, à la suite de sa communication " La mondialisation et la société de l'information. La nécessité de renforcer la coordination internationale " de début 1998 (Com 98-50 du 4.2.98) , s'efforce d'organiser la coordination des États membres de l'Union européenne en vue de défendre une position commune dans le cadre des relations bilatérales et dans les enceintes internationales. Le contenu le plus clair de cette position, en l'état, trouve son expression dans l'initiative prise en mai 1998 au sein de l'OMC (voir *infra*).

Les États de l'Union européenne

Les États membres procèdent actuellement à la transposition en droit national des directives 95/46 du 24 octobre 1995 sur la protection des données personnelles et la libre circulation de celles-ci, et 97/66 du 15 décembre 1997 complémentaire et spécifique au secteur des télécommunications. Les autorités nationales de protection des données ont, en général, estimé nécessaire, en ce qui concerne Internet, de développer leurs activités de conseil en direction tant des fournisseurs de services que des utilisateurs (comme la CNIL, l'Agence de protection des données espagnole, par exemple, a publié un guide destiné aux utilisateurs d'Internet).

Elles font également preuve, comme la CNIL, de grandes précautions quant à la mise en ligne sur Internet de registres tenus par l'administration (exemple du refus opposé par les autorités allemandes à la mise à la disposition du public, par Internet, du registre de population tenu par les autorités administratives locales).

Un seul État a procédé à ce jour à l'adoption d'une loi spécifique. Il s'agit de l'Allemagne où la loi fédérale sur le multimédia du 1er août 1997 comporte un article 2 sur la protection des données. Les dispositions originales de cette loi concernent l'obligation pour les fournisseurs de services d'offrir une possibilité d'accès et de paiement anonyme (ou sur la base de pseudonyme) à leurs clients " dans la mesure où cela est raisonnable et réalisable techniquement " (§4) . Les données de connexion relatives à une personne ne peuvent être transmises à un tiers sans son accord (§4) ou utilisée à des fins de prospection commerciale, d'enquête de consommation ou de recherche en vue de la conception de services (§5). Elles ne peuvent être conservées au-delà de la connexion que dans la mesure où elles sont nécessaires à la facturation du service et pour une période n'excédant pas 80 jours (§6), le droit d'accès par la personne aux données qui la concerne devant pouvoir s'exercer en ligne si elle le souhaite (§7). Le commissaire fédéral à la protection des données est compétent pour assurer le contrôle de l'application de cette loi (§8).

La Conférence des commissaires européens à la protection des données réunis à Dublin les 23 et 24 avril 1998 a adopté, sur proposition de la CNIL, une résolution tendant, d'une part, à rappeler que les réglementations européennes en matière de protection des données sont applicables à tout traitement de données mis en œuvre dans le cadre d'Internet, d'autre part, à ce que le groupe réuni dans le cadre de l'article 29 de la directive 95/46 examine les modalités de cette

application.

Les États hors Union européenne

Australie

L'Australie fait partie des pays qui ont adopté, de longue date, une loi de protection des données pour le secteur public instituant une autorité indépendante pour le contrôle de son application. Après des hésitations sur la politique à mener notamment sous le précédent gouvernement fédéral qui avait annoncé pendant une période son intention de proposer une législation pour le secteur privé, le gouvernement actuel encourage le secteur privé à adopter des codes de conduite. Une campagne en ce sens est actuellement en cours.

Canada

Le Canada qui a adopté depuis longtemps également des lois sur la protection des données pour le secteur public tant au niveau fédéral que dans la plupart des provinces, ne dispose d'une loi applicable au secteur privé que dans la province du Québec.

En 1995, l'organisation canadienne de standardisation (CSA) a mis au point un code de conduite destiné aux entreprises. Plusieurs professions ont également élaboré des codes de conduite, notamment dans le secteur bancaire et dans celui du marketing direct.

Le développement des autoroutes de l'information a incité à une plus ample réflexion. Actuellement une large consultation publique est en cours au niveau fédéral qui a pour objet l'adoption d'une loi en 2000 fixant des principes pouvant se décliner, par profession, selon la technique du code de conduite. Le projet de loi devrait être rendu public en septembre 1998.

Enfin, le Canada joue un rôle important pour l'organisation de la conférence d'Ottawa d'octobre 1998, notamment en matière de données personnelles (voir *infra*).

Japon

Le Japon a adopté diverses législations régissant au plan national et local les fichiers publics. Cependant, il n'existe pas d'autorité particulière ayant compétence pour en garantir l'application. Des codes de conduite sectoriels traitent de la matière dans le secteur privé, notamment dans les secteurs bancaire et des télécommunications.

Dans le cadre d'initiatives destinées à favoriser le développement du commerce électronique international, le MITI a fait élaborer en 1997 un code de conduite destiné aux entreprises privées, largement inspiré par la directive européenne. En avril 1998, le MITI a créé sous sa tutelle une " autorité de surveillance " qui pourrait mettre en œuvre, d'ici deux années, une procédure de certification des entreprises et instruire les plaintes des particuliers, le MITI demeurant compétent pour intervenir auprès des entreprises.

États-Unis

Les premiers travaux liés à la protection des données dans le cadre des réseaux électroniques datent des années 1994-1995. Ils ont abouti en 1996, à la suite de nombreuses auditions et versions du document, à la publication de lignes directrices reprenant les principes de l'OCDE de manière détaillée, sans toutefois prévoir de mécanismes de mise en œuvre.

La communication du président Clinton de juillet 1997 (voir *supra*) lance véritablement le programme de travail gouvernemental pour le commerce électronique sous la responsabilité du conseiller Ira Magasiner ; celui-ci a un an pour apporter des solutions à un certain nombre de

" chantiers " dont celui des données personnelles. L'administration américaine incite alors les entreprises à développer des politiques de protection des données : codes de conduites, dispositifs techniques... En avril 1998, le département américain du commerce constate les faibles progrès de l'autorégulation et, tout en menaçant en quelque sorte l'industrie de présenter une législation, il incite les entreprises à approfondir leur démarche d'autorégulation, axée sur les pratiques loyales en matière de traitement de l'information (information des entreprises, choix des consommateurs, accès des consommateurs à leurs données, sécurité, selon des principes très libéraux " notice, choice, access, security "), en y ajoutant l'exigence que des mécanismes de recours soient offerts aux personnes.

Pour sa part, la Federal Trade Commission (FTC) a rendu public le 4 juin 1998 les résultats d'une étude menée auprès de 1400 sites Internet commerciaux américains. Il en ressort que 14 % des sites donnent des informations sur leur pratiques en matière de traitement de données personnelles, cependant que 2 % seulement ont développé une politique approfondie dans le domaine ; en outre, constatant la situation préoccupante des sites qui collectent des données auprès d'enfants sans l'accord de leurs parents, la FTC s'est prononcée, dans son rapport au Congrès, en faveur d'une législation de protection spécifique pour ceux-ci ; elle annonce une initiative en ce sens dans le courant de l'été 98.

Ce rapport de la FTC a suscité une vive réaction de la part du gouvernement fédéral : le vice-président Al Gore a déclaré que le *statu quo* n'était plus acceptable et a annoncé la mise en œuvre d'une véritable Déclaration des droits électroniques (" Electronic Bill of Rights ").

Concernant les procédés techniques d'autorégulation, plusieurs initiatives privées, soutenues par l'industrie électronique, doivent être mentionnées. Il s'agit, tout d'abord, de l'organisation " TRUST e ", qui procède à la certification des politiques de protection des données de sites Internet (75 à ce jour) ; il s'agit ensuite du projet du consortium du World Wide Web " Plateform for Privacy Preference " (P3P), essentiellement animé par des entreprises américaines et destiné à offrir à l'utilisateur final la possibilité de gérer lui-même la communication de ses données en fonction de la " pratique " énoncée par le site et de ses " préférences ". Les incitations économiques ne sont cependant pas exclues de cette négociation. Ces mécanismes devraient être inclus et diffusés au plan mondial dans les prochaines versions des logiciels de navigation sur l'Internet d'ici la fin de l'année 1998.

Une conférence sur la protection de la vie privée prévue par l'administration américaine pour faire le bilan de l'autorégulation en vue du rapport au président Clinton en juillet, repoussée à plusieurs reprises ce printemps, devait se tenir les 23 et 24 juin 1998.

Les organisations internationales

Le Conseil de l'Europe

Dans le cadre des travaux liés à la Convention 108 sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, le Conseil de l'Europe a rendu public le 15 avril 1998 " les lignes directrices sur la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel dans les inforoutes, qui peuvent être intégrées ou annexées à des codes de conduites ".

Ce texte, qui s'adresse aux utilisateurs d'Internet et aux fournisseurs d'accès, émane du Groupe de projet sur la protection des données (CJ-PD). Dans ce cadre, une coordination des États membres de l'Union européenne a été organisée. Le texte devrait être soumis au Conseil des ministres du Conseil de l'Europe pour approbation dans les mois qui viennent.

L'Organisation internationale de normalisation (ISO)

L'Organisation internationale de normalisation, et plus particulièrement son Comité pour la politique en faveur des consommateurs (COPOLCO) examine la proposition canadienne faite en 1995 tendant à l'élaboration d'une norme pour la protection de la vie privée des consommateurs à l'égard du traitement de leurs données personnelles.

L'Organisation pour la coopération et le développement économique (OCDE)

Dans le cadre des travaux consécutifs à l'adoption en 1980, sous forme de recommandation, de lignes directrices en matière de protection des données, le Comité de la politique de l'information, de l'informatique et des communications (PIIC), et plus particulièrement son groupe d'experts sur la sécurité de l'information et la vie privée, a organisé deux journées d'étude en février 1998 sur la question de la vie privée sur Internet ; par ailleurs, il a examiné en mai 1998 les résultats d'une étude menée sur 50 sites Internet choisis dans divers États membres pour leur exemplarité ; cette étude montre qu'il existe encore un réel décalage entre le monde des institutions et organisations qui développent une approche ainsi que des instruments en matière de protection des données et celui des sites Internet qui, malgré leurs bonnes intentions, manquent d'orientations précises pour l'application des lignes directrices sur les réseaux numériques.

En vue de la conférence ministérielle d'Ottawa des 7-9 octobre 1998, le comité PIIC prépare une déclaration réaffirmant la pertinence des lignes directrices dans le contexte de l'Internet. Une coordination des États membres de l'Union européenne est en cours d'organisation.

L'Organisation mondiale pour le commerce (OMC)

En vue de la réunion de l'OMC de mai 1998, la Communauté européenne et ses États membres ont adopté le 23 avril 1998 une déclaration précisant les sujets et objectifs à poursuivre dans le cadre de l'OMC à propos du commerce électronique. Cette communication porte en particulier sur la protection des données. Elle propose de " favoriser la confiance entre États membres de l'OMC afin d'éviter les éventuels blocages d'informations et la distorsion de concurrence " en établissant une discussion en vue " d'assurer une protection effective de la vie privée des personnes à l'égard du traitement des données personnelles sur la base de principes clairs, de leur transparence à l'égard de tous et de l'effectivité de leur application ".

Les critères ainsi énoncés sont de nature à pouvoir conduire à l'adoption d'instruments contraignants de type législatif au plan national et conventionnel au plan international.

À la suite de cette proposition, un groupe de travail devrait être organisé dont les travaux pourraient s'étendre sur plusieurs années.

Conclusion

Le débat international sur les données personnelles est nourri. Les expériences des divers pays consacrent plus l'autorégulation des acteurs au cas par cas que la démarche contraignante et générale de l'Union européenne. Cependant, les rapports récents de la FTC et de l'OCDE montrent les limites de dispositifs fondés sur la seule " bonne volonté " des acteurs dans un environnement très concurrentiel. **La pression de l'opinion publique et des fondateurs de l'Internet qui s'émeuvent de plus en plus des risques liés à l'utilisation commerciale des données et la position affichée par les autorités fédérales américaines, pourrait offrir un contexte favorable au rapprochement des deux points de vue.**

La difficulté est l'incertitude de la situation politique aux États-Unis : si le rapport au président Clinton de juillet 1998 conduisait à un constat d'échec, il ne resterait que le recours au Congrès dont la position et le calendrier d'intervention sont difficiles à prévoir en période préélectorale.

Les solutions nouvelles : un accord international et une nécessaire combinaison du droit et des mesures d'autorégulation

Dans un environnement décentralisé et international, les moyens de protection de la vie privée et des données personnelles ne peuvent se limiter à l'action réglementaire traditionnelle ; ils doivent être aussi recherchés dans la mise en œuvre de procédés variés d'autorégulation associant les acteurs économiques et les utilisateurs à l'application effective des principes fixés par la loi nationale ou internationale.

Contrairement à ce que certains débats ont pu laisser supposer, ces deux approches ne sont pas exclusives ; elles doivent au contraire se combiner, se conforter mutuellement afin d'obtenir une action efficace. L'essentiel est de s'entendre au plan international sur un nombre limité d'objectifs communs que ces deux outils déclineront.

La France a une voix singulière à faire entendre qui ne saurait se résoudre à la seule exportation de son " modèle " de protection des données ; elle doit et peut, compte tenu de son expérience dans ces matières, ouvrir des voies de propositions.

La nécessité d'un accord international

Les risques sur les données personnelles, dénoncés plus haut et résultant des pratiques enregistrées sur le réseau ont montré les limites d'une approche nationale. Par ailleurs, l'expérience récente de l'autorégulation aux États-Unis souligne le fait que celle-ci ne peut être réellement efficace qu'en s'inscrivant dans un cadre et dans des principes communs qu'elle décline.

Il apparaît donc nécessaire de définir au niveau mondial un corpus minimum de principes de protection des données et une coordination des États pour la poursuite et la répression des éventuelles violations.

La transposition de la directive du 24 octobre 1995 et la nécessité de protection " adéquate " que fixe l'article 25 pour les transferts vers des pays tiers offrent une opportunité unique de discuter avec nos partenaires de ces principes communs pouvant faire l'objet d'une convention internationale.

Le groupe de l'article 29 de la directive européenne sur la protection des données personnelles, dans son analyse du rapport entre droit et autorégulation, s'est d'ailleurs prononcé, par deux document de juin 1997 et janvier 1998, en faveur d'un instrument international contraignant. Le forum de la Société de l'information, réuni à Bruxelles, a également marqué à plusieurs reprises que, pour la préservation des droits de la personne qui prend souvent le visage du consommateur, il fallait fixer des droits au sens strict du terme.

Des principes communs, mais lesquels ?

La liste indicative suivante pourrait être proposée pour nourrir la réflexion politique et technique :

– caractère loyal et licite de la collecte des informations personnelles ;

– caractère pertinent et non excessif des données collectées au regard des finalités du traitement ;

– exactitude des données collectées et droit d'accès et de rectification de celles-ci ;

– information claire de l'utilisateur sur les données collectées et leurs finalités ;

– devoir de garantir la sécurité et la confidentialité des données collectées ;

– droit d'opposition, gratuit et sans justification de toute personne à ce que des données relatives à sa vie privée soient mises en circulation sur les réseaux.

Ces principes très généraux devraient fixer le cadre international contraignant au sein duquel se développeraient les mécanismes d'autorégulation (codes de conduite, dispositifs techniques, contrats...).

L'accord international pourrait sans doute éclairer les principes de la directive relatifs aux conflits de loi : la directive, dans un souci de réalisme et de clarification, énonce que la loi nationale est applicable " lorsque le traitement est effectué dans le cadre des activités du responsable du traitement sur le territoire de l'État membre " ; c'est l'établissement du responsable du traitement qui détermine la loi compétente ; le responsable du traitement est plus loin défini comme la personne physique qui " seule ou conjointement avec d'autres, détermine les finalités et moyens du traitement à caractère personnel " ; enfin, la directive permet de rattacher à la loi nationale d'un État membre le cas où des données sont collectées dans cet État, " par quelque moyen que ce soit ", pour être traitées par une entreprise établie dans un pays tiers, ceci afin d'éviter la délocalisation dans des " paradis numériques ".

Cependant, comment définir le lieu d'établissement ? Quels " moyens de traitement " justifient le rattachement territorial ? La discussion sur la fiscalité (voir *infra* deuxième partie) montre la difficulté de raisonner par exemple par rapport au serveur et la nécessité de préciser les critères de rattachement. Au-delà de ces difficultés pratiques, quel est le sens d'une logique, fondée sur des flux de données alors que dans les réseaux, chaque message est découpé en paquets qui vont transiter par des chemins différents et par des pays offrant ou non une protection équivalente ? Lors de ces acheminements, plusieurs opérateurs auront assuré une partie de la connexion sans que rien n'indique s'ils sont soumis ou respectent des obligations relatives à la vie privée. De même, comment apprécier les lieux de transfert des données dans le cas d'une communauté virtuelle (" smart communities ") qui échange des informations entre ses membres partout dans le monde. En réalité, toute donnée mise en ligne sur Internet ou tout autre réseau ouvert est potentiellement à destination de tous les pays du globe connectés au réseau, ce qui rend un peu théorique la question du transfert.

Le recours aux procédés d'autorégulation

Il revient aux acteurs économiques et aux utilisateurs d'élaborer les moyens permettant de mettre en œuvre les principes fixés plus haut.

Les codes de conduite et les procédés contractuels

Divers moyens sont possibles :

– **élaboration de codes de conduite et de déontologie** fixant les règles que les signataires s'engagent à respecter : secret des correspondances, sécurité des données, exploitation... Le code de déontologie de l'association des fournisseurs d'accès en France (AFA) est encore assez modeste et il conviendra de préciser la position des acteurs français à travers l'organisme de corégulation (voir quatrième partie) ; le système des codes de conduite apporte également une réponse au problème du transfert vers les pays tiers, les sociétés adhérentes, respectant les principes de la directive, signent un engagement contractuel leur donnant droit à autorisation de transfert (*cf.* article 26-2 précité de la directive de 1995). Ces codes peuvent être extrêmement complets comme celui du Syndicat des entreprises de vente par correspondance et à distance et animer une profession ; la dernière initiative du Syndicat de définir une liste de clients refusant de voir leurs données personnelles collectées (" liste Robinson ") et l'élaboration d'une Charte de

qualité montrent l'efficacité d'une démarche professionnelle qui noue par ailleurs des contacts avec ses homologues internationaux. La Fédération du marketing direct européen, de même, a défini avec ses membres des lignes directrices communes sur le respect des données personnelles et envisage d'apposer une " icône vie privée " sur les site de chacun d'entre eux permettant à chaque utilisateur de connaître la politique de " vie privée " du groupement ;

– **engagement contractuel** de respecter certaines règles dans la mise en œuvre de telles ou telles activités. Cette possibilité d'engagement contractuel est expressément mentionné à l'article 26-2 de la directive de 1995 : " Un transfert ou un ensemble de transferts peuvent également être autorisés lorsque le responsable du traitement offre des garanties suffisantes à l'égard de la protection de la vie privée et des libertés et droits fondamentaux de la personne, garanties qui peuvent résulter notamment de clauses contractuelles appropriées. " Ces dispositions devraient permettre à de grandes multinationales d'exporter librement leurs données et les transférer partout dans le monde, même dans des pays où la protection n'est pas équivalente, sous réserve de " clauses contractuelles appropriées " ;

– **engagement unilatéral** dans certaines situations particulières : cas d'une multinationale ayant des établissements dans le monde entier.

La question qui demeure concernant ce droit " mou " progressivement adopté par les acteurs est celle de l'éventuelle validation de ces normes juridiques par une autorité indépendante. Faut-il une forme de reconnaissance publique de ces approches pour qu'elles soient réellement efficaces ? La réponse minimale est celle de faire réaliser une étude, un inventaire des solutions proposées et de rendre des conclusions publiques. À l'inverse, l'approche maximaliste consisterait après examens et expertises à donner un agrément, homologuant le code, l'entreprise ou le projet. Cette solution s'éloigne largement de l'autorégulation pour mettre en place des pratiques administrées peu cohérentes avec le monde de l'Internet ; elle nécessiterait de plus des moyens substantiels de contrôle et d'audit des agréments ainsi délivrés.

Une solution intermédiaire semble préférable : elle consiste à ce que, volontairement, les acteurs privés se soumettent à une reconnaissance de conformité aux principes de la loi nationale ou du règlement sous le contrôle d'un organisme indépendant. Cette reconnaissance n'aurait pas de réelles conséquences juridiques mais elle serait un gage de l'attention des acteurs aux questions de vie privée et un élément de la crédibilité de ceux-ci auprès des utilisateurs.

Le contrôle de cette reconnaissance pourrait se faire, soit *a priori* ou en cours de projet à la demande des acteurs, soit *a posteriori* en cas de plaintes. Il ne s'agirait, en aucun cas, de fixer un cadre de référence, de façon autoritaire, mais d'apporter, à la demande des acteurs, une reconnaissance semi-officielle de leurs engagements, par exemple sous la forme d'un label.

Il est clair que dans le cas français, la CNIL a vocation à exercer un tel rôle, d'autant plus qu'elle pourrait toujours utiliser ses autres prérogatives pour vérifier, de sa propre initiative, la conformité effective des pratiques de l'entreprise aux engagements pris.

Les dispositifs techniques

Ces dispositifs, de type P3P (voir *supra*), sont fort utiles pour assurer la protection de la vie privée de l'utilisateur en faisant de celui-ci le pilote de l'utilisation ou de la diffusion de ses données personnelles sur le réseau : l'utilisateur paramètre son ordinateur selon sa propre sensibilité et l'utilisation de ses données personnelles par les sites visités ou par le fournisseur d'accès doit suivre les choix indiqués.

Divers produits existent et offrent deux types de paramétrage : soit le " opt-in " par lequel

l'internaute indique de façon positive s'il accepte la collecte de ses données, son abstention interdisant celle-ci ; soit le " opt-out " où il est offert à l'internaute de sortir de la collecte, son silence l'autorisant.

Beaucoup de débats ont lieu autour de ces techniques : la formule " d'opt-out " semble plus réaliste pour le développement du commerce électronique et de nature à limiter les sollicitations permanentes de l'utilisateur dont il risque de se lasser. La formule " opt-in " offre cependant des avantages en termes de création de communautés virtuelles commerciales dans lesquelles l'internaute entrerait délibérément en échange de services particuliers.

En tout état de cause, ceci n'est pas du ressort de la loi ou du règlement mais relève de l'autorégulation. Le rôle de la CNIL pourrait cependant être d'alerter et d'informer le consommateur sur la qualité de chacun des produits proposés.

Les techniques d'anonymisation

L'anonymat est une question complexe, au carrefour d'intérêts éthiques, économiques et politiques : l'individu veut se promener et agir librement comme dans sa vie quotidienne réelle, les entreprises veulent l'identifier pour mieux le servir, les autorités répressives ont besoin de retrouver les coupables d'infractions et donc de les identifier.

L'équation est facile à poser, moins facile à résoudre. Quelques remarques cependant peuvent éclairer le débat :

– l'individu doit pouvoir rester anonyme sur le réseau pour aller et venir, faire des paiements, envoyer des lettres... Un sondage récent organisé aux États-Unis concluait que 82 % des utilisateurs sont favorables à l'anonymat, mais seulement 52 % pour les paiements anonymes ;

– cet anonymat peut se faire au moyen de la pseudonymisation ;

– cet anonymat ne saurait cependant interdire de retrouver l'identité des personnes si nécessaire ; la " netétiquette " inclut d'ailleurs le non-anonymat et l'on verra les besoins de la police et de la justice en cas d'enquête (voir *infra* quatrième partie).

L'article 8 de la proposition de " directive sur un cadre commun pour les signatures électroniques " dispose d'ailleurs que le signataire d'un certificat peut demander de substituer un pseudonyme à son nom dans le certificat mais consent à ce que ses données soient transmises aux pouvoirs publics qui en font la demande.

Les logiciels d'anonymisation devraient être autorisés et permettre l'accès et le paiement anonymes sous réserve de ne pas interdire l'identification de l'émetteur du message en cas d'enquête judiciaire. Dans cette situation devrait être ainsi fournie, en tant que de besoin, aux autorités de police l'identité des utilisateurs (voir *infra* quatrième partie). Si l'on souhaitait aller au-delà et interdire la fourniture ou l'utilisation de services ou de produits offrant un anonymat total, c'est-à-dire ne permettant pas la traçabilité des utilisateurs, une loi serait nécessaire.

L'information

Toutes les études qui s'intéressent au respect de la vie privée sur les réseaux s'accordent sur un point : la nécessité d'une éducation des utilisateurs à partir de la connaissance des usages et des risques ; cette éducation dépasse la seule information de l'individu ; elle se traduit par un processus de prise de décision de l'utilisateur responsable qui va arbitrer lui-même le mode de protection de ses données, soit par des dispositifs techniques d'autoprotection, soit par un dépôt de plaintes... Les acteurs privés et notamment les organismes professionnels peuvent jouer un rôle en ce sens ; l'organisme de corégulation (voir *infra* quatrième partie) pourrait également y

contribuer ; la CNIL évidemment doit participer à cette mission d'éducation.

Évolution du rôle de la CNIL

À l'issue de l'analyse menée plus haut, il semble clair que le rôle de la CNIL doit évoluer et s'adapter à ces nouvelles techniques de régulation de la vie privée : il ne s'agit plus seulement d'appliquer la réglementation, mais d'accompagner de façon souple les mécanismes d'autorégulation dans un cadre international. Cette approche nécessite une réorientation du mode de fonctionnement de l'institution. La CNIL doit en effet, comme l'avait recommandé le rapport de M. Guy Braibant, renforcer son contrôle *a posteriori* (mise en œuvre des sanctions pénales prévues à l'article 24 de la loi du 6 janvier 1978) et se doter d'une compétence nouvelle d'expertise et de veille dans le domaine des nouvelles technologies afin :

– d'avoir un rôle de vigilance et d'information de l'utilisateur ;

– de " suivre " le respect par les acteurs de leurs engagements au titre de l'autorégulation : labelisation des codes de déontologie, contrats... ;

– de valider et de conseiller les utilisateurs par rapport aux dispositifs techniques ;

– de mener une action de concertation internationale avec les acteurs publics et privés.

La CNIL doit constituer un lieu de discussions et d'échanges sur ces questions de vie privée mais aussi être l'outil de recours et de sanction, avant l'intervention du juge.

Ces missions nouvelles nécessitent des personnels et des moyens adaptés et un mode de fonctionnement en réseau à l'image de l'Internet ; elles auront aussi pour conséquence de modifier profondément l'approche des problèmes à laquelle la CNIL était habituée.

Alors qu'aux États-Unis, certains (Center for technology and democraty, groupe de pression d'inspiration libérale) réfléchissent à la création d'un centre d'expertise indépendant sur la vie privé, il serait dommage que les difficultés d'évolution " culturelle " empêchent la CNIL de constituer celui-ci au plan français.

Conclusion

Le monde en réseau n'est pas symbole de vide juridique en matière de données personnelles ; cependant, la protection effective de celles-ci nécessite une action combinée de la puissance publique et des acteurs privés ; l'intervention du régulateur doit s'adapter à ce constat et s'enrichir d'un rôle de suivi des diverses pratiques d'autorégulation. Enfin, aucune solution nationale n'étant pleinement efficace, le dispositif de protection appelle une coopération internationale, entre États mais aussi entre acteurs privés.

Dans tous les cas, il convient d'être vigilant et de mener une action préventive ou répressive, à l'égard des contenus mais aussi des comportements ou pratiques.

Ceci est-il suffisant ? N'assiste-t-on pas au-delà des seuls traitements de données personnelles, à une remise en cause plus profonde de la personne humaine, de ses droits et de ses libertés, de son identité même ?

La réponse est difficile.

Les moteurs de recherche par leur puissance de traitement et le rapprochement qu'ils opèrent entre les fichiers peuvent mettre en place un système universel d'identification.

Les produits nouveaux de type " passeport " par lesquels un individu accepte de divulguer un

certain nombre de renseignements personnels (par exemple : nom, prénom, couleur des yeux...) pour faciliter sa navigation sur les réseaux sont aussi des moyens d'identification universelle.

Or l'identité virtuelle, en tant que telle, n'existe pas aujourd'hui : on ne peut être incriminé pour un vol de pseudonyme qui n'est qu'un vol d'informations non sanctionnable en tant que tel (sauf utilisation frauduleuse de ce pseudonyme).

Que dire de même des images d'une personne lorsqu'elles sont manipulées ou associées à des contextes contestables ? Le droit à l'image devrait permettre de se défendre ; mais *quid* de la création d'une identité virtuelle entièrement fausse portant le nom d'une personne réelle, agissant, parlant, communiquant mais sans liaison avec la personne réelle ? Où est le clone, où est la personne si les données de référence sont les mêmes ?

Ne faut-il pas dès lors repenser la protection de façon générale, **en réfléchissant à la question des droits de la personne virtuelle,** différents peut-être de ceux de la personne réelle ?

Comme le soulignait à la réunion de l'OCDE des 16 et 17 février 1998 consacrée à la vie privée, Stefano Rodota, président de l'Autorité pour la protection des données personnelles en Italie, l'enjeu actuel est celui de la " construction d'une citoyenneté électronique ". Comment la définir ? Il ajoutait que " les données personnelles sont un élément essentiel de celle-ci et que l'individu revendique aujourd'hui un droit à la libre construction de sa sphère privée ainsi qu'à la dignité humaine. "

Le rapport n'a pu réellement aborder ces questions qui dépassent le seul champ juridique et qui nécessitent une réflexion philosophique, politique et éthique. Il serait souhaitable de l'engager au plus vite afin de tenter de comprendre les changements important qui sont liés à la civilisation numérique.

Deuxième partie

Favoriser les échanges par une confiance accrue des acteurs

Le commerce électronique sur Internet, dont les volumes sont aujourd'hui encore modestes, de l'ordre de six milliards de francs pour l'Europe en 1997, connaît une forte croissance. Les analyses prospectives pour l'Europe l'évaluent à plus de 18 milliards de francs pour 1998, 42 milliards en 1999, 90 milliards en l'an 2 000. La grande variété des offres sur Internet, qu'elles concernent la vente de vin, d'automobiles, de livres, de disques, de logiciels, de voyages, de services financiers, etc, rencontre un succès croissant auprès des consommateurs. Ces derniers ont en effet la possibilité de mettre en concurrence des vendeurs répartis sur l'ensemble de la planète, à des conditions financières avantageuses. Internet permet des transactions sans intermédiaires et donc une réduction importante des coûts de distribution. Dans ce nouveau marché mondial, marqué par la globalisation et les ajustements concurrentiels immédiats, qui n'est pas sans rappeler le fonctionnement des marchés financiers, la concurrence entre acteurs sera vive et l'impératif de différenciation des offres absolu.

Toutefois, le succès rencontré par de nouveaux marchands électroniques tels " Amazon.com " (vente de livres) ou " Auto-by-tel " (vente de voitures) ne doit pas dissimuler le fait que cette nouvelle forme de commerce est encore largement dominée par les relations inter-entreprises et par des modalités plus traditionnelles de transaction : échanges " classiques " de données informatisées entre entreprises (EDI), ou ventes à distance " traditionnelles " (avec des commandes par courrier, téléphone, minitel ou maintenant Internet). Ainsi, le commerce inter-

entreprises représente aujourd'hui près de 70 % du commerce électronique sur Internet en Europe et 90 % en France, ce qui n'a rien d'anormal compte tenu de la place qu'occupe encore le minitel auprès des particuliers.

En fait, le commerce électronique sur Internet ne devrait connaître un véritable essor auprès des particuliers, malgré le caractère *a priori* attractif de certaines offres, que si certaines conditions sont réunies et ceci au plan mondial, compte tenu des caractéristiques transfrontières du réseau. Cette conviction ressort des diverses réflexions sur le sujet, notamment du rapport remis en janvier 1998 par M. Francis Lorentz au ministre de l'Économie, des Finances et de l'Industrie. Elle fait l'objet d'un large consensus chez les professionnels et dans les diverses enceintes internationales mobilisées sur ce sujet que ce soit dans le cadre de l'OCDE, à l'OMC, à la Commission des Nations unies pour le droit commercial international (CNUDCI), ou à la Commission européenne.

L'objectif principal consiste à insuffler plus de confiance dans une nouvelle forme d'échanges, encore entravée par des contraintes diverses. À celles d'ordre technique et économique liées à l'engorgement des réseaux, à l'insuffisance du nombre de terminaux équipés de logiciels de navigation accessibles à tous et à la relative insécurité des échanges, s'ajoutent d'autres formes de résistances, dont certaines tiennent à des obstacles psychologiques et juridiques, les deux étant fortement liés.

Comment contourner ces obstacles, lever les appréhensions aujourd'hui en partie légitimes des consommateurs, voire de certaines entreprises qui ne perçoivent pas encore les gains potentiels d'une présence sur l'Internet, ne serait-ce que pour assurer une promotion mondiale, à peu de frais, de leurs produits ou services ?

Il apparaît indispensable de sécuriser les échanges et de créer un cadre juridique transparent et rassurant pour les utilisateurs des réseaux. Plusieurs orientations devraient y contribuer significativement :

– la première priorité consiste à assurer un **cadre juridique sécurisant pour les consommateurs** offrant un niveau de protection comparable à celui applicable en Europe aux ventes à distance effectuées selon les méthodes classiques (chapitre I) ;

– tout aussi importante, est la reconnaissance de la valeur juridique des outils d'une transaction dans le monde virtuel d'Internet. La **signature et le message électroniques doivent tenir lieu d'écrit ou de signature manuscrite** pour apporter la preuve d'une transaction en cas de contestation, et permettre dans des conditions fiables et souples pour les usagers **l'identification d'une partie et l'authentification d'un message** (chapitre II).

La confidentialité des échanges assurée par le chiffrement des messages, sera aussi essentielle pour rassurer les acteurs. Le cadre légal de la cryptologie doit s'efforcer de trouver un juste équilibre entre les besoins des acteurs et les préoccupations de sécurité publique. Ceci suppose une **libéralisation des instruments de cryptologie**, mais aussi la mise en place d'un dispositif de recouvrement des clés de chiffrement adéquat et si possible harmonisé au plan international (chapitre III).

Le commerce électronique ne se développera pas s'il remet en cause la souveraineté des États au plan fiscal, et s'il engendre des distorsions de concurrence et des risques pour le consommateur. Sans pouvoir procéder dans les délais impartis à l'examen complet, sans doute nécessaire, de cette délicate question, des indications sont données sur les principales voies à explorer en vue **d'adapter la fiscalité au commerce électronique** (chapitre IV).

Enfin, **l'architecture des noms de domaine**, véritable " colonne vertébrale " de l'Internet, doit

être améliorée dans le cadre d'une réflexion internationale **en veillant à une meilleure articulation avec le droit des marques** (chapitre V).

La mise en œuvre de ces priorités suppose de clarifier le cadre juridique actuel, en grande partie applicable à l'Internet, et de procéder à certaines adaptations. Il est impératif d'associer les professionnels à leur mise en œuvre et de les encourager à mettre en place des dispositifs d'autorégulation. En outre, le caractère transnational de l'Internet rend nécessaire l'harmonisation des solutions au plan international, notamment par un nouveau cadre conventionnel offrant la garantie qu'un socle minimal de principes sera partagé par la communauté mondiale des utilisateurs.

Chapitre 1

Transactions électroniques et protection du consommateur

Assurer aux consommateurs une protection d'un degré comparable, lors de transactions dématérialisées, à celle dont ils jouissent à l'occasion de ventes à distance classiques, constitue un objectif prioritaire. Cette protection ne constitue pas seulement un objectif en soi. Elle sera sur Internet l'un des moyens offerts aux entreprises de différencier leur offre, dans un contexte de concurrence internationale croissante, et de tirer le bénéfice de véritables avantages comparatifs. Le haut niveau de protection offert aux consommateurs en France – et bientôt en Europe lorsque la directive du 20 mai 1997 relative à la protection des consommateurs en matière de contrat à distance sera transposée –, constitue donc un véritable atout pour séduire des consommateurs très sensibles au degré de protection qui leur est offert.

Dans l'ensemble, le dispositif actuel de protection du consommateur est applicable à l'Internet, il conviendra toutefois de procéder à quelques clarifications ou adaptations au plan national et surtout international.

Certaines orientations pourraient en premier lieu être privilégiées en France. Tout d'abord, des ambiguïtés doivent être levées concernant le régime juridique de la publicité, et la nature d'une transaction électronique, qui est une vente à distance et ne constitue qu'exceptionnellement une opération de démarchage (dans le cas du " spamming "). Des adaptations du cadre juridique sont en outre nécessaires pour clarifier le champ d'application de certaines législations spécifiques – concernant notamment la publicité sur l'alcool et l'obligation d'emploi de la langue française –, mieux identifier les parties et assurer une information transparente des consommateurs, qui doivent être mis à même de manifester clairement leur consentement. Il apparaît enfin indispensable d'associer les professionnels et de favoriser le mise en place rapide de codes de conduite et de contrats types.

Deux approches destinées à mettre en place les instruments d'une protection internationale des consommateurs doivent en second lieu être combinées. La première orientation consiste à définir quelques principes fondamentaux de protection du consommateur : les transactions sur Internet s'effectueront pour partie avec des commerçants non européens, d'où l'intérêt de négocier une convention internationale relative aux transactions électroniques, s'inspirant des principes retenus par la directive européenne du 20 mai 1997 sur les ventes à distance. La seconde orientation concerne l'adaptation des règles de conflit de loi relatives à une transaction électronique. Il est probable que le droit applicable aux transactions commerciales relèvera encore largement d'une base nationale dans les années à venir. Il importe dès lors d'adapter les règles de conflit de lois existantes, notamment celles résultant de la convention de Rome du 19 juin 1980, en tenant compte de la destination des messages par le jeu d'un faisceau d'indices,

afin de préserver un juste équilibre entre l'impératif de protection des consommateurs et la nécessité de ne pas imposer des contraintes irréalistes aux entreprises.

Deux autres aspects significatifs du régime des transactions électroniques et de la protection des consommateurs ne sont pas abordés dans ce chapitre. Il s'agit tout d'abord de la protection des données personnelles face au développement, parfois transfrontière, de fichiers et de bases de données. Ce point a été traité dans la première partie du rapport. Une autre question est relative à la sécurisation des paiements et des services financiers, ces derniers n'étant pas couverts par la directive précitée sur la vente à distance (une directive sur les services financiers est en préparation). Ce problème ne fait pas l'objet d'un traitement distinct dans le cadre de cette étude. Il est traité dans trois rapports récents, auxquels il est recommandé de se référer . Si la sécurisation des paiements paraît essentielle pour permettre un réel essor du commerce électronique, les réponses à ce besoin relèvent très largement de la normalisation, de solutions techniques et organisationnelles. Il importe avant tout de mettre à la disposition des consommateurs des moyens de paiement fiables. Des difficultés juridiques ont toutefois été identifiées .

Assurer en France la transparence et la sécurité juridique des transactions électroniques

Une transaction électronique est généralement précédée d'une publicité. La publicité est aujourd'hui la première source de revenus directement liée à Internet (conception de sites, référencement par des moteurs de recherche). Il apparaît donc primordial de lever certaines ambiguïtés relatives à son régime juridique sur Internet afin de protéger les consommateurs et de ne pas entraver le développement de cette activité. Les consommateurs et les professionnels ont aussi naturellement besoin de connaître le cadre juridique de la transaction qui suivra la publicité, et notamment de savoir dans quels cas la vente à distance en ligne sera qualifiée de démarchage.

Au-delà de certaines **clarifications,** il semble en fait nécessaire dans un souci de clarté et de transparence à l'égard des consommateurs de procéder à certaines **adaptations,** afin d'encadrer les modalités d'information et d'acceptation d'une offre et d'assurer une meilleure identification des professionnels. Aussi utiles soient-elles, ces adaptations réglementaires resteront néanmoins insuffisantes sans le concours des professionnels, qu'il convient d'associer à cet effort de sécurisation des transactions.

Lever les ambiguïtés relatives au régime de la publicité sur Internet

La publicité sur Internet, " échappe aux schémas de la publicité classique et soulève de nombreuses questions juridiques " . Ces difficultés sont principalement de deux ordres : dans quelle mesure un message promotionnel sur Internet peut-il-être qualifié de publicité ? Quels sont les textes relatifs à la publicité qui sont applicables à Internet ?

Des formes de publicité très variées

La publicité ne fait pas l'objet d'une définition générale en droit français. Ses critères sont variables en fonction des supports concernés . Une définition (très) générale est en revanche donnée par la directive no 84-450/CEE du 10 septembre 1984 relative à la publicité trompeuse : " Toute forme de communication faite dans le cadre d'une activité commerciale, industrielle, artisanale ou libérale dans le but de promouvoir la fourniture de biens ou de services, y compris de biens immeubles, les droits et obligations. " Une définition très proche, qui ne concerne que la publicité télévisée, est donnée à l'article premier de la directive télévision sans frontières no 89-

552 modifiée en 1997.

Au total, il semble possible de retenir au moins deux critères : la finalité du message, critère déterminant, dont l'objet est d'assurer la promotion d'un bien, d'un service, d'une entreprise et la destination du message qui doit être adressé au public. Un troisième critère, l'existence d'une contrepartie, est prévu par les textes sur la publicité télévisée qui obéit à un régime très strict (décret précité du 27 mars 1992 en France). Ce critère, qui n'est pas général, peut toutefois s'avérer utile pour distinguer certaines formes peu transparentes de publicité (voir, *infra*, le problème de l'identification de la publicité).

Dans ces conditions il est possible d'identifier – sans que cette liste soit exhaustive compte tenu de l'évolution des techniques et des pratiques – plusieurs formes de publicité sur Internet :

– les **bandeaux publicitaires** qui sont affichés généralement en haut ou en bas de l'écran. En cliquant sur le bandeau, l'utilisateur peut obtenir des informations complémentaires de caractère promotionnel ou accéder à un forum de discussion qui pourra avoir, le cas échéant, un caractère publicitaire ;

– les **messages interstitiels** : il s'agit de messages publicitaires qui s'affichent très brièvement en plein écran entre les pages de présentation d'un site ;

– le **courrier électronique** : la messagerie électronique permet d'adresser à une personne ou à une liste de personnes des messages. Lorsqu'ils ne sont pas personnalisés et ne présentent donc pas le caractère d'une correspondance privée, les messages électroniques peuvent présenter le caractère d'une publicité (voir spamming). En revanche, ne relèverait pas d'une telle qualification l'envoi à un destinataire unique d'un courrier, même s'il revêt un caractère promotionnel ;

– les **forums de discussion** : ce sont des espaces de discussion thématiques fonctionnant en différé, qui mettent en relation des utilisateurs partageant les mêmes centres d'intérêt. En pratique, l'internaute sélectionne préalablement des forums et reçoit des messages adressés par des membres du groupe (il peut aussi en envoyer). Si le groupe est à diffusion large, il y aura indéniablement message public et donc, le cas échéant, publicité si ce message a un objet promotionnel ;

– les **sites Web** : un site Web constitue sans doute la forme la plus développée de publicité à ce jour sur Internet. Un tel site permet de créer une véritable vitrine virtuelle présentée dans le monde entier, identifiée par un nom de domaine et référencée par des annuaires (moteurs de recherche). Le caractère public du site est manifeste. Le caractère promotionnel sera lui plus difficile à identifier et notamment à distinguer d'un contenu éditorial. Cette difficulté a ainsi conduit les experts comptables à renoncer en 1997 à créer un site d'information sur leurs activités de crainte que cette initiative ne soit qualifiée de démarchage publicitaire ;

– le **référencement d'un site par un moteur de recherche** peut aussi constituer une forme de publicité, à l'image d'un catalogue ou d'un annuaire, notamment si l'indexation est payante. Certains moteurs de recherche, tels Yahoo ! qui revendique la qualité de " média de masse ", en tirent l'essentiel de leurs ressources.

Ainsi, c'est fréquemment qu'un message sur Internet sera qualifié de publicité. Il importe en conséquence de sensibiliser les utilisateurs d'Internet sur ce point, mais aussi d'apporter des précisions sur les conséquences juridiques liées à cette qualification.

Des incertitudes sur les législations applicables

Une difficulté traitée plus loin concerne la législation applicable à un message publicitaire émis de l'étranger : il s'agit d'un problème très sensible de droit international privé, car une publicité licite dans un pays peut être prohibée dans un autre État (voir *infra*, pour l'application de la loi pénale, la quatrième partie de ce rapport). Les difficultés particulières liées à l'application de la loi sur l'emploi de la langue française sont aussi abordées plus loin (voir *infra*, les développements sur l'information des consommateurs et sur la loi applicable).

À supposer que les législations communautaire et nationale s'appliquent, il reste à déterminer le contenu de la réglementation de la publicité sur Internet. À la différence de certaines formes de publicité qui font l'objet d'une réglementation spécifique (notamment la publicité télévisée), le cas des services en ligne n'a pas fait l'objet d'un traitement réglementaire spécifique. **Il ne semble pas nécessaire de préconiser une réglementation de la publicité spécifique à l'Internet.** En revanche, certaines clarifications concernant des législations en vigueur ayant vocation à s'appliquer à l'Internet pourraient utilement être apportées.

? *Certains principes, de portée générale, s'appliquent sans conteste à Internet*

Ces principes sont notamment l'interdiction de la publicité trompeuse, l'encadrement de la publicité comparative et la transparence de la publicité.

La **publicité trompeuse** est interdite par l'article 2 de la directive du 10 septembre 1984 précitée qui en donne une définition large : " Toute publicité qui, d'une manière quelconque, y compris sa présentation, induit en erreur ou est susceptible d'induire en erreur les personnes auxquelles elle s'adresse ou qu'elle touche ou qui, pour ces raisons, porte préjudice ou est susceptible de porter préjudice à un concurrent. " L'article L. 121-1 du code de la consommation, interdisant la publicité trompeuse, a été maintenu à l'issue du délai de transposition de la directive, dès lors qu'il assurait une protection étendue des consommateurs, compatible avec le texte de la directive (Crim. 27 mars 1996, Bull. Crim. no 139). Il interdit toute publicité trompeuse sous quelque forme que ce soit. En France, la publicité trompeuse est réprimée pénalement. Le délit est constitué dès lors que la publicité est reçue en France. Le responsable de l'infraction est l'auteur pour le compte duquel la publicité a été diffusée (article L. 121-5 du code de la consommation). Un fournisseur d'accès ou d'hébergement ne pourra donc être poursuivi que sur le fondement de la complicité.

L'encadrement de la **publicité comparative** a aussi vocation à s'appliquer à l'Internet. Cette forme de publicité, également sanctionnée pénalement, est désormais encadrée par la directive sur la publicité trompeuse qui a été modifiée à cet effet en 1997 (directive 97/55). Elle retient une définition très large de la publicité comparative : " Toute publicité qui, explicitement ou implicitement, identifie un concurrent ou des biens ou services offerts par un concurrent. " Cette directive n'a pas encore fait l'objet d'une transposition. Il conviendra de veiller à cet occasion à ce que les services en ligne soient couverts par le champ d'application de la législation. Aujourd'hui, la publicité comparative est admise mais sous certaines conditions. Il est interdit de faire figurer ce type de publicité sur certains supports (emballages, factures, titres de transport, moyens de paiement, billets d'accès à des spectacle). Il n'apparaît manifestement pas souhaitable d'inclure les réseaux numériques dans cette liste des supports interdits. Il faut aussi souligner que l'obligation actuelle posée à l'article L. 121-12 du code de la consommation fait obligation à l'annonceur de communiquer l'annonce comparative aux concurrents concernés " avant toute diffusion ". Cette formulation n'est pas très heureuse. Il serait préférable de l'interpréter ou de la modifier à l'avenir comme imposée " avant toute mise à disposition du public ".

L**'obligation d'identification de la publicité**, enfin, paraît essentielle. En France, l'article 43 de la loi du 30 septembre 1986 relative à l'audiovisuel, qui s'applique aux services en ligne, dispose

que " les messages publicitaires diffusés par les services mentionnés au présent article doivent être présentés comme tels ". Cette obligation doit être maintenue et rendue applicable à toute communication au public.

Il faut toutefois souligner qu'une telle obligation sera difficile dans certains cas à faire appliquer, dans le cas par exemple d'un référencement payant sur un moteur de recherche. Mais l'exigence de loyauté doit primer. L'article 11 du code international des pratiques loyales en matière de publicité de la chambre de commerce internationale retient d'ailleurs cette obligation d'identification : " La publicité doit pouvoir être nettement distinguée comme telle, quels que soient la forme et le support utilisés ; lorsque le message publicitaire est diffusé dans des médias qui comportent également des informations ou des articles rédactionnels, il doit être présenté de façon que son caractère publicitaire apparaisse instantanément. " En conséquence, les annonceurs anglais membres de l'Advertising Standards Authority (ASA), équivalent du Bureau de vérification de la publicité (BVP) français, mentionnent la nature publicitaire des sites.

? *Le champ d'application de certaines réglementations spécifiques est plus incertain*

Des législations particulières (sur le tabac, l'alcool, les médicaments, etc.), antérieures au développement de l'Internet, sont parfois d'interprétation délicate. Reflet de conceptions culturelles et sociales divergentes, ce type de législation est très variable selon les États. En respectant les standards du pays d'émission, un annonceur étranger respectera le plus souvent au moins deux des trois principes généraux rappelés (publicité trompeuse et identification, la publicité comparative obéissant à des régimes plus variables). En revanche, les réglementations spécifiques souvent mal connues risquent de ne pas être appliquées.

Dans certains cas, il n'est pourtant pas douteux que ces législations, fortement marquées en France par des préoccupations de santé publique, s'appliquent à l'Internet. Il en va ainsi des dispositions législatives prohibant la publicité en faveur du **tabac**. L'article 2 de la loi du 10 janvier 1991 dispose que " toute propagande ou publicité, directe ou indirecte, en faveur du tabac ou des produits du tabac ainsi que toute distribution gratuite sont interdites. Ces dispositions ne s'appliquent pas aux enseignes des débits de tabac, ni aux affichettes disposées à l'intérieur de ces établissements... " Une directive devrait très prochainement consacrer les mêmes principes.

Il en va de même pour le régime de la publicité sur les **médicaments**, très encadré et, dont le champ d'application est très large. Constitue en effet une publicité pour des médicaments à usage humain, selon les dispositions de l'article L. 551 du code de la santé publique, " toute forme d'information, y compris le démarchage, de prospection ou d'incitation, qui vise à promouvoir la prescription, la délivrance, la vente ou la consommation de ces médicaments, à l'exception de l'information dispensée, dans le cadre de leurs fonctions, par les pharmaciens gérant une pharmacie à usage intérieur ".

D'autres législations sont d'interprétation plus délicate. Il en va par exemple ainsi de la publicité sur **l'alcool**, qui obéit à un régime moins strict que celui du tabac. L'article L. 17-4 du code de la santé publique, issu de la loi du 10 janvier 1991 relative à la lutte contre l'alcoolisme, donne d'une part une liste limitative des supports sur lesquels la publicité en faveur de l'alcool est autorisée sous certaines conditions – presse écrite, radio, affiches ou enseignes –, et d'autre part, admet certains types de messages : les messages et circulaires commerciales, catalogues et brochures envoyés par les fabricants, producteurs et négociants.

Il convient donc d'apprécier si une publicité sur Internet entre dans cette liste limitative des supports et des messages autorisés. Il ressort de l'examen des travaux parlementaires que le

législateur souhaitait inclure dans cette liste les messages adressés par minitel ou par téléphone. Est-il dès lors possible d'assimiler Internet au minitel et de considérer que l'interdiction de la publicité en faveur de l'alcool, qui pour l'essentiel concerne la télévision, ne vaut pas pour les services en ligne ? Cette interprétation paraît raisonnable, mais gagnerait à une consécration législative levant tout doute. Internet ne constituant pas à proprement parler un support (ce point est traité dans la cinquième partie de ce rapport), il conviendrait d'inclure les messages en ligne dans la liste des messages sur l'alcool autorisés. Cet exemple montre la nécessité de déterminer plus clairement l'applicabilité des législations spécifiques sur la publicité aux services en ligne, lorsque le champ d'application de l'interdiction n'est pas général (comme dans le cas du tabac).

L'importance de règles déontologiques en matière de publicité

Au-delà des clarifications du cadre législatif et réglementaire, l'autorégulation des professionnels paraît particulièrement importante dans ce domaine. Les efforts accomplis pour adapter les pratiques publicitaires aux réseaux numériques seront d'autant plus fructueux qu'ils seront coordonnés, notamment au sein de l'Alliance européenne pour l'éthique en publicité qui regroupe les organismes d'autodiscipline de vingt-deux pays.

Il serait opportun que certains principes déontologiques proposés soient rapidement mis en œuvre . On citera notamment : l'engagement des annonceurs à ne recourir qu'à une publicité loyale, décente et bien identifiée les autorisant à se prévaloir d'un label de qualité, à l'image de ceux délivrés par le " Better Business Bureau " aux États-Unis ; l'identification par une icône représentant le drapeau de l'État des consommateurs concernés par une offre commerciale (ce signe distinctif constituerait un critère déterminant pour apprécier, en cas de conflit de loi, s'il y a lieu d'appliquer la législation française : voir *infra*, les développements relatifs aux critères à prendre dans le cadre d'une convention internationale) ; la possibilité offerte aux internautes souhaitant se protéger contre l'envoi intempestif de messages publicitaires (" spamming ") de s'inscrire, par messagerie électronique, sur une liste Robinson " stop publicité ", du type de celle mise en place par le Syndicat des entreprises de vente par correspondance et à distance, pour recenser tous les consommateurs désireux de ne plus recevoir de documents promotionnels.

Clarifier la qualification juridique d'une transaction sur Internet : vente à distance avec ou sans démarchage ?

Cette question controversée conditionne le régime juridique de la transaction, le degré de protection offert aux consommateurs et les sanctions encourues par un professionnel négligent.

Une transaction sur Internet relève du régime de la vente à distance mais le droit de rétractation n'est qu'en partie applicable à l'Internet

Le champ d'application du régime de la vente à distance est très large. Il convient de se référer sur ce point à un texte important, qui a explicitement vocation à s'appliquer aux services en ligne : la directive 97/7/CE du 20 mai 1997 relative à la protection des consommateurs en matière de contrat à distance. Deux définitions données à l'article 2 de cette directive, qui n'a pas encore été transposée en droit national sont éclairantes. Par " contrat à distance ", la directive entend " tout contrat concernant des biens ou services conclu entre un fournisseur et un consommateur dans le cadre d'un système de vente ou de prestations de services à distance organisé par le fournisseur qui, pour ce contrat, utilise exclusivement une ou plusieurs techniques de communication à distance jusqu'à la conclusion du contrat elle-même ". Et par " technique de communication à distance ", " tout moyen qui, sans présence physique et simultanée du fournisseur et du consommateur peut être utilisé pour la conclusion du contrat entre les parties ".

Dès lors, les grands principes posés par cette directive, d'inspiration très similaire au droit de la consommation français, seront applicables aux transactions dématérialisées. Ces principes concernent pour l'essentiel : l'information préalable du consommateur, la confirmation de certaines informations essentielles par écrit ou sur un autre support durable, les modalités d'exécution du contrat, les garanties en cas de paiement par carte, les garanties offertes en cas d'envoi de fournitures non commandées, les systèmes de recours ou de réclamation, le droit de rétractation pendant sept jours.

Cette dernière disposition revêt une importance particulière. Aujourd'hui, le délai de rétractation est applicable en France, en vertu de l'article L. 121-26 du code de la consommation, aux seuls contrats portant sur les produits et non sur les services : " Pour toute opération de vente à distance, l'acheteur d'un *produit* dispose d'un délai de 7 jours francs à compter de la livraison de sa commande pour faire retour de ce produit au vendeur pour échange ou remboursement, sans pénalités à l'exception des frais de retour. "

La directive " vente à distance " retient une approche plus large incluant les services. Toutefois l'exercice de ce droit ne doit pas conduire à permettre au consommateur de bénéficier d'un service sans en acquitter le prix, par exemple en cas de téléchargement de logiciels ou d'œuvres littéraires et artistiques retournés au vendeur après reproduction. Aussi, la directive prévoit que, sauf si les parties en ont convenu autrement, le droit de rétractation ne peut pas s'exercer dans certains cas. Elle mentionne : les contrat de fournitures de services dont l'exécution a commencé avant la fin du délai de sept jours ; la fourniture d'enregistrements audio ou vidéo ou de logiciels informatiques *descellés* par le consommateur ; la fourniture de journaux, de périodiques ou de magazines. Il semble que la précision relative au descellement des logiciels et enregistrements signifie que seule est visée la livraison physique de ces produits. Dans le cas des services en ligne, il convient donc semble-t-il de se référer à l'exception concernant les services dont l'exécution a commencé avant la fin du délai de sept jours après le jour de la conclusion du contrat. En pratique, ne seraient donc couverts par le droit de rétractation que d'une part, les biens commandés en ligne mais livrés physiquement à l'exclusion des enregistrements et logiciels descellés et, d'autre part, les services dont la consommation n'a pas commencé avant l'expiration d'un délai de sept jours après la conclusion du contrat (par exemple, la prestation d'une agence de voyage).

Il est dans ces conditions souhaitable **d'inciter à l'utilisation de la possibilité offerte par la directive de prévoir un droit de rétractation par voie contractuelle dans les cas où le droit de rétractation ne peut s'exercer** (un tel droit peut s'avérer utile en cas de recours, par exemple, à des services de dépannage ou d'assistance en ligne)**. Lorsque le droit de rétractation ne s'applique pas, il apparaît au moins nécessaire que les consommateurs en soient dûment informés**.

Retenir la qualification de démarchage à titre exceptionnel

Le régime du démarchage à domicile relève des articles L. 121-23 et suivants du code de la consommation. Certaines de ces dispositions seront manifestement peu adaptées à des transactions en ligne. Il en va ainsi de l'obligation de remettre un écrit comportant des mentions obligatoires et de l'interdiction de recevoir du client un paiement avant l'expiration d'un délai de réflexion de sept jours. En outre, l'article 2 bis de la loi n° 89-421 du 23 juin 1989 prévoit que " à la suite d'un démarchage par téléphone ou par tout moyen technique assimilable, le professionnel doit adresser au consommateur une confirmation écrite de l'offre qu'il a faite. Le consommateur n'est engagé que par sa signature ".

Lorsque le client a l'initiative de la transaction, il n'est pas douteux que la qualification de démarchage doit être écartée, même s'il a pris connaissance de l'offre commerciale par un

message adapté à ses préférences, ce qui sera fréquent avec le développement de la navigation en mode " push " (voir *supra* première partie). En revanche, lorsque le message a été reçu dans des conditions comparables à une communication téléphonique non sollicitée, la qualification de démarchage pourrait le cas échéant être retenue. Il en irait ainsi dans le cas du " spamming ", pratique très contestée qui consiste en l'envoi massif de messages publicitaires non sollicités.

Qualifier le " spamming " de démarchage aurait un caractère dissuasif très opportun compte tenu des sanctions retenues par la loi. Les infractions à la réglementation sur le démarchage sont en effet sanctionnées pénalement par des peines d'emprisonnement de un mois à un an et/ou par une amende de 1 000 à 20 000 francs.

Les conséquences pénales d'un démarchage irrégulier et la nature d'une offre commerciale sur Internet conduisent néanmoins à préconiser qu'une interprétation stricte de la notion de démarchage soit retenue pour la qualification des ventes à distance sur le réseau.

S'assurer que les consommateurs ont été bien informés et ont manifesté clairement leur consentement

L'information loyale de l'acheteur constitue l'un des fondements du droit de la consommation et une priorité sur Internet. Si l'on s'en tient au droit national et communautaire, il serait pour le moins impropre d'évoquer la notion de vide juridique. La directive du 20 mai 1997 sur la vente à distance, comme on l'a vu, est très détaillée sur ce point. Elle dresse un inventaire complet des informations dont le consommateur doit bénéficier et précise que ces informations doivent être loyales : le but commercial doit apparaître sans équivoque et les informations doivent être fournies de manière claire et compréhensible par tout moyen adapté à la technique de communication à distance utilisée. Le droit français de la consommation en vigueur offre de même un haut niveau de protection sur ce point : identification de l'entreprise, information sur les caractéristiques du produit, sur les prix, sur les conditions de vente.

Quelques adaptations des dispositifs en vigueur pourraient néanmoins être envisagées pour tenir compte des spécificités d'une transaction électronique.

Encadrer les modalités d'information lors de la prise de commande

Le Conseil national de la consommation a bien mis en lumière dans son rapport précité de 1997, à l'examen des pratiques de nombreux sites commerciaux, la fréquence des défaillances dans l'information sur les conditions de vente et sur les modalités de cette information.

Or, il importe que l'acheteur soit informé correctement dès le début du processus de commande, et qu'il manifeste clairement avoir pris connaissance des conditions de l'offre commerciale. Le processus d'acceptation d'une offre devrait comporter des phases bien distinctes afin de s'assurer que le consommateur a donné son consentement de manière claire et transparente. À chaque étape de la prise de commande, l'acheteur devrait manifester son acceptation. Deux grandes phases pourraient être distinguées.

Tout d'abord, une phase d'information claire et synthétique, sans que les points mentionnés puissent faire l'objet d'un renvoi à des conditions générales de vente par un lien hypertexte optionnel :

– information sur le produit ou le service sélectionné et sa garantie ;

– information sur le prix total du produit ou du service ;

– information sur l'entreprise (voir *infra*) ;

– information sur les conditions de vente, la loi applicable au contrat et le tribunal compétent ;

– information sur le délai de réflexion.

Ayant pris connaissance de ces informations, le consommateur pourrait décider de passer à la phase d'acceptation de l'offre, comportant elle-même plusieurs étapes :

– acceptation de l'offre, avec rappel des caractéristiques du produit ou du service ;

– acceptation du prix et des modalités de paiement ;

– acceptation des autres conditions du contrat ;

– manifestation finale du consentement.

Il serait souhaitable d'imposer que la manifestation finale du consentement prenne la forme soit d'une confirmation par courrier électronique avec une obligation de conservation du message, soit au moins de deux clics distincts, sur deux boutons séparés : le premier sur l'icône " J'accepte l'offre ", le second étant précédé d'une mention du type " Confirmez-vous bien votre commande ? ". Ainsi, le risque d'une manipulation par inadvertance serait limité. L'importance pratique de ce dispositif prend toute son importance si l'on se trouve dans l'un des cas où le droit de rétractation n'est pas applicable (voir *supra*). La dernière mention pourrait rappeler deux ou trois points essentiels : la loi applicable à la transaction, l'information sur l'existence d'une garantie et d'un droit de rétractation.

Informer les consommateurs concernés dans leur langue

Le droit communautaire s'efforce de parvenir à un équilibre entre deux préoccupations : la libre circulation des produits et la libre prestation de service d'une part, la protection du consommateur et de la santé d'autre part. En pratique, les solutions retenues pour ce qui concerne l'utilisation des langues sont très variables selon les secteurs concernés : pour les produits sensibles et notamment les médicaments et préparations dangereuses, le droit communautaire prévoit que la mise en vente est subordonnée à l'utilisation de la langue officielle de l'État membre. Dans d'autres cas, il est fait seulement référence à l'utilisation d'une langue facilement compréhensible par l'acheteur. Parfois, la question est renvoyée à la compétence des États membres. C'est le cas pour le régime des langues en matière de contrat à distance, renvoyé à la compétence des États membres par la directive du 20 mai 1997 précitée. Cette directive prévoit toutefois une exigence essentielle : que les informations préalables à la conclusion d'un contrat distance soient " fournies de manière claire et compréhensible par tout moyen adapté à la technique de communication à distance utilisée, dans le respect notamment des principes de loyauté en matière de transactions commerciales ".

Encadrer les modalités de l'offre commerciale en France n'aurait pas grand sens si les consommateurs français n'étaient pas informés dans leur langue . Il ressort toutefois des auditions que **l'application de la législation sur l'emploi de la langue française à l'Internet n'est pas aisée** . Il s'agit de la loi no 94-665 du 4 août 1994 relative à l'emploi de la langue française qui entend clairement protéger les consommateurs en imposant dans son article 2 l'emploi de la langue française " dans la désignation, l'offre, la présentation, le mode d'emploi ou d'utilisation, la description de l'étendue et des conditions de garantie d'un bien, d'un produit ou d'un service, ainsi que dans les factures et quittances ". Cet article précise ensuite que " les mêmes dispositions s'appliquent à toute publicité écrite, parlée ou audiovisuelle ". L'usage conjoint d'une ou plusieurs langues étrangères n'est jamais interdit, mais dans ce cas l'article 4 de la loi précise que la version française doit être " aussi lisible, audible et intelligible que la présentation en langue étrangère ".

Le décret no 95-240 du 3 mars 1995 précise les sanctions pénales qui sont prévues en cas de non-respect de ces prescriptions. Il s'agit d'amendes prévues pour les contraventions de la 4° classe et, en cas de condamnation, le juge peut faire application des articles 132-66 à 132-70 du code pénal qui permettent d'infliger une amende pour chaque produit ou document contrevenant à la loi. Dès lors qu'elle est sanctionnée pénalement, cette loi sera en théorie applicable par le juge français à tous les sites étrangers ne respectant pas l'obligation d'emploi de la langue française (voir *infra*, la quatrième partie sur la loi applicable aux infractions pénales). Il importe dès lors de prêter attention à son champ d'application. Un champ trop large conduirait à des violations systématiques de la loi par des sites étrangers, aujourd'hui très majoritairement en anglais, mais qui compte tenu de la nature transnationale du réseau, sont accessibles du territoire national. Il est probable qu'il en résulterait une absence de sanctions en pratique, à l'image de l'obligation de déclaration au procureur de la République prévue par l'article 43 de la loi du 30 septembre 1986, qui n'est ni respectée ni sanctionnée tant les contrevenants sont nombreux et l'obligation manifestement inadaptée.

Le régime des services en lignes au regard de l'obligation d'emploi de la langue française est mal compris. Ni la loi, ni une circulaire du 19 mars 1996 éclairant les modalités d'application de cette loi , n'apportent de précisions sur le traitement des services en ligne, à la différence du cas de la télévision qui est abordé. S'agissant de la publicité, il est précisé dans la loi elle-même que l'obligation d'emploi du français ne vaut pas pour les publicités dont la finalité est l'apprentissage d'une langue étrangère ou qui sont conçues pour être intégralement diffusées en langue étrangère. Un exemple est donné par la circulaire de 1996 : les publicités diffusées dans le cadre des programmes des chaînes étrangères reçus par câble ou satellite.

Le champ d'application de la loi paraît donc très large et inclure les services en ligne sans restrictions spécifiques. Dans le cas d'informations et notices relatives à des produits commandés en ligne mais livrés par les circuits traditionnels de la vente à distance cela ne présente pas de difficultés : il n'y a pas lieu d'opérer une distinction entre une commande en ligne et hors ligne, dès lors qu'il y a une livraison physique du bien susceptible de donner lieu à un contrôle en douane et à une vérification de l'étiquetage et, le cas échéant, des notices d'accompagnement, ce qui est prévu par les textes. Le problème est plus délicat en pratique pour ce qui concerne les services téléchargés en ligne. Un contrôle du respect de l'emploi de la langue française paraît dans ce cas bien difficile à opérer.

Des difficultés peuvent aussi survenir dans la transaction elle-même. La loi semble imposer l'emploi de la langue française pour toute transaction avec un consommateur français. Dès lors que les consommateurs français sont concernés par une offre commerciale à laquelle ils ont la faculté de souscrire, il paraît légitime d'imposer le respect de l'emploi de la langue française. En revanche si la transaction n'a pas été précédée d'une offre commerciale à destination des consommateurs français, qu'un consommateur a néanmoins décidé d'effectuer une commande en ligne, par exemple en anglais, ce qui est très fréquent aujourd'hui, est-il réaliste d'imposer le déroulement de la transaction en français ? Il est souhaitable de veiller au respect de l'emploi de la langue du consommateur, et il en va d'ailleurs de l'intérêt commercial bien compris des entreprises, si l'on se réfère aux pratiques dans les circuits de distribution classiques, ce qui nuance tout constat alarmiste. Mais le non- respect de cette obligation ne devrait sans doute être sanctionné que si le consommateur a été sollicité.

De même, il paraît difficile d'imposer l'emploi de la langue française pour la publicité lorsque les messages n'ont pas été conçus à destination des consommateurs français. Or, à la lecture de la loi, la liste des exceptions est très limitée et ne traite pas, on l'a vu, de la question des services en ligne. Une exclusion de la publicité télévisée conçue pour être diffusée à l'étranger est explicitement prévue par la loi. Ce raisonnement devrait aussi prévaloir pour les services en

ligne. En pratique, l'obligation d'emploi de la langue française ne devrait concerner que la publicité expressément destinée aux consommateurs français.

Au total, il apparaît **nécessaire de clarifier le champ d'application de la loi du 4 août 1994 et de retenir une solution réaliste s'agissant des services en ligne, tenant compte de la destination des messages.** Une modification de la loi en ce sens devrait permettre une mise en œuvre effective de l'obligation d'emploi de la langue française.

Renforcer l'identification des professionnels sur Internet

L'identification des parties, et notamment du vendeur ou du prestataire de service, peut être assurée par les **procédures de certification par un tiers** (voir *infra*, le chapitre sur le message et la signature électroniques). Mais ces procédures ne s'appliquent qu'en cas de transaction commerciale. Or, il paraît important que le consommateur puisse s'assurer, lorsqu'il consulte un site à caractère commercial, avant toute transaction, de l'identité de la personne ou de l'entreprise qui a la responsabilité de celui-ci.

Il est tout d'abord évident qu'en cas d'enquête, par exemple à l'initiative de la Direction générale de la concurrence, de la consommation et de la répression des fraudes, les autorités administratives et judiciaires doivent pouvoir **obtenir des bureaux d'enregistrement des noms de domaine (voir *infra*) les informations nécessaires à l'identification du titulaire du nom de domaine en cause** (nom ou raison sociale et adresse postale). En revanche, il paraît excessif d'exiger de ces bureaux qu'ils mettent ces informations en ligne, à la libre disposition du public . Seules les administrations nationales et la justice doivent y avoir accès.

L'idée de créer un " registre du commerce " européen, ou même mondial, des commerçants électroniques est parfois évoquée. Elle est séduisante mais peu réaliste. Compte tenu de la croissance très rapide du nombre des sites sur l'Internet, un tel registre paraît difficile à réaliser sur un plan technique. En outre, il entrerait en concurrence avec les annuaires professionnels (" pages jaunes ") qui commencent à se développer à l'initiative du secteur privé. Enfin, l'intérêt de registres supranationaux ne paraît pas évident, dès lors qu'existent d'autres modes de protection. En revanche, il serait souhaitable que les **gouvernements incitent, suivant en cela l'exemple de la France, les gestionnaires de leurs registres du commerce nationaux à mettre ceux-ci en ligne sur l'Internet**, à titre payant le cas échéant. Une action en ce sens pourrait utilement être menée au sein de l'Union européenne.

La seule exigence qui paraît devoir être imposée aux sites commerciaux est, comme pour les serveurs télématiques, de **faire apparaître de manière claire, sur la page d'accueil** , **certaines mentions**, en particulier le nom ou la raison sociale de l'organisme responsable du site ainsi que son adresse postale. Cette obligation pourrait faire l'objet d'une convention internationale ou, à tout le moins d'une directive communautaire. Chaque État serait naturellement libre d'imposer des mentions supplémentaires. Par exemple, pour les responsables de sites résidant en France, il serait logique de leur appliquer des obligations similaires à celles retenues pour les serveurs télématiques (nom de l'éditeur de contenu ou sa raison sociale, le nom du directeur de la publication et, le cas échéant les principaux actionnaires de l'organisme éditeur ; sur ce point, voir *infra* quatrième partie du rapport). À défaut, il serait envisageable d'appliquer le droit commun concernant les mentions obligatoires qui doivent figurer sur tous les documents commerciaux (papier à en-tête, factures,...), c'est-à-dire le type de la société (société anonyme, SARL,...), le numéro d'ordre dans le registre du commerce et des sociétés et le montant du capital social. Le défaut de ces mentions légales serait naturellement passible de sanctions pénales.

Au-delà de ces quelques mentions obligatoires, la **mise en place de " labels " délivrés par des**

organismes professionnels ou par des organisations de consommateurs doit être encouragée. Ces labels attesteraient de l'honorabilité des sites concernés et pourraient être retirés par les organismes les ayant délivrés en cas de comportement déloyal du responsable du site à l'égard des consommateurs. La Commission européenne pourrait favoriser le développement de ces labels en incitant des organisations européennes de consommateurs à les développer en liaison avec des organismes professionnels, et à **prévoir dans les contrats les liant aux consommateurs des clauses d'identification de l'auteur de l'offre**. Le contrat type de commerce électronique élaboré par la chambre de commerce et d'industrie de Paris répond à ce besoin. Il prévoit la mention du nom du commerçant ou de la dénomination sociale, un numéro d'identification unique ; l'adresse du siège social ou, si elle est différente, l'adresse de l'établissement responsable de l'offre ; l'adresse électronique ; les coordonnées téléphonique et de télécopie.

Encourager les professionnels à la mise en place d'instruments garantissant un respect effectif des droits du consommateur

Si le droit de la consommation trouve à s'appliquer à l'Internet sous réserve que certaines ambiguïtés soient levées, comme dans d'autres domaines, des difficultés plus sérieuses pourraient concerner l'application effective du droit. La protection législative et réglementaire ne saurait à elle seule permettre d'aboutir à une situation satisfaisante. Il importe d'associer les professionnels, en particulier les entreprises de vente à distance, à la mise en place d'instruments garantissant le respect effectif des droits du consommateur. Les exemples de la déontologie en matière de publicité et de l'identification des professionnels illustrent cette nécessité (voir *supra*). Au-delà, diverses initiatives sont susceptibles de contribuer à une protection efficace des consommateurs.

Encourager la mise en place de codes professionnels de conduite et l'élaboration de contrats types

En France, le syndicat national des entreprises de vente par correspondance et à distance devrait compléter son code professionnel pour tenir compte du développement des échanges en ligne. La portée de cette décision n'est pas négligeable, les adhérents au syndicat s'exposant à des sanctions en cas de violation de ce code. Toute personne physique ou morale peut demander la saisine d'un comité de surveillance lorsqu'elle constate une violation du code professionnel. En cas de manquement grave, cette intervention peut conduire au retrait de l'emblème du syndicat (ce qui n'est pas sans conséquence sur l'image de l'entreprise, en particulier sur Internet où il est susceptible de jouer le rôle d'un véritable label), voire à l'exclusion de l'entreprise du syndicat. Une telle initiative, relayée le cas échéant par des associations de protection des consommateurs, pourrait très utilement être étendue au niveau européen.

L'adaptation des pratiques commerciales des entreprises et de l'organisation du commerce électronique permettrait aussi de répondre aux attentes des consommateurs qui souhaitent effectuer des transactions dans un cadre sécurisé. **Les pratiques contractuelles** apparaissent à cet égard déterminantes. Il est à craindre, cependant que dans certains cas, l'acheteur conserve des doutes sur la portée du contrat le liant au commerçant, compte tenu notamment du recours à l'incorporation de clauses (le plus souvent les conditions générales de vente) par des liens hypertextes.

De ce point vue, le recours au contrat type tel celui utilisé dans le cas de la relation liant l'acheteur à sa banque pour l'utilisation d'une carte bancaire est une pratique sécurisante. Ce type d'approche gagnerait à être étendu à la relation commerciale. Consciente de cette nécessité, la chambre de commerce internationale et la chambre de commerce et d'industrie de Paris élaborent d'ores et déjà des contrats types. Il faut toutefois veiller à ce que les contrats ne soient

pas déséquilibrés au détriment des consommateurs .

Des tiers inspirant confiance aux consommateurs pourraient permettre un réel développement du commerce électronique

La sécurité de la transaction reposera aussi dans une large mesure sur **l'intervention de tiers inspirant confiance au consommateur**. Le rôle des **tiers de certification** paraît déterminant (voir *infra*, les développements sur la signature électronique). Leur principale fonction consiste en effet à identifier les parties et à garantir l'intégrité du message transmis et donc, la portée de la transaction. Il est donc essentiel de permettre la mise en place rapide d'une telle offre de services en Europe.

D'autres acteurs pourraient jouer à l'avenir un rôle important : les **galeries marchandes** assumant pleinement leur rôle d'interface avec le consommateur. Certaines expériences ont eu lieu, comme " Surf & buy " à l'initiative d'IBM. Dans ce dernier cas, il s'agissait d'une opération temporaire qui a pris fin en janvier 1998. Surtout, la galerie marchande ne constituait qu'une vitrine. En pratique, la transaction s'effectuait avec l'un des " magasins " abrités sous une enseigne commune. Les galeries marchandes pourraient à l'avenir jouer un véritable rôle d'intermédiaire, soit en offrant des prestations spécifiques (sélection des magasins, élaboration d'une charte imposant des obligations aux magasins, gestion des paiements etc.), soit en assumant elle-même les responsabilités du vendeur dans le cadre d'une relation contractuelle triangulaire. Le consommateur serait sans doute plus rassuré d'être lié par contrat avec la galerie marchande qu'avec un vendeur inconnu. La galerie se substitueraient donc au magasin, moyennant une commission financière plus importante, à charge pour elle de se retourner ensuite contre le vendeur avec lequel elle aurait aussi passé un contrat. Une telle initiative serait sans doute finalement profitable à toutes les parties. La sécurité juridique offerte au consommateur trouvant une juste contrepartie dans sa fidélisation.

Il semble toutefois que le développement de ce type de galeries marchandes demeure malheureusement marginal. On assiste au contraire à l'émergence de nouveaux intermédiaires peu impliqués dans l'opération de vente. Il faut évoquer le développement des " quoters ", sites de référencement ciblés par services ou produits (livres, disques compacts, logiciels, voyages, annonces classées, voitures), qui n'assument généralement pas la responsabilité de la bonne fin des opérations d'achat ou de vente liée à la commercialisation des produits et services référencés. Les moteurs de recherche (annuaires) comme Yahoo ! Excite, Lycos ainsi que certains fournisseurs d'accès comme AOL agrègent les offres commerciales des différents " quoters ", assumant des fonctions désignées sous le nom de " portals ", afin d'en faciliter la commercialisation, ce qui leur procure des recettes publicitaires substantielles. Aujourd'hui ces portals représenteraient 15 % du trafic sur Internet mais 59 % des revenus en ligne.

Ce constat invite à ne pas tout attendre de ces différentes initiatives, et à mettre en œuvre rapidement un cadre juridique international permettant d'encadrer les transactions électroniques avec des entreprises non européennes.

Mettre en place un cadre juridique international adapté aux transactions électroniques et à la protection du consommateur

L'insuffisance du cadre juridique international actuel

L'évaluation du cadre international suppose d'opérer une distinction entre les règles de fond et les règles relatives à la loi applicable.

Règles de fond : la disparité entre le cadre communautaire et le cadre mondial

Au sein de l'Union européenne se met progressivement en place un cadre juridique offrant une protection élevée des consommateurs, applicable aux transactions électroniques. Outre les directives sur la vente à distance et sur la protection des données à caractère personnelles déjà longuement évoquées, peuvent être mentionnées : celle sur la publicité trompeuse du 10 septembre 1984 précitée ; la directive du 25 juillet 1985 relative à la responsabilité du fait des produits défectueux ; celle du 22 décembre 1986 modifiée relative aux crédits à la consommation ; celle du 5 avril 1993 sur les clauses abusives.

En revanche, il convient de noter **l'absence de règles de fond internationales protégeant les consommateurs dans le cadre de transactions électroniques**. Certaines initiatives internationales sont intéressantes, notamment celles déjà évoquées consistant à promouvoir une normalisation du cadre contractuel liant les parties à une transaction électronique. Compte tenu de l'importance du cadre contractuel dans les relations commerciales électroniques transnationales, la pratique du recours à des contrats type, jusqu'alors largement réservés aux échanges entre professionnels tend à se développer, notamment sous l'égide de la Chambre de commerce internationale. Ces démarches n'ont toutefois pas pour objet la mise en place d'un cadre global, même limité, relatif à la protection des consommateurs.

Face à cette lacune, l'OCDE prépare une recommandation du Conseil relative aux " *lignes directrices régissant la protection du consommateur dans le cadre du commerce électronique* ". Les orientations retenues par le projet de recommandation sont très louables :

– niveau de protection équivalent pour les consommateurs qui effectuent des transactions électroniques à celui d'une vente à distance traditionnelle ;

– information claire des consommateurs, dans une langue qu'ils comprennent, sur l'identité de l'entreprise menant des activités de commerce électronique et sur les biens et services offerts ;

– information complète concernant l'offre ;

– consentement clair et transparent du consommateur ;

– délai de réflexion approprié offert aux consommateurs ;

– information sur le droit applicable au contrat et le tribunal compétent ;

– mise en place de mécanismes d'authentification ;

– mise en place de mécanismes de réclamation et d'autodiscipline ;

– sensibilisation des consommateurs ;

– développement de la coopération internationale.

Toutefois, il est peu probable, compte tenu du niveau des exigences et de certaines orientations retenues, qu'elles soient susceptibles d'être mises en œuvre à court terme par un grand nombre d'États. En outre, ces recommandations ne constituent pas, comme leur nom l'indique, un cadre conventionnel contraignant. Elles ne concernent en outre que les pays membres de l'OCDE, même si les États non membres sont aussi invités à les mettre en œuvre.

Loi applicable à la transaction : l'inadaptation partielle du cadre conventionnel actuel

Deux conventions ont vocation à s'appliquer à la transaction électronique : la convention de la Haye du 15 juin 1955 relative aux ventes internationales d'objets mobiliers corporels et celle de Rome du 19 juin 1980 dont l'objet est plus large. Cette dernière couvre en effet les contrats de toute nature, qu'ils portent sur des biens ou sur des services. Lorsque les deux conventions sont susceptibles de régir une relation contractuelle, c'est celle de la Haye dont l'objet est plus spécifique qui a vocation à être appliquée, sachant que ces deux conventions ont une portée universelle . Elles s'appliquent donc dans le monde entier. Peu importe que les parties choisissent la loi d'un État non contractant, elles seront malgré tout applicables dès lors que le tribunal saisi est celui d'un État contractant. La convention de Rome est signée par la majorité des États membres de l'Union européenne ; elle a été ratifiée par la France le 1er avril 1991. La convention de la Haye n'a en revanche été ratifiée que par 9 États, dont la France. Ainsi, le tribunal d'un État ayant ratifié les deux conventions, saisi d'un litige concernant une transaction électronique, appliquera la convention de la Haye si le litige concerne des produits commandés en ligne et celle de Rome si le litige porte sur un service, sous réserve d'un texte encore plus spécifique (notamment une règle de compétence posée par une directive ou un règlement communautaires dans le cadre intra-européen). Or, aucune de ces deux conventions ne paraît pleinement adaptée aux échanges électroniques.

La **convention de la Haye**, outre le fait qu'elle n'est ratifiée que par peu d'États retient, à défaut d'accord entre les parties, la loi dans laquelle le vendeur a sa résidence habituelle au moment où il reçoit la commande. Toutefois, il est prévu que la loi applicable sera celle de l'acheteur " si c'est dans ce pays que la commande a été reçue soit par le vendeur, soit par son représentant, agent ou commis voyageur ". Cette formulation paraît inapplicable à l'Internet. Comme le souligne le professeur J. Huet : " On mesure la difficulté que soulève à cet égard le commerce électronique, dans un processus dématérialisé où sont abolies les distances, on peut soutenir tout aussi bien que la commande est reçue dans l'établissement du vendeur, à qui elle est adressée et qu'elle est reçue au domicile de l'acheteur, d'où elle est exprimée. Néanmoins, il semble que la première interprétation soit plus respectueuse du texte et qu'il faille donc faire jouer la loi du pays du vendeur. " Cette convention ne réserve au juge la possibilité d'écarter la loi applicable au contrat en vertu de ces principes que si son application est manifestement contraire aux règles d'ordre public.

Ainsi, **en pratique la convention de la Haye devrait conduire à faire le plus souvent application de loi du vendeur**, sauf si les parties en conviennent autrement, ce qui sera peu fréquent lorsque le vendeur prend l'initiative du contrat.

Il en va de même pour la **convention de Rome**, dont le champ d'application est plus large et soulève aussi des problèmes d'interprétation.

Cette convention retient tout d'abord le **principe d'autonomie de la volonté des parties**, qui peuvent choisir la loi applicable au contrat. Ce choix peut, en vertu de l'article 3.1. de la convention, " être exprès ou résulter de façon certaine des dispositions du contrat ou des circonstances de la cause ". La seule limitation au choix des parties, qui peuvent retenir une loi étrangère, concerne selon l'article 3.3 de la convention, l'impossibilité de déroger aux lois impératives d'un État dans lequel tous les autres éléments de la situation sont localisés au moment où les parties ont fait le choix de la loi étrangère. Si les parties y dérogent, les tribunaux conservent la possibilité de faire application des lois impératives du pays dans lequel le contrat est localisé.

En l'absence de choix de la loi applicable par les parties, le contrat sera régi par la loi du pays avec lequel le contrat présente les liens les plus étroits (article 4.1). Un contrat est présumé présenter les liens les plus étroits avec le pays où la partie qui doit fournir la prestation caractéristique – c'est-à-dire l'obligation pour laquelle un paiement est dû –, a au moment de la

conclusion du contrat, sa résidence habituelle ou son principal établissement (cette présomption ne peut-être écartée que lorsqu'il résulte de l'ensemble des circonstances que le contrat présente des liens plus étroits avec un autre pays). **En pratique, le vendeur ou le prestataire de service seront donc favorisés par la convention au détriment du consommateur,** dès lors que dans le silence du contrat, c'est en principe le lieu de résidence de celui qui effectue la prestation qui détermine la loi applicable.

La convention de Rome contient certes dans son article 5 des stipulations protectrices des consommateurs, mais leur rédaction les rend difficilement applicables à l'Internet. La convention prévoit dans son article 5.2 que le choix par les parties de la loi applicable ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle, mais dans certaines circonstances seulement, peu compatibles avec le fonctionnement de l'Internet :

1. " si la conclusion du contrat a été précédée dans ce pays d'une proposition spécialement faite ou d'une publicité, **et** si le consommateur a accompli dans ce pays les actes nécessaires à la conclusion du contrat " ;

2. " si le cocontractant du consommateur ou son représentant a reçu commande du consommateur dans ce pays " ;

3. " si le contrat est une vente de marchandises et que le consommateur se soit rendu dans ce pays et y ait passé commande, à la condition que le voyage ait été organisé par le vendeur dans le but d'inciter le consommateur à conclure une vente ".

Il convient d'écarter d'emblée les circonstances prévues au 2 et au 3 dont on voit mal comment elle pourraient jouer sur Internet, sauf à considérer, par une interprétation audacieuse, qu'un simple serveur, relais technique d'une offre, puisse être regardé comme le représentant du vendeur à l'étranger.

Ce sont donc les circonstances prévues au 1 qui pourraient le cas échéant jouer. Les conditions posées par l'article 1 de l'article 5 sont cumulatives. Il faudrait tout d'abord démontrer que le professionnel a pris l'initiative de la vente dans le pays du consommateur en lui adressant " une proposition spécialement faite " ou une publicité. Mais aucun critère n'est fixé. On en revient à une difficulté déjà évoquée : qu'est ce qu'une publicité sur Internet ? En outre, en l'absence de critères objectifs plus précis, le consommateur pourrait éprouver des difficultés pour apporter la preuve que la transaction a bien été précédée d'une sollicitation du vendeur . La seconde condition est d'interprétation encore plus approximative dans le cas d'une transaction en ligne : que faut-il entendre par " actes nécessaires à la conclusion du contrat " dans le cas d'une transaction qui n'est pas localisable ? Un simple " clic " dont il sera difficile d'apporter la preuve ? Et si le consommateur passe sa commande à partir d'un ordinateur portable ? Enfin, un clic identifie dans le meilleur des cas un ordinateur et non un consommateur. Si le consommateur accepte une offre commerciale, ne faut-il pas plutôt prendre en compte le lieu d'établissement du vendeur qui l'a préparée ? Cette dernière interprétation est le plus souvent retenue . Au total on constate que chacune des deux conditions, qui doivent jouer cumulativement, est difficile à satisfaire dans le cadre d'une transaction via Internet.

Ainsi, **le cadre conventionnel actuel apparaît, pour ce qui concerne le régime des transactions électroniques, à la fois assez ambigu et finalement relativement défavorable au consommateur**. Une adaptation ponctuelle des règles de conflit de lois concernant spécifiquement les transactions électroniques, et donc dérogeant aux conventions de portée plus générales, serait donc souhaitable.

La nécessité d'une convention internationale relative aux transactions électroniques et à la protection du consommateur

Un dispositif sur la loi applicable plus protecteur mais réaliste

Le dispositif sur la loi applicable doit tenir compte de la disparité signalée entre le cadre communautaire et le cadre mondial. Au sein de l'Union européenne, dès que l'harmonisation du droit de la consommation sera suffisante et effective, il y aura lieu de retenir l'application de la loi d'émission (celle du vendeur). Une convention internationale devrait en revanche retenir un dispositif différent. Toute solution simpliste conduisant à ne retenir que la loi du pays d'émission ou celle de réception doit être écartée. Appliquer systématiquement la loi du pays d'émission ne permet pas une protection suffisante du consommateur. Appliquer dans tous les cas la loi du pays de réception est trop contraignant pour les professionnels qui devraient moduler les contrats en fonction de chaque législation nationale.

Aussi, il semble préférable de ne pas trop s'écarter de la philosophie de la convention de Rome, en l'adaptant à la marge afin de trouver un juste équilibre entre deux types de préoccupations qui ne sont pas nécessairement incompatibles : protéger les consommateurs, mais aussi favoriser le développement des échanges électroniques internationaux. Les principes suivants semblent de nature à répondre à cet objectif :

Il convient de maintenir le principe de l'autonomie de la volonté des parties prévu par la convention de Rome, corrigé par l'impossibilité de déroger aux lois impératives du pays dans lequel le contrat est localisé.

Il serait en revanche souhaitable de **permettre de faire jouer aisément les stipulations protectrices du consommateur prévues par la convention de Rome, en adaptant et en assouplissant le dispositif prévu**, le cas échéant par un protocole additionnel, et de faire en sorte qu'en l'absence de choix de la loi applicable par les parties au contrat, le vendeur ne soit pas systématiquement favorisé par le jeu des critères posés.

Il conviendrait de tenir compte d'un nouveau critère, la destination du message, par le jeu d'un faisceau d'indices à déterminer par exemple : la langue, la monnaie, la présentation de l'offre commerciale, l'utilisation de signes distinctifs manifestant la volonté du vendeur (labels, drapeaux,...). La condition relative à l'accomplissement des actes dans le pays serait abandonnée**.**

Si la transaction est précédée d'un message à destination du consommateur, c'est-à-dire que le vendeur a sollicité l'acheteur, le consommateur devra bénéficier d'un cadre juridique sécurisant. En revanche, un consommateur non sollicité, qui a pris l'initiative d'une transaction dont tout lui laisse penser qu'elle relèvera du droit du pays du vendeur ne doit pas s'attendre à un traitement équivalent. L'idée sous-jacente à cette proposition consiste à responsabiliser les parties. Plusieurs cas de figure doivent être distingués à cet effet :

– dans le silence du contrat sur la loi applicable : si la transaction est précédée d'un message à destination du consommateur, il y aura alors lieu de faire application de la loi du lieu de résidence du consommateur ; si le consommateur n'a pas été sollicité, c'est la loi du lieu de résidence du vendeur qui s'appliquera ;

– si le contrat prévoit à l'inverse que c'est la loi du lieu de résidence du vendeur qui s'applique à la transaction, il faut aussi tenir compte de la destination du message. S'il ressort de l'examen des critères de la destination du message que le consommateur a été sollicité, alors le choix par les parties de la loi applicable ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent les dispositions impératives de la loi du pays dans lequel il a sa

résidence habituelle.

La nécessité de définir un socle minimal de principes relatifs à la protection du consommateur

Pour prévenir la nécessité d'avoir à faire jouer les règles de conflit de lois, qui resteront inappliquées pour des transactions de faible montant, il semble nécessaire que la communauté internationale retienne des règles de fond qui constitueront un socle minimal de protection du consommateur.

Deux options paraissent possibles. La première conduirait à fixer des exigences minimales quant aux informations essentielles à porter à la connaissance du consommateur (prix total, conditions de vente, rétractation possible, loi applicable) et à imposer que ces informations soient portées préalablement à la commande à la connaissance du consommateur. Une deuxième option, plus ambitieuse, pourrait s'inspirer des orientations retenues par la directive européenne sur la vente à distance, sans toutefois aller aussi loin : des règles de fond plus détaillées traiteraient de l'information des consommateurs, des modalités de l'acceptation de l'offre sur le modèle de ce qui est proposé plus haut et, du délai de réflexion.

La deuxième option est plus séduisante mais plus difficile à faire accepter. Sa mise en œuvre ne paraît pas irréaliste, mais peut-être seulement à moyen terme.

Chapitre 2

La reconnaissance de la valeur juridique du document et de la signature électroniques

Les échanges de données *via* l'Internet posent des problèmes spécifiques liés à la dématérialisation des opérations . Les messages électroniques se substituent désormais fréquemment aux documents sur support papier. Ce processus donne lieu à de multiples interrogations sur le statut juridique des messages électroniques qui freinent l'essor des échanges en ligne : lorsque la loi exige un écrit, peuvent-ils satisfaire à cette obligation ? Ces messages sont-ils dotés d'une valeur probante ? Une signature électronique peut-elle conférer à un message électronique une valeur juridique ?

Un projet de directive communautaire sur la signature électronique est en préparation. Dans son état actuel, il s'inspire des travaux menés depuis plusieurs années sur ce sujet dans le cadre de la CNUDCI qui a adopté une loi modèle, visant notamment à faire produire aux signatures électroniques des effets équivalents, en matière de droit de la preuve, aux signatures manuscrites. Elle prévoit aussi la mise en place en Europe de tiers de certification chargés de vérifier l'identité des signataires et d'authentifier les messages.

En tout état de cause une réforme, qui dépasse d'ailleurs le champ d'application de la directive, apparaît nécessaire pour offrir aux usagers de l'Internet un cadre juridique sécurisant. Le recours à une signature électronique permet en effet l'identification des parties et garantit l'intégrité des messages électronique. La reconnaissance de la valeur juridique accompagnée de la mise en place de services de certification fiables devrait aussi relancer le chantier. Elle devrait aussi permettre, de donner un élan au chantier de la dématérialisation des procédures administratives (déclarations fiscales, sociales, marchés publics...) au bénéfice des usagers, particuliers ou entreprises.

Une signature apposée sur un document est susceptible d'emporter trois types d'effets, qu'il convient de clairement distinguer :

– l'expression par l'auteur de l'acte de son consentement ;

– l'établissement de la preuve de cet acte juridique en cas de contestation (valeur juridique *ad probationem*) ;

– le respect, le cas échéant, d'un formalisme conditionnant la validité d'acte (valeur juridique *ad validitatem*).

Dans ce dernier cas, lorsqu'un écrit ou une signature manuscrite sont exigés *ad validitatem*, il ne saurait être question de déroger à cette exigence par une disposition unique de portée générale. Cette question n'a donc pas été abordée par ce rapport, elle nécessite un examen au cas par cas des différentes législations .

L'objet de ce chapitre est de proposer une solution de nature à permettre qu'un message électronique signé puisse satisfaire sans restrictions aux deux premières fonctions identifiées ci-dessus.

Ainsi, la valeur juridique du document et de la signature électronique est aujourd'hui encore imparfaite. Il apparaît par conséquent indispensable de reconnaître la valeur probatoire du document électronique authentifié par une signature électronique fiable et de favoriser la mise en place d'une offre de services de certification.

La nécessité de reconnaître la valeur juridique du document et de la signature électroniques n'est qu'imparfaitement rendue possible par le droit civil

La prise en compte du document électronique varie en fonction des régimes de preuve et suppose de bien distinguer deux objectifs : recevabilité et force probante

Une définition synthétique de la preuve peut être retenue : " Prouver, au sens courant du terme... est ce qui sert à établir qu'une chose est vraie. Il n'en va pas autrement en matière juridique, à cette précision près que c'est le juge qu'il s'agit de convaincre de la vérité d'une allégation : la preuve juridique est une preuve judiciaire ". Elle joue aussi un rôle central dans le respect des impératifs de sécurité juridique.

Deux grands systèmes de preuve sont généralement distingués : le **système de la preuve libre** (Danemark) qui laisse une marge d'appréciation au juge pour admettre les preuves qui lui sont présentées et le **système de la preuve légale** (Allemagne, Espagne, Portugal) qui encadre l'intervention du juge, chargé seulement de contrôler la conformité des preuves produites à celles exigées par la loi.

Cette distinction doit être nuancée, elle prend mal en compte les pays de droit coutumier et le système français. Le système anglo-saxon se caractérise par la place privilégiée qu'il accorde au témoignage (règle du " hearsay rule " ou du ouï-dire) qui n'est recevable que s'il émane de quelqu'un qui a eu personnellement connaissance des faits. Le **système français quant à lui peut être qualifié de mixte** (de même que le droit belge ou luxembourgeois) : la preuve n'est libre que dans certains domaines.

Le système de la preuve libre est retenu en France pour le droit pénal, le droit administratif, l'essentiel du droit commercial (à l'exception, en vertu de l'article 109 du code de commerce, de

la preuve du commerçant contre le consommateur) et une partie importante du droit civil : les actes juridiques n'excédant pas un seuil fixé à 5 000 F par le décret no 80-533 du 15 juillet 1980 en application de l'article 1341 du code civil. Au-dessus de ce seuil, en droit civil et pour les actes " mixtes " entre consommateurs et commerçants, le régime est celui de la preuve légale.

L'examen de la prise en compte du document électronique par le droit de la preuve suppose de bien distinguer deux objectifs : la recevabilité du message électronique comme moyen de preuve et la force probante de ce message.

Un système de preuve libre comme le Danemark permet la prise en compte d'un message électronique dès lors qu'il autorise que toute preuve soit produite en justice. À l'inverse, un système de preuve légale, comme celui qui régit en France les actes juridiques de droit civil d'une valeur supérieure à 5 000 F constitue **un obstacle à la recevabilité** des documents électroniques comme mode de preuve. Dans ce cas, la loi prive de toute efficacité certaines preuves, en interdisant au juge de les examiner.

À ce problème de la recevabilité s'ajoute celui du degré de force probante d'un document. En France, dans le régime de la preuve légale, la loi pour répondre à des impératifs de simplicité et de sécurité détermine non seulement les cas où un écrit est exigé, mais aussi la force probante des différents modes de preuve, établissant entre eux une véritable hiérarchie. On trouve au sommet de cette hiérarchie l'acte authentique (le plus souvent un acte notarié) et l'acte sous-seing privé, c'est-à-dire signé des parties. Ce n'est que dans le cas où la loi ne détermine pas le degré de force probante d'un mode de preuve que le juge apprécie sa valeur librement.

Le droit civil français accorde une place privilégiée à l'écrit, d'où l'intérêt de permettre à des actes électroniques d'être considérés comme équivalant à des écrits. Dans certains cas, la préconstitution d'un écrit est une nécessité. Mais la préconstitution d'une preuve fiable peut aussi s'avérer une précaution utile, même dans les cas où la loi n'exige pas un écrit . Dans un système de preuve libre, il faut parvenir à emporter l'intime conviction du juge. La partie sur laquelle repose la charge de la preuve a tout intérêt à se préconstituer une preuve si elle souhaite réduire le risque de preuve qui pèse sur elle. En outre, même dans un régime de preuve libre, existe une certaine hiérarchie des modes de preuve. Les écrits comportant la signature des parties tendront à prévaloir sur les autres modes de preuve.

En dépit de certains éléments de souplesse, le droit actuel ne permet pas de répondre à ces objectifs.

Le droit civil ne permet qu'une prise en compte imparfaite du document électronique

L'article 1341 du code civil, de portée générale, dispose : " Il doit être passé acte devant notaire ou sous signatures privées de toutes choses excédant une somme ou une valeur fixée par décret, même pour dépôts volontaires, et il n'est reçu aucune preuve par témoin contre et outre le contenu aux actes, ni sur ce qui serait allégué avoir été dit avant, lors ou depuis les actes, encore qu'il s'agisse d'une somme ou d'une valeur moindre. "

Ce texte pose deux règles : d'une part, l'obligation de préconstituer une preuve écrite sous la forme d'un acte authentique ou d'un acte sous seing privé pour des actes supérieur à un seuil, d'autre part, l'interdiction de prouver par témoignage contre ces actes, sans qu'intervienne la moindre limitation de valeur (le seuil actuel des 5 000 F ne joue donc pas pour cette seconde règle qui fait de la prééminence de l'écrit un principe général).

Le régime de la preuve écrite rend délicate l'admission d'un document électronique

Lorsque l'on se réfère plus en détail aux conditions de la validité des actes sous seing privé, on constate que deux formalités spécifiques sont imposées : le double original pour les contrats synallagmatiques (art. 1325 C. Civ.), la mention manuscrite de la valeur en chiffres et en lettres pour la promesse unilatérale (art. 1326 C. Civ).

Il est soutenu par une partie de la doctrine que le message électronique constitue un écrit qui pourrait être assimilé sans grandes difficultés à un acte sous seing privé, sous réserve de lever l'obstacle formel posé à l'article 1326 C. Civ. : d'une part, le code civil ne comportant pas de définition de la signature, le vocabulaire utilisé (caractères, procédés, lisibilité,...) permettrait de prendre en compte une signature informatique ; d'autre part, la formalité du double original, sanctionnée par la nullité de l'acte, souffre des exceptions dans les cas où l'une des parties a déjà exécuté son obligation avant la rédaction de l'écrit et, surtout, si les parties déposent un exemplaire entre les mains d'un tiers susceptible de produire l'acte à leur demande (Cass. civ., 3e ch, 5 mars 1980, Bull. Civ. III, no 52, p. 38).

Si une interprétation très souple des textes demeure possible, il ne semble pas que le régime actuel de l'acte sous seing privé soit adapté aux échanges électroniques. La notion d'original n'a pas de sens s'agissant d'un message numérique et il serait dangereux de considérer comme satisfaisant à l'obligation d'une signature un procédé dont la loi n'aurait pas fixé les conditions de validité. En tout état de cause, une adaptation législative serait nécessaire pour modifier l'article 1326 C. Civ. Enfin, l'on comprendrait mal que le législateur soit intervenu en 1980 pour prévoir un nouveau cas limité d'exception à l'exigence d'un écrit, si le code civil permettait la reconnaissance plus ambitieuse des documents électroniques.

Néanmoins, une ligne jurisprudentielle audacieuse traduit une volonté de tendre à une assimilation d'un document électronique offrant certaines garanties à un écrit. Ainsi, un arrêt récent de la chambre commerciale de la Cour de cassation va dans ce sens (Cass. com. 2 décembre 1997). Selon la Cour, un écrit peut être établi et conservé sur tout support, y compris par télécopie (cas de l'espèce), dès lors que son intégrité et son imputabilité à l'auteur désigné ont été vérifiées, ou ne sont pas contestées. Elle considère qu'il revient aux juges du fond d'analyser les circonstances dans lesquelles a été émis l'écrit pour établir s'il peut être retenu comme établissant la preuve d'un acte. Les chambres civiles de la Cour de cassation semblent en revanche plus prudentes. Ainsi, un arrêt de la première chambre civile du 14 février 1995 considère encore qu'une photocopie ne peut valoir que comme commencement de preuve par écrit, ne vaut pas par elle-même écrit, et ne peut en tout état de cause être examinée que *ad probationem* et non *ad validitatem*.

Cependant, le fait qu'un message électronique puisse, en l'état actuel des textes, être assimilable à l'un des écrits visés à l'article 1341 du code civil, demeure très contesté.

Le régime des exceptions à l'écrit ne permet qu'une prise en compte partielle et aléatoire du document électronique

Certains auteurs ont estimé que la valeur juridique d'un document électronique pouvait, en l'état de la législation, être prise en compte au titre des exceptions à l'écrit prévues par la loi. Mais cette analyse appelle elle aussi des réserves.

Le code civil admet sous certaines conditions la prise en compte par le juge d'un commencement de preuve par écrit (article 1347), l'impossibilité matérielle ou morale de produire un écrit (article 1348 al. 1) et, depuis une réforme législative de 1980, les copies constituant une reproduction fidèle et durable (article 1348 al. 2).

Plutôt que d'admettre la pleine valeur probante de l'acte numérique, il a d'abord été suggéré de

ranger le message électronique dans la catégorie du commencement de preuve par écrit. La jurisprudence a déjà admis que la photocopie et plus récemment la télécopie constituent un commencement de preuve par écrit. Toutefois, certaines décisions énoncent au contraire que ces documents n'ont aucune valeur juridique (Com. 15/12/1992 Bull no 419). En tout état de cause, il ne s'agit que d'un début de preuve qui devra être complété par d'autres éléments extrinsèques à l'acte (témoignages, indices). En outre, le commencement de preuve doit émaner, en vertu d'une jurisprudence constante et depuis une ordonnance de 1667, de celui contre lequel la demande est formée. En pratique, il paraît donc difficile d'apporter les éléments de preuve requis dans un contexte d'échanges informatiques.

Une seconde possibilité serait d'intégrer le document électronique dans les dérogations ouvertes par l'article 1348 al. 1, qui vise le cas de l'impossibilité de se procurer un écrit. L'impossibilité matérielle de se procurer un écrit dispense de l'exigence d'un écrit pour établir la preuve d'un acte juridique. Il est aussi parfois soutenu que l'impossibilité matérielle de se procurer un écrit couvre les pratiques issues de l'usage des nouvelles technologies. Mais cette impossibilité est laissée à la libre appréciation du juge et il est difficile de retenir cette qualification dès lors qu'elle résulte d'un état de la technique ou d'un choix délibéré. La prise en compte ne semble envisageable qu'à la condition d'ajouter l'impossibilité technique à l'impossibilité matérielle et morale. Toutefois, il y aurait un risque à retenir une formulation aussi large sans autres conditions. Et il peut être soutenu qu'il n'est jamais impossible techniquement d'accompagner un échange électronique par un contrat écrit. L'esprit de l'article 1348 semble plutôt de réserver la dérogation à un fait exceptionnel, auquel il paraît difficile d'assimiler l'état de la technique.

Une dernière possibilité consisterait à ranger l'acte numérique dans la catégorie des copies constituant une reproduction fidèle et durable. Cette exception ouverte par l'article 1348 al. 2 du code civil résulte en revanche clairement de la volonté du législateur de tenir compte de novations techniques. Pour autant, la logique de la copie, qui suppose l'existence d'un original, se prête mal à l'informatique. En langage numérique, il n'y a pas de différence entre une copie et un original (la notion d'original n'existe plus) et les manipulations sont aisées. Comment dans ces conditions s'assurer que la copie est la reproduction fidèle de l'original ?

En définitive, aucune des solutions d'exception ne semble pleinement satisfaisante pour permettre une véritable reconnaissance de la valeur juridique du document électronique.

Le recours aux conventions de preuve n'a vocation à intervenir qu'à titre complémentaire

Une dernière marge de souplesse est offerte par le droit, c'est la possibilité pour les parties de conclure des conventions de preuve.

Les dispositions sur la preuve ne sont pas d'ordre public. La jurisprudence admet les conventions de preuve (Cass. civ. 1re, Sté Crédicas 8 nov. 1989). Les parties peuvent donc admettre par contrat la force probante de messages électroniques. Il pourrait être envisagé de reconnaître une valeur légale à ces conventions de preuve déjà admises en jurisprudence, pour promouvoir leur usage. Le recours à ces conventions doit en effet être encouragé entre professionnels à titre complémentaire, notamment en matière de paiement .

Mais le recours à des conventions de ce type présente des difficultés dans un milieu ouvert comme le réseau Internet, entre des acteurs qui bien souvent n'auront pas noué de relations contractuelles préalables. De plus, il est à craindre que certaines conventions contiennent des clauses abusives. Aussi, leur usage devrait rester subsidiaire et encadré.

Au total, si le droit actuel offre des marges de souplesse compte tenu notamment d'évolutions jurisprudentielles, une adaptation du code civil reste nécessaire pour répondre aux besoins des

acteurs de l'Internet.

La nécessité d'une réforme législative est largement reconnue

Des adaptations législatives ponctuelles et des propositions nationales

? *Le législateur a déjà admis ponctuellement qu'un message électronique tienne lieu d'écrit*

Sans assimiler de manière générale un message électronique à un écrit, le législateur a admis qu'un tel message tienne lieu d'écrit dans des domaines particuliers afin de simplifier et d'accélérer les formalités administratives et notamment fiscales. En premier lieu, la dématérialisation des factures est prévue par l'article 47 de la loi de finances pour 1990 dispose que : " Les factures transmises par voie télématique constituent (...) des documents tenant lieu de factures d'origine ". Cette dématérialisation est conditionnée par l'obtention d'une autorisation préalable auprès de l'administration fiscale et par le respect de procédures de contrôle. En second lieu, la transmission d'une déclaration administrative par voie électronique est admise par l'article 4 de la loi no 94-126 du 11 février 1994. Il est prévu qu'un document électronique répondant aux exigences posées " tienne lieu d'une déclaration écrite ayant le même objet ". La mise en œuvre d'une déclaration par voie électronique implique une obligation préalable de passer un contrat avec l'administration et de respecter un certain nombre d'exigences : identification de l'auteur de l'acte ; intégrité, lisibilité, fiabilité de la transmission ; horodatation ; accusé de réception ; conservation du message. Ces adaptations législatives constituent un premier pas vers une reconnaissance plus générale de la valeur juridique des messages électroniques qui a fait l'objet de recommandations diverses.

? *Des recommandations ont été formulées visant à la reconnaissance de la valeur probatoire du document électronique en droit français*

Le Conseil national du crédit et du titre a estimé dans son rapport de mai 1997 sur *" Les problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres* " qu'il était souhaitable de procéder à une modification du code civil limitée, dans la lignée de la modification opérée par le législateur en 1980 qui avait consisté à créer une nouvelle exception à l'exigence d'un écrit, en présence d'une copie fidèle et durable (*supra*). L'adjonction de l'alinéa 2 à l'article 1348 en 1980 avait été effectuée en ayant à l'esprit l'archivage des chèques. Le CNCT propose de créer une nouvelle exception à l'exigence d'un écrit par l'adjonction d'un troisième alinéa à l'article 1348 ainsi rédigé : " Elles reçoivent encore exception lorsque le titre est établi ou conservé sous forme électronique dans des conditions assurant son intégrité et permettant l'imputabilité à son auteur ".

Réuni sous l'égide du **GIP " droit et justice ",** à la demande de la direction des affaires civiles et du Sceau du ministère de la justice, un groupe de professeurs de droit a proposé une adaptation plus importante du code civil. Cette proposition ne retient pas la voie des exceptions à l'écrit, ni même celle de l'équivalent à l'écrit, elle préfère considérer que le message électronique constitue un écrit. Il est suggéré de définir la preuve littérale (c'est-à-dire écrite) dans des termes qui couvrent à la fois l'écrit sur support papier et l'écrit électronique et que la preuve contraire ne puisse être apportée, sous réserve de dispositions légales spécifiques ou de conventions de preuve, que dans le cas de présomptions graves, précises et concordantes. Dans un second temps, ce groupe a estimé nécessaire, comme le Conseil d'État, de prévoir une reconnaissance juridique de la signature électronique.

Un contexte international incitatif

? *De nombreux pays reconnaissent d'ores et déjà la valeur probante des messages*

électroniques

Le **Québec** a modifié son code civil dès 1993 pour reconnaître valeur probante aux " inscriptions informatisées ". Le législateur a reconnu cette valeur dans une section spécifique (sect. VI), distincte de celle relative aux actes sous seing privé (sect. IV) et des autres écrits (sect. V) . Le législateur québécois a aussi prévu dans un article 2826 (qui figure dans la section IV sur les actes sous seing privé) que le document signé sur support papier l'emporte sur le document conservé sur support électronique. Le Québec a fait le choix de ne pas ranger les " inscriptions de données informatisées " dans les catégories existantes d'écrit. La valeur probante de l'acte reproduisant les données est présumée dès lors que certaines conditions sont réunies (document intelligible, caractère intègre et intégral des données conservées).

En Europe, les initiatives sont dans l'ensemble plus récentes et plus ponctuelles. Le **Royaume-Uni** a adopté en 1995 un *Civil Evidence Act* qui admet qu'un document administratif soit admis à titre de preuve, sous réserve de son authentification au moyen d'une procédure fiable. En **Allemagne**, il est admis que les documents informatiques entrent soit dans la catégorie des preuves écrites sans signature soit dans celle des " observations " qui permettent au juge de se déterminer en fonction de sa perception *in concreto*. En outre, une loi du 1 août 1997, dite " loi multimédia " met en place un cadre juridique et technique pour les signatures électroniques et le chiffrement. La loi prévoit la création d'instances de certification (*supra*), sous la forme de sociétés commerciales agréées par une instance de certification suprême relevant de l'État fédéral. **L'Italie** a aussi adopté une loi le 15 mars 1997, complétée par un décret du 5 août 1997, sur les documents dématérialisés et sur la signature électronique. Les contrats dématérialisés authentifiés par des signatures électroniques certifiées se voient reconnaître la force probante d'un écrit. La certification est effectuée par un tiers, soit une autorité administrative de certification relevant de l'État, soit par les notaires (autorité notariale de certification).

? *Enfin, la nécessité de reconnaître la validité du message électronique est affirmée par des organismes internationaux*

La **Commission des Nations unies pour le droit commercial international (CNUDCI)** mène une action volontariste pour inciter les États à lever les obstacles à l'admissibilité des messages électroniques comme mode de preuve, dont témoigne l'adoption d'une loi type sur le commerce électronique en 1996. L'article 9 de la loi type de la CNUDCI admet dans son 1er alinéa la force probante d'un message de données qui n'est pas présenté sous forme d'original. La démarche très pragmatique de la CNUDCI est à rapprocher des initiatives récentes (*supra*) du législateur national qui s'est attaché à faire d'un document électronique un " équivalent fonctionnel " à l'écrit sous certaines conditions.

La **Commission européenne** a également insisté, notamment dans sa communication du 8 octobre 1997 intitulée " Assurer la sécurité et la confiance dans la communication électronique ", sur la nécessité d'une adaptation des législation nationales visant la reconnaissance de la valeur juridique d'un document électronique signé. Elle estime que " l'utilisation de la forme écrite remplit plusieurs fonctions, par exemple de mise en garde, de preuve d'authenticité. Les documents fournis avec une signature électronique peuvent également remplir ces fonctions, à conditions que les signatures numériques soient sûres et fiables. Si des documents fournis avec une signature numérique remplissent les exigences de la forme écrite, cela aurait un impact très positif (...) ". **Surtout, un projet de directive sur la signature électronique** précise notamment à quelles conditions une signature peut être considérée comme fiable et invite les États membres à reconnaître à ces signatures des effets juridiques équivalents à ceux produits par des signatures manuscrites.

En conclusion, il ressort de ces différents travaux qu'une reconnaissance rapide de la valeur

juridique du document électronique s'impose et rend nécessaire une adaptation du code civil. La proposition retenue s'inscrit dans la lignée des réformes législatives de 1990 et 1994 et s'attache à reconnaître les effets juridiques du recours à une signature électronique fiable. Elle vise à lever un certain nombre d'incertitudes sans toutefois bouleverser l'économie générale du code civil.

Reconnaître la valeur probatoire du message électronique et favoriser la mise en place d'une offre de services de certification

Reconnaître la valeur probatoire du message électronique authentifié par une signature électronique fiable

En résumé l'économie du dispositif proposé est la suivante :

1. une signature électronique remplit les fonctions d'une signature dès lors qu'elle est fiable ;

2. lorsqu'un document électronique assorti d'une signature électronique est présenté pour établir la preuve d'un acte, il ne saurait être contesté au seul motif qu'il se présente sous forme électronique ; il tient lieu d'acte sous seing privé dès lors qu'il est assorti d'une signature fiable et qu'il est conservé avec celle-ci de façon durable ;

3. si le document électronique est accompagné d'un certificat répondant à certaines exigences, délivré par une autorité de certification accréditée, la fiabilité de la signature et la conservation durable du document signé (si le certificat a aussi cet objet) sont présumées. Dans le cas inverse, il appartiendra à celui qui entend se prévaloir d'un document électronique signé mais non certifié de démontrer que les conditions de fiabilité et de conservation sont remplies.

Plusieurs précisions doivent être apportées pour éclairer la portée du dispositif proposé.

Définir dans le code civil les fonctions d'une signature et préciser les exigences qui permettent de considérer qu'une signature électronique remplit ces fonctions

La signature électronique est intimement liée au document électronique . Celui-ci n'a véritablement de valeur que si son émetteur peut être identifié. Aucun texte législatif ou réglementaire ne définit aujourd'hui la signature en droit interne. Mais le droit impose fréquemment qu'un acte soit signé. L'approche retenue est fonctionnelle. Constitue une signature un procédé qui permet de remplir avec efficacité certaines finalités : identification du signataire et manifestation de sa volonté d'adhérer au message signé qui est réputé intègre. Rien ne s'oppose *a priori* à la prise en compte d'une signature électronique qui remplirait les fonctions attendues d'une signature .

La définition suivante de la signature pourrait être retenue : **une signature identifie le signataire et manifeste son consentement au contenu de l'acte auquel elle est attachée et aux obligations qui en découlent**.

Les fonctions de la signature étant précisées, il importe de définir à quelles conditions une signature électronique liée à un document de même nature peut produire les effets d'une signature.

Selon la proposition du Conseil national du crédit et du titre, la valeur probante d'un titre n'est admise que sous réserve du respect d'une double condition : la non-altération du contenu de l'acte d'une part, et l'imputabilité à son auteur d'autre part. L'exigence du respect de ces conditions, exprimées de manière synthétique, paraît essentielle, notamment celle d'imputabilité à l'auteur parfois occultée (notamment dans la loi du Québec, ce qui est assez surprenant). La

proposition du GIP Droit Justice est très proche : identification de l'émetteur et message établi et conservé dans des conditions de nature à en garantir la fiabilité. Ces conditions sont à rapprocher de celles fixées par la loi type de la CNUDCI, assez similaires.

Il est proposé de retenir sur ce point une approche comparable et, de considérer qu'une signature électronique remplit les fonctions d'une signature dès lors qu'elle est fiable. Cette fiabilité est conditionnée par le respect des exigences suivantes :

– **intégrité** : elle est liée aux données qu'elle authentifie et elle est créée dans des conditions qui permettent la conservation des données et le respect de leur intégrité ;

– **imputabilité** : elle est imputable au signataire qu'elle identifie.

Admettre que le document électronique tienne lieu d'écrit

En premier lieu, lorsqu'un document électronique assorti d'une signature électronique fiable est présenté pour établir la preuve d'un acte, il ne saurait être contesté au seul motif qu'il se présente sous forme électronique. Il s'agit ici de lever les réserves concernant l'admissibilité en preuve d'un document électronique et de faciliter la préconstitution des preuves, même lorsqu'un écrit n'est pas exigé par la loi. Ainsi, un document électronique assorti d'une signature sera admis dans des conditions identiques à une écrit manuscrit (il ne sera donc assimilé ni à une copie, ni à un simple commencement de preuve par écrit).

Il convient toutefois de maintenir l'exigence des écrits sous seing privé pour les actes importants (article 1341 du code civil), mais aussi de prévoir qu'un document électronique signé tient lieu d'acte sous seing privé sous certaines conditions.

? *Il n'est pas souhaitable de restreindre à l'excès le champ d'application du régime de la preuve légale qui est protecteur*

Une option radicale pour permettre la prise en compte des documents électroniques consisterait à instaurer en France un régime de liberté de la preuve ou à réévaluer très nettement le seuil prévu à l'article 1341 du code civil. Cette option radicale, qui conduirait *de jure* dans le premier cas et *de facto* dans le second cas à bouleverser l'économie actuelle du code civil, serait dangereuse compte tenu de la nature des actes en cause et du caractère protecteur des règles de la preuve littérale.

En revanche, il est sans doute **nécessaire de réévaluer le seuil de 5 000 F** exigé pour les actes civils par le décret no 80-533 du 15 juillet 1980 en application de l'article 1341 du code civil. Ce relèvement ne doit être effectué qu'avec la plus grande prudence si l'on ne souhaite pas vider le régime de la preuve légale de sa substance. **Il paraît suffisant de s'en tenir à une réévaluation du seuil compensant l'érosion monétaire (suivant en cela les recommandations du CNCT) en retenant un chiffre aisément mémorisable et compatible avec le prochain passage à l'EURO (équivalent à 1000 ou 1500 euros par exemple)**.

La question se pose, au-delà du droit civil de la modification du régime de la preuve des **actes dits " mixtes " en droit commercial**, fixé par l'article 109 du code de commerce dont la rédaction actuelle résulte de la loi du 12 juillet 1980 qui dispose : " À l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit disposé autrement par la loi. " En vertu de ce texte, la preuve peut être rapportée par tout moyen contre les commerçants. Cette souplesse résulte de la volonté de ne pas entraver la rapidité des relations commerciales, sachant que la loi astreint par ailleurs les commerçants à tenir des registres et une comptabilité. Mais la volonté d'assurer une protection efficace des consommateurs a conduit le législateur à astreindre les commerçants au respect des dispositions de l'article 1341 dans leurs

relations avec les particuliers.

Il semble **inopportun de revenir aujourd'hui sur cette exception au régime de liberté de la preuve qui prévaut en matière commerciale**, consacrée par le législateur en 1980 pour plusieurs raisons. D'une part, le commerçant est en mesure d'invoquer une exception à l'exigence d'un écrit en raison d'un usage (11 janv. 1994, Bull. Civ. V, no 16 p. 13). D'autre part, les actes mixtes bénéficieront du relèvement du seuil prévu à l'article 1341. Enfin, les relations commerciales se prêtent bien au recours aux conventions de preuve.

? *Un document électronique doit pouvoir, sous certaines conditions, satisfaire à l'exigence légale d'un écrit et tenir lieu d'acte sous seing privé*

Une première solution consisterait à créer une nouvelle exception à l'écrit. Mais placer l'acte numérique au rang des exceptions à la preuve littérale laisse place à un régime de liberté de la preuve qui permet la recevabilité du message électronique mais sans le doter d'une force probante particulière. L'acte numérique est doté d'une valeur relative, relevant, comme d'autres éléments (indices, témoignages, ...), de l'appréciation du juge. Le " risque de preuve " n'est donc qu'atténué. Ce régime ne paraît pas adapté à un message accompagné d'une signature véritablement fiable. Ce serait faire peser des conditions relatives à la signature disproportionnées par rapport à ses effets. En tout état de cause, cette solution ne répondrait pas aux prescriptions du projet de directive sur la signature électronique s'il est adopté.

Une autre solution consisterait à considérer, en retenant une conception très large de l'écrit, que le document électronique signé constitue un acte sous seing privé, c'est-à-dire un écrit doté d'une force probante particulière. Si l'objectif est pertinent (assimiler à un acte sous seing privé), cette solution n'est pas sans présenter quelques inconvénients. Elle conduit tout d'abord à une dilatation de la notion d'écrit, assimilé dans l'esprit du plus grand nombre à des inscriptions manuscrites. Ainsi, pour ne prendre que cet exemple, la récente directive du 20 mai 1997 sur la vente à distance prend bien soin de distinguer l'écrit d'autres types de supports et, de préciser dans son article 5, pour tenir compte des échanges en ligne, que " le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition et auquel il a accès confirmation " d'informations commerciales. Cette assimilation supposerait en outre l'instauration d'un régime spécifique pour le message électronique, ce qui vide cette solution d'une grande partie de son intérêt. Elle rend nécessaire une adaptation du régime éprouvé des actes sous seing privé qui donne par ailleurs satisfaction aux praticiens pour les écrits sur support papier et paraît difficile à transposer dans l'univers informatique.

Au total, il paraît suffisant de prévoir, sur le modèle des interventions récentes du législateur **que le message électronique tienne lieu d'écrit ou d'acte sous seing privé** et d'inclure à cette fin de nouvelles dispositions législatives dans le chapitre sur la preuve littérale (voir *infra*). Cette assimilation est naturellement conditionnée par le respect de conditions : le document doit être assorti d'une signature fiable, et être conservé de façon durable sous le contrôle des signataires ou, d'un tiers à qui ces derniers souhaitent confier cette fonction.

Il reviendra au juge, si la fiabilité de la signature ou la conservation du message sur support durable sont contestées, de procéder aux vérifications nécessaires par l'intermédiaire d'un expert. C'est l'examen des circonstances de la production du message à laquelle se réfère la Cour de cassation dans son arrêt précité du 2 déc. 1997. Si le message est signé et conservé de façon durable, il sera admis en preuve dans des conditions identiques à un écrit original.

Répondre à l'exigence d'un écrit ne signifie pas pour autant répondre aux exigences de tous les écrits : il est question ici des actes sous seing privé et non des actes authentiques, qui exigent la

présence d'un notaire éclairant les parties sur la portée de leurs engagements et qui ne sont pas affectés par la proposition.

En outre, la question des conflits de preuve entre deux actes sous signatures privées, l'un sur support papier, l'autre conservé sur support électronique, demeure ouverte. Pour la majorité des personnes auditionnées, il serait prématuré de faire prévaloir aujourd'hui un message électronique, même authentifié, sur un acte sur support papier assorti de la signature manuscrite des parties et ayant le même objet. Cette hiérarchie paraît conforme à l'état des mœurs. Selon le professeur Linant de Bellefonds : " La logique juridique de l'autonomie de la volonté consisterait à dire que l'expression la plus récente de cette dernière oblitère la plus ancienne. Or ceci nous paraît fondamentalement imprudent. Dans tous les cas, l'écrit devrait prévaloir car il s'agit d'un acte investi d'une force de démonstration particulière. " Néanmoins, dès lors que de strictes exigences relatives à la fiabilité de la signature et à la conservation du message de façon durable sont imposées, il paraît difficile de maintenir longtemps la prééminence de l'écrit sur support papier, entouré finalement de moindres garanties. En outre, des personnes de mauvaise foi pourraient archiver d'avance des écrits manuscrits contraires à leurs engagements électroniques, ou négocier des avenants électroniques à des contrats écrits dont elles savent par avance qu'elles ne les respecteront pas. Aussi, pour limiter les risques de répudiation unilatérale est-il sans doute préférable de s'en remettre à la sagesse du juge et de lui laisser le soin de trancher les conflits de preuve en fonction des circonstances de l'espèce.

Créer un régime de présomption légale réfragable

Il convient d'apporter la plus grande attention à la question de la charge de la preuve et de créer un régime de présomption légale réfragable, lié au recours à un prestataire de services de certification accrédité, pour inverser cette charge.

Si des conditions légales sont posées, il importe de s'assurer que celui sur qui pèse le risque de preuve est bien en mesure d'y faire face. Ainsi, comment un particulier pourrait-il apporter la preuve de la fiabilité d'un système informatique ? Il apparaît suffisant d'exiger une signature fiable et une conservation durable du document sous le contrôle du signataire. Il appartiendra alors au juge, en cas de contestation, d'apprécier le respect des conditions.

Mais partant du constat qu'il sera néanmoins difficile d'apporter la preuve que les conditions sont réunies, il semble souhaitable de mettre en place un régime de présomption légale. En conformité avec le projet de directive sur la signature électronique, il convient **d'admettre qu'un document électronique certifié par un tiers dûment accrédité (voir *infra*) conduit à présumer satisfaites les exigences légales.** Il s'agit de conférer une plus grande sécurité juridique aux échanges électroniques et de rassurer les utilisateurs. Cette présomption doit demeurer réfragable. Il revient à celui qui conteste la méconnaissance des exigences légales de prouver qu'elles ont été méconnues. Ainsi, en cas de contestation, le recours aux services d'un tiers certificateur conduit à inverser la charge de la preuve.

Ainsi, lorsqu'un message électronique est présenté pour établir la preuve d'un acte, il est présumé doté de la force probante d'un écrit sous signatures privées s'il est accompagné d'un certificat délivré par un tiers certificateur accrédité, indépendant du signataire, dans des conditions précisées par décret, qui garantissent l'intégrité du message, l'imputabilité à l'auteur désigné et sa conservation durable.

Les modalités de l'adaptation proposée du code civil

Une possibilité consisterait à substituer à l'actuel §3 du chapitre sur la preuve littérale, intitulé " Des tailles ", tombé en désuétude, un §3 relatif à la preuve des documents électroniques.

Le §3 intitulé " Des tailles " est situé dans le code civil après un §1 " Du titre authentique " et un §2 " De l'acte sous seing privé ". Il comporte un seul article 1333 ainsi rédigé : " Les tailles corrélatives à leurs échantillons font foi entre les personnes qui sont dans l'usage de constater ainsi les fournitures qu'elles font ou reçoivent en détail ".

Ce texte a été rédigé à une époque où l'analphabétisme était encore important. " C'est précisément le développement de l'alphabétisation qui explique la désuétude dans laquelle est tombé un procédé probatoire que le code civil assimile à l'écrit : les tailles. Il s'agit d'un mode de preuve autrefois utilisé pour constater des fournitures usuelles faites à un consommateur. Un morceau de bois est fendu en deux parties égales et correspondantes. L'une d'entre elle (la taille proprement dite) est conservée par le fournisseur, l'autre (l'échantillon) est aux mains du client. Lors d'une livraison, la taille et l'échantillon sont rapprochés et une entaille transversale ou coche est faite à la fois sur les deux pièces de bois. En cas de discordance entre le nombre de coches portées sur la taille et sur l'échantillon, les livraisons ne sont prouvées que jusqu'à concurrence du plus petit nombre de coches, sauf preuve de fraude ou d'erreur. Ce succédané archaïque de l'écrit ne semble plus employé aujourd'hui. "

Ce dispositif correspond très exactement à ce qu'il convient d'admettre mais pour des motifs différents : le contexte a fort heureusement changé et ce n'est plus pour pallier l'analphabétisme qu'un nouveau dispositif doit être introduit. Mais le besoin est tout aussi pressant de voir reconnaître que le message électronique, sans être au sens strict un écrit, puisse tenir lieu d'écrit. En pratique, aux morceaux de bois striés succéderaient dans l'immédiat des clés certifiées (et peut être dans un proche avenir de nouvelles formes d'empreintes comme l'iris de l'œil), dont le rapprochement aurait la même finalité. Une garantie supplémentaire résulterait de l'intervention d'un tiers mais l'esprit reste proche.

C'est finalement en conformité avec l'esprit du code civil et, sans modifier en rien les catégories existantes d'écrits qu'il est possible de prendre pleinement en compte les évolutions technologiques.

Favoriser la mise en place d'une offre de services de certification

L'importance en pratique de la certification dans les échanges électroniques

En pratique, les signatures électroniques sont aujourd'hui rendues fiables par un recours à des techniques cryptographiques similaires à celles utilisées pour le chiffrement. Parmi celles-ci, le procédé dit de la " signature numérique à clé publique " est sans doute le mieux adapté à la signature de messages électronique et tout laisse penser que son usage devrait rapidement se généraliser au niveau mondial. Ce procédé permet de signer des messages électroniques dont l'origine et l'intégrité sont certifiées par un tiers dit de certification. Ce nouveau métier accompli par des sociétés comme Verisign, suscite un intérêt auprès de certains intermédiaires qui y voient un prolongement logique de leur activité : notaires et banques, par exemple.

Deux clés complémentaires sont émises et assignées à un utilisateur. L'une d'elle, la clé de signature ou clé privée, reste confidentielle alors que l'autre, la clé de vérification est rendue publique. " Dès lors que le destinataire est en mesure de vérifier que la signature numérique a bien été créée par le détenteur de la clé nommée dans le certificat, il a non seulement la certitude qu'elle émane bien de lui, mais aussi la garantie que le message n'a pas été modifié depuis sa création par le biais de la fonction de hachage comprise dans la procédure de certification. L'intégrité du message et donc sa fidélité est préservée. "

La certification des signatures par un tiers constitue un procédé qui doit être encouragé et sans

doute encadré si des effets juridiques y sont attachés . Il est sans doute préférable de s'en tenir dans le code civil à la reconnaissance des effets d'une signature électronique fiable authentifiant un message électronique, sans aborder les modalités du procédé de certification. Le parti inverse, retenu par l'Allemagne dans sa récente loi sur le multimédia du 1er août 1997, présente l'inconvénient majeur de faire peser un risque d'obsolescence sur le dispositif légal, compte tenu de l'évolution rapide des techniques. Une fois connu le cadre et les conditions d'exercice des activités de certification, qui seront précisés dans la directive sur la signature électronique, les modalités pourront être précisées sur ce point en droit interne.

L'intervention des tiers de certification doit avoir lieu dans des conditions de nature à favoriser l'apparition rapide en Europe d'une offre de service

Pour stimuler l'offre de services de certification, plusieurs leviers sont envisageables. L'État peut tout d'abord créer lui-même une demande en développant le recours à des tiers de certification. Deux chantiers semblent à cet égard prometteurs : le développement des téléprocédures et la dématérialisation des marchés publics, notamment de fournitures.

Les pouvoirs publics doivent surtout s'efforcer d'instituer un cadre juridique créant un équilibre entre les contraintes pesant sur l'activité de certification et les effets juridiques qu'il convient d'attacher au recours aux certificats.

Les principes suivants pourraient guider l'élaboration de ce cadre.

L'activité de certification ne doit pas obéir à un régime de licence obligatoire. L'exercice de cette profession doit demeurer libre. Toute signature électronique fiable doit être admise en preuve, même si elle est assortie d'un certificat délivré par un tiers certificateur non accrédité. Ce point est très explicitement précisé dans le projet de directive sur la signature électronique. Dès lors que les certificats délivrés offriront différents niveaux de garanties, il n'est pas nécessaire d'encadrer la délivrance de certificats les plus modestes, se bornant par exemple à attester l'identité d'un contractant. En revanche, il paraît légitime de réserver certains effets juridiques à la production d'un certificat délivré par un certificateur accrédité garantissant le respect des exigences légales. Aussi, seul le recours à un tel tiers dispense le signataire d'un document électronique d'avoir à apporter la preuve que les conditions légales sont satisfaites en cas de procès (bénéfice de la présomption).

La création d'un régime de présomption légale implique néanmoins de définir des exigences précises concernant les certificats et les certificateurs (qui émettent les certificats garantissant le respect des exigences relatives aux messages ou aux signatures électroniques). Les tiers certificateurs auront le choix de solliciter une accréditation pour exercer leur métier. La délivrance de cette accréditation suppose le respect d'un certain nombre d'exigences précisées en annexe à la directive en préparation sur la signature électronique. Elles concernent tant les tiers certificateurs que les certificats. S'agissant des **certificateurs,** il paraît suffisant de retenir des exigences minimales relatives : aux moyens techniques et aux ressources financières garantissant un certain niveau de service à moyen terme (stockage des données pendant une certaine période de temps par exemple) ; au respect de principes déontologiques, notamment l'indépendance par rapport au signataire et le respect et la protection des données personnelles collectées à l'occasion de la certification ; à la fiabilité des produits et des techniques utilisés (tant par le signataire que par l'autorité elle-même) pour émettre les signatures et conserver le cas échéant les messages. Il importe de dispenser l'usager d'un service de certification d'avoir à établir lui-même qu'il a utilisé un logiciel fiable. Le recours à un certificateur qui accepte de délivrer un certificat doit dispenser le signataire de l'accomplissement de toute autre formalité. C'est le tiers certificateur qui devra vérifier que la clé secrète du signataire a été émise à l'aide de produits et

de techniques fiables. Cette évaluation pourrait avoir lieu au regard de normes de qualité européennes. Concernant les **certificats,** les pouvoirs publics n'ont pas vocation à définir à la place des acteurs tous les niveaux de certificats qui seront offerts. En revanche, il leur revient de préciser les exigences requises pour que des certificats produisent des effets juridiques déterminés. Deux cas au moins doivent être envisagés. D'une part, les conditions générales requises pour qu'un certificat permette de faire présumer remplies les exigences relatives à la signature fiable et à l'obligation de conservation du document de façon durable. D'autre part, les exigences spécifiques, proportionnées qui peuvent être requises dans le cadre de relations entre des acteurs du secteur public et des particuliers.

Le bénéfice de l'accréditation doit enfin être subordonné au respect d'exigences précises. L'accréditation pourrait être délivrée par des organismes privés offrant de sérieuses garanties tels le COFRAC (Comité français d'accréditation, qui est une association) au regard d'exigences définies par l'État par décret, dans le respect des orientations fixées par la directive sur la signature électronique. Le respect de la charte devrait faire l'objet de contrôles *a posteriori*, soit de manière aléatoire sous forme d'audit, par ces organismes en liaison le cas échéant avec des services de l'État (Direction générale de la consommation de la concurrence et de la répression des fraude, Service central de sécurité des systèmes d'information, par exemple), soit par des expertises à l'occasion d'une contestation de la fiabilité d'un certificat lors d'un procès. En cas de non-respect des exigences, l'accréditation serait retirée. Le tiers certificateur ne pourrait plus se prévaloir du label correspondant au respect de la charte de qualité et donc offrir des certificats faisant bénéficier une signature d'une présomption de fiabilité, sauf à se soumettre spontanément et avec succès à un nouveau contrôle qui permettrait d'obtenir une nouvelle accréditation.

Il importera enfin de préciser les obligations et le régime de responsabilité applicable aux autorités de certification à l'égard de leurs clients.

Instaurer un principe de reconnaissance mutuelle au plan international

Enfin, le développement du commerce électronique international impose la définition d'un cadre juridique commun qui garantisse la fluidité et la sécurité des échanges. Une fois acquis au plan national et communautaire, le principe de reconnaissance mutuelle des services de certification, indispensable au développement des échanges entre des partenaires ayant recours à des tiers différents (avec un réel risque qu'un tiers refuse un certificat provenant d'une entreprise d'un autre pays), devra être étendu. Des accords internationaux devront déterminer à quelles conditions les certificats émis par des autorités de certification extra-européennes pourront être retenus comme équivalents à ceux émis par des autorités établies dans l'Union européenne. Il importera en particulier de veiller à la réciprocité et de s'assurer que les processus retenus reposent sur une approche technologiquement neutre et procurent un niveau de fiabilité comparable.

L'harmonisation des principes relatifs à la signature électronique sera effective en Europe à court terme. L'un des objectifs du projet de directive sur la signature électronique en cours de discussion est naturellement de parvenir à une reconnaissance mutuelle des certificateurs afin de garantir la libre circulation des services dans ce domaine en Europe. Cette directive devrait trouver un prolongement au niveau mondial, dans le cadre d'une convention internationale qui garantisse la reconnaissance mutuelle des services de certification. Il semble possible d'aboutir sur ce point, compte tenu du travail effectué dans le cadre de la CNUDCI et de la ferme volonté politique de certains États tiers à l'Union européenne de lever les obstacles à une reconnaissance mutuelle des produits et services liés à la signature électronique.

Les enjeux de la cryptologie sur Internet

Sur Internet, la cryptologie est indispensable pour assurer la confidentialité des messages, mais également la sécurité des transactions et des moyens de signature électronique. Les moyens cryptologiques permettront également d'empêcher la contrefaçon des œuvres et des contenus protégés par le droit d'auteur (voir *infra* troisième partie)

Les pouvoirs publics sont convaincus de la nécessité de libéraliser dans une large mesure la fourniture et l'utilisation de moyens de cryptologie afin de favoriser l'essor du commerce électronique. Cet objectif trouve cependant ses limites dans les préoccupations de sécurité publique. En particulier, il demeure nécessaire que la police judiciaire et les services de sécurité puissent continuer à pratiquer, dans le cadre légal, des interceptions de messages sans que la personne placée sous surveillance en soit informée. C'est cet équilibre que la loi du 26 juillet 1996 et ses décrets d'application ont tenté d'instaurer. Toutefois, l'accueil réservé des professionnels et la nécessité de procéder à l'évaluation du nouveau dispositif ont conduit le Gouvernement à annoncer une vaste consultation sur ce sujet à l'automne 1998. Quelques pistes de réflexion seront donc esquissées en vue d'une éventuelle évolution du cadre légal de la cryptologie.

La libéralisation de la cryptologie est réelle mais encore partielle

Le cadre juridique actuel de la cryptologie est fixé par l'article 28 de la loi du 29 décembre 1990 sur la réglementation des télécommunications, dans sa rédaction issue de l'article 17 de la loi du 26 juillet 1996, et par ses décrets d'application en date du 24 février 1998 et du 23 mars 1998 . Le nouveau régime distingue les moyens de cryptologie selon qu'ils sont destinés exclusivement à assurer des fonctions de signature électronique et d'authentification ou qu'ils assurent des fonctions de confidentialité (*i.e.* chiffrement du contenu d'un message ou d'un fichier).

Moyens de cryptologie assurant des fonctions de signature et d'authentification, sans fonction de confidentialité

La nouvelle législation a très largement libéralisé l'utilisation des moyens de cryptologie servant exclusivement à la signature électronique, à l'authentification d'un message, à sa non-répudiation et au contrôle de son intégrité. L'utilisation en est libre, sous réserve que le fournisseur du moyen de cryptologie (par exemple le vendeur du logiciel) ait fait, avant toute commercialisation, une déclaration simplifiée auprès de l'administration (SCSSI) décrivant les caractéristiques techniques de ce moyen de cryptologie. Celui-ci ne doit en aucun cas permettre à l'utilisateur de chiffrer un message ou un fichier. L'importation et l'exportation de ce type de moyens de cryptologie sont également libres.

Moyens de cryptologie assurant des fonctions de confidentialité des messages ou des fichiers

Lorsque la clé de chiffrement utilisée a une taille inférieure ou égale à 40 bits , le régime applicable est comparable à celui décrit plus haut pour les moyens servant seulement à la signature électronique et à l'authentification des messages : l'utilisation et l'importation sont libres, et la fourniture doit simplement faire l'objet d'une déclaration. L'exportation des moyens de cryptologie vers des pays n'appartenant pas à l'Union européenne est toutefois soumise à autorisation, conformément à l'accord international conclu à Wassenaar le 19 décembre 1995.

En revanche, lorsque la clé a une taille supérieure à 40 bits, ce qui correspond à un niveau de protection assez élevé, le contrôle administratif est beaucoup plus strict. La fourniture, l'importation et l'exportation de ces moyens de cryptologie sont subordonnées à l'autorisation du Premier ministre (SCSSI). L'utilisation requiert également une autorisation préalable, sauf si l'utilisateur accepte de remettre l'ensemble des clés de chiffrement à un organisme spécialement habilité à cet effet, appelé " tiers de séquestre " (ou encore " tiers de confiance "). Celui-ci doit être agréé par le SCSSI qui vérifie que les conditions de sécurité prévues sont suffisantes. Il veille surtout à la capacité technique de l'organisme à gérer de telles clés et à les remettre sans délai et confidentiellement à la police judiciaire ou aux services de sécurité à des fins d'interception des messages . La réglementation exige également que les employés susceptibles de remettre les clés aux services de sécurité disposent d'une habilitation au niveau " secret défense ". La simple remise de clé ne donne lieu à aucun paiement de l'administration au " tiers de séquestre " ; seule la mise en œuvre par celui-ci d'une clé pour déchiffrer un message peut être facturée 400 F à l'administration requérante.

La réglementation encadre strictement les délais de réponse de l'administration, en considérant notamment que l'absence de décision expresse pendant quatre mois vaut autorisation tacite (sauf demande de pièces complémentaires par le SCSSI).

La mise en œuvre du nouveau cadre légal se heurte à certaines difficultés

Les milieux économiques ont largement approuvé la libéralisation des moyens de cryptologie servant à la signature électronique et à l'authentification des messages, ainsi que des moyens de chiffrement utilisant des clés de taille inférieure ou égale à 40 bits. En revanche, de nombreuses critiques se sont élevées quant au système des " tiers de séquestre ", en soulignant l'isolement de la position française au niveau international, les problèmes économiques soulevés par ce dispositif et son manque d'efficacité.

Il est certes un peu tôt pour porter un jugement sur l'efficacité de la nouvelle réglementation, dont la mise en œuvre n'a commencé qu'avec la publication des décrets d'application du 24 février 1998. On peut toutefois constater que la mise en place des " tiers de séquestre " est lente (aucun n'a encore été agréé et il semblerait n'y avoir que très peu de candidatures). En outre, les autorisations de fourniture et d'utilisation des moyens de cryptologie " forts " (i.e. clé de plus de 40 bits) restent difficiles à obtenir en pratique. Par conséquent, à l'heure actuelle, il reste quasiment impossible, en réalité, d'utiliser des moyens cryptologiques " forts ", sauf à confier les clés de chiffrement directement au SCSSI comme l'ont fait quelques entreprises. En outre, on peut s'interroger sur le caractère économiquement rentable de la fonction de " tiers de séquestre " et donc sur le niveau d'exigence posé par la réglementation. Au-delà de ces interrogations pratiques, qui trouveront peut-être des réponses positives dans un proche avenir, un certain nombre d'éléments du nouveau dispositif juridique régissant la cryptologie en France sont préoccupants.

La première préoccupation tient à la **singularité de la position française** et à l'attitude qu'adopteront les autres pays développés en matière de cryptologie. La France est en effet la seule, à ce jour, à avoir instauré un système de " tiers de séquestre ". Or un tel mécanisme suppose le recours à des produits et une technologie très spécifiques, puisqu'il faut prévoir la remise automatique des clés de chiffrement à un organisme tiers, alors que quasiment aucun produit de cryptologie (logiciels notamment) commercialisé dans le monde à l'heure actuelle ne le permet. Il faudra donc développer des produits, assez complexes à concevoir, destinés aux seuls utilisateurs français, ce qui aura certainement des répercussions en termes de prix et donc de compétitivité pour les entreprises françaises. Ces dernières risquent en outre d'être gênées

dans leurs relations avec les entreprises étrangères qui ne manqueront pas de critiquer la fiabilité des " tiers de séquestre " et le risque d'interception des communications par les services de sécurité français.

Ces problèmes d'ordre économique risquent de rendre difficile le maintien du système des " tiers de séquestre " si une solution analogue n'est pas retenue par d'autres pays développés, au moins dans la Communauté européenne. Or l'Allemagne et le Royaume-Uni n'imposent aucune restriction à l'utilisation de la cryptologie et ne l'envisagent aujourd'hui qu'avec beaucoup de réticences et d'hésitations. Le Royaume-Uni ne paraît toutefois pas exclure totalement l'hypothèse d'un mécanisme de " tiers de séquestre " ou, à tout le moins, de recouvrement de clés. Cette question fait par ailleurs l'objet d'un vif débat aux États-Unis, qui ne restreignent que l'exportation des moyens de cryptologie d'un niveau de protection élevé.

La seconde interrogation que l'on peut avoir à l'égard du dispositif retenu par le Gouvernement pour régir la cryptologie tient à son **efficacité**. Le système des " tiers de séquestre " est relativement contraignant pour les utilisateurs, et potentiellement coûteux pour les entreprises comme on l'a vu. Or on peut craindre que les délinquants se refusent à remettre leurs clés à des " tiers de séquestre " ou utilisent des méthodes de chiffrement difficilement détectables, par exemple des procédés de stéganographie (*i.e*. incorporation de messages codés dans des images numériques transmises apparemment " en clair "). Les services de sécurité font valoir que, dans ce cas, il sera toujours possible de sanctionner les délinquants pour violation des règles sur la cryptologie. Une telle réponse n'est néanmoins pas totalement satisfaisante, car il suffirait pour atteindre cet objectif de sanctionner le refus par une personne de remettre ses clés de chiffrement à la demande de la justice. Il ne paraît nullement nécessaire d'introduire le système complexe des " tiers de séquestre ".

Ces préoccupations ont d'ailleurs conduit tant la Commission supérieure du service public des postes et télécommunications, composée de parlementaires, que l'Autorité de régulation des télécommunications (ART) à se montrer très réservées sur les projets de décrets d'application de la loi du 26 juillet 1996 qui leur avaient été soumis.

Certains aménagements du cadre légal de la cryptologie pourraient être envisagés à terme

Si le Gouvernement souhaitait assouplir quelque peu les modalités d'application de la loi du 26 juillet 1996, les pistes de réflexion suivantes pourraient être explorées.

Il faudra tout d'abord, en tout état de cause, **veiller à réviser périodiquement la taille de la clé de chiffrement en deçà de laquelle l'utilisation des moyens de cryptologie est libre**. Le seuil actuel est fixé à 40 bits, mais il devra probablement être rehaussé à 56 bits très prochainement compte tenu de l'élévation rapide du niveau moyen de protection des produits de cryptologie commercialisés dans le monde. Le degré de protection doit en effet évoluer au rythme des progrès des technologies permettant le décryptage des messages.

En second lieu, **certaines exigences prévues à l'égard des " tiers de séquestre " pourraient sans doute être abandonnées**, notamment l'habilitation " secret défense " pour les personnes appelées à communiquer les clés à la police judiciaire ou aux services de sécurité. Une telle habilitation ne paraît en effet nullement nécessaire eu égard au rôle effectif des personnes concernées. Plus généralement, il faudrait que puissent être agréés au titre de " tiers de séquestre " un grand nombre d'organismes, ce qui impliquerait sans doute un assouplissement des contraintes posées par la réglementation (notamment sur les caractéristiques du système informatique utilisé, sur la permanence des personnels habilités à communiquer les clés...). Ainsi, le rôle de " tiers de séquestre " pourrait sans difficulté être assuré, par exemple, par les

fournisseurs d'accès à l'Internet à l'égard de leurs abonnés et par les organismes professionnels tels que les chambres de commerce et d'industrie ou les centres de gestion agréés à l'égard de leurs adhérents. On peut également envisager d'agréer des sociétés de conseil en informatique pour jouer ce rôle pour leurs clients. Un nombre élevé de " tiers de séquestre " permettrait aux entreprises, notamment les PME, d'y avoir plus facilement recours. Il faut d'ailleurs souligner que les entreprises ont un intérêt propre à l'existence d'un " tiers de séquestre ", puisque celui-ci pourrait leur remettre les clés de chiffrement utilisées par un employé qui refuserait de les communiquer à son employeur (par exemple après un licenciement) ou qui ne serait plus en mesure de le faire (s'il décédait).

En troisième lieu, on pourrait envisager que **des individus puissent jouer le rôle de " tiers de séquestre " à l'égard des employés de certaines organisations publiques ou privées**. Cette possibilité devrait toutefois être réservée à des organisations comptant un nombre élevé d'employés (*i.e*. grandes entreprises, établissements publics,...) afin que le responsable du séquestre des clés, qui pourrait être l'administrateur du réseau informatique, puisse avoir une certaine autonomie par rapport aux autres employés dont il détient les clés de chiffrement. Il serait également prudent de lui assurer une certaine indépendance par rapport à l'employeur, en lui conférant éventuellement le statut de salarié protégé. Le responsable du séquestre des clés devrait en outre être agréé par l'administration, qui pourrait exiger certaines garanties de compétence technique et de moralité. Des sanctions sévères seraient prévues pour le cas où il refuserait de livrer les clés qu'il détient et pour le cas également où il violerait le secret absolu auquel il serait astreint quant aux demandes de clés qui lui seraient faites (que ce soit en informant la personne concernée ou son employeur). Il faudrait également, naturellement, que le système technique de recouvrement et de conservation des clés offre des garanties de sécurité suffisantes, notamment quant aux modalités de communication des clés aux autorités habilitées à cet effet par la loi.

Par ailleurs, compte tenu du contrôle exercé sur les " tiers de séquestre " et de l'obligation pour les utilisateurs d'avoir recours à ces derniers, **la fourniture et l'importation de moyens de cryptologie comportant un dispositif de séquestre de clés (d'une taille supérieure à 40bits) devraient être soumises à une simple obligation de déclaration simplifiée** (et non subordonnée à autorisation comme actuellement). Il est en revanche important que cette déclaration permette au SCSSI de vérifier la fiabilité du système de recouvrement de clé et l'absence de faille technique permettant des interceptions notamment au profit de services d'espionnage étrangers (" back doors "). L'administration doit se voir reconnaître le pouvoir d'interdire l'utilisation en France des moyens de cryptologie présentant des défaillances à cet égard. Quant au contrôle sur les exportations, il doit être adapté aux engagements pris par la France dans ce domaine, notamment " l'arrangement de Wassenaar " du 19 décembre 1995 précité.

Enfin, **il serait très utile de constituer, auprès du Premier ministre (par exemple dans le cadre du SCSSI), un pôle technique doté des moyens matériels et informatiques nécessaires pour le décryptage des messages** qui lui seraient transmis par les services de police ou de sécurité dans le cadre des interceptions de correspondance autorisées par la loi. La création de ce pôle technique spécialisé permettrait de concentrer, au niveau interministériel, les moyens financiers nécessaires à l'acquisition d'équipements performants. Des conventions de coopération pourraient même être passées avec des laboratoires de recherche ou avec les services de décryptage d'autres gouvernements européens.

À plus long terme, il faudra tirer la conséquence des politiques menées en matière de cryptologie par les autres pays occidentaux, notamment les États membres de la Communauté européenne. **Il ne sera en effet possible de conserver durablement un dispositif de " tiers de séquestre ",**

relativement contraignant pour les entreprises, que si la réglementation française parvient à inspirer celle mise en œuvre par les autres pays développés. Sinon, il faudra se borner à exiger que les moyens de cryptologie utilisés en France permettent le recouvrement des clés à l'initiative de l'émetteur ou du destinataire du message, qui sera alors tenu de les remettre lui-même à la justice ou aux services de sécurité sous peine de sanctions pénales sévères. Le système du " tiers de séquestre " ne sera plus qu'une faculté offerte aux utilisateurs.

Chapitre 4

L'adaptation de la fiscalité au commerce électronique

Le fonctionnement de l'Internet rend difficile la mise en œuvre de certains concepts traditionnels de la fiscalité et le recouvrement des impôts et taxes.

Certaines règles apparaissent tout d'abord inadaptées ou difficiles à mettre en œuvre sur Internet. C'est le cas par exemple pour la TVA. Les sites marchands étrangers ignorent souvent les modalités de la taxation dans le pays de l'acheteur ou simplement le régime dont relève cet acheteur (assujettissement du client à la TVA, par exemple), ce qui les conduit par exemple fréquemment à vendre les biens et services hors taxes et à reporter sur le consommateur la charge d'acquitter les taxes et droits de douane, et rend très aléatoire la perception des sommes dues.

À cela s'ajoute l'impact de la géographie actuelle du commerce électronique et de la disparité des régimes de taxation (tous les États ne prélevant pas de taxe à la consommation par exemple). La taxation de certaines prestations au lieu du vendeur favorise certains États tiers à l'Union européenne, ou les entreprises de ces États, lorsque leur régime fiscal est plus favorable qu'au sein de l'Union.

Mais les principales difficultés concernent le recouvrement des taxes, compte tenu de la nature de l'Internet, réseau international, décentralisé, mettant les parties en relation sans intermédiaire, y compris parfois pour la livraison de biens " immatériels ", tels les logiciels téléchargés, qui rend difficile l'identification des transactions.

Les enjeux sont considérables pour les États membres de l'Union européenne sur lesquels pèse un réel risque budgétaire – la TVA représente en effet 18, 6 % des leurs recettes fiscales –, même si les risques ne sont pas immédiats, compte tenu notamment du volume modéré actuellement du commerce électronique.

Les enjeux sont aussi non négligeables pour les entreprises et les consommateurs. La disparité des régimes fiscaux peut conduire à des distorsions de concurrence au détriment des entreprises européennes. Les incertitudes sur le régime fiscal des transactions, le risque d'une éventuelle double imposition, ou le report de la charge fiscale sur le consommateur pourraient dissuader l'acheteur soucieux de ne pas méconnaître ses obligations fiscales ou douanières d'avoir recours au commerce électronique.

Il n'a pas été possible dans les délais impartis pour la remise de ce rapport, de mener l'étude approfondie que nécessite l'examen complet de cette question. Il apparaît d'ores et déjà que certaines adaptations importantes des règles fiscales seront requises, concernant notamment le régime de la TVA qui relève de la sixième directive européenne du 17 mai 1977 dont la modification requiert une approbation à l'unanimité des États membres de l'Union. Leur examen nécessite donc une concertation étroite avec toutes les parties concernées et rend en outre nécessaire une analyse des implications économiques et budgétaires des solutions juridiques proposées. Enfin, il y aurait lieu de tenir compte de nombreux travaux en cours dans les

enceintes internationales et notamment dans le cadre de l'Union européenne et de l'OCDE. Aussi, semble-t-il préférable de s'en tenir dans le cadre de ce rapport à la mention des **principales difficultés rencontrées** et à quelques indications sur des **voies à explorer pour permettre de fiscaliser les transactions sur Internet.** Il apparaît que la détermination de l'assiette est rendue difficile par la dématérialisation des transactions, mais que les principales difficultés concernent le recouvrement des impôts et taxes.

La détermination de l'assiette est rendue difficile par la dématérialisation des transactions

Il convient de distinguer le principal enjeu, le prélèvement de la TVA rendu difficile par la dématérialisation des opérations, d'un problème plus ponctuel affectant la fiscalité directe : l'interprétation à donner du concept d'établissement stable dans le cadre de transactions via un serveur Internet.

Le prélèvement de la TVA face à la dématérialisation des transactions

Les opérations qui donnent lieu à la livraison physique d'un bien commandé via Internet soulèvent peu de problèmes

Lorsque la commande est effectuée en ligne mais que la livraison donne lieu à la circulation physique de la marchandise dans l'Union européenne, il s'agit d'une vente à distance classique, portant sur un produit qui obéit au régime prévu par la 6e directive précitée.

Toutefois, l'augmentation du nombre de petits paquets (par exemple des disques compacts) rend plus difficile les contrôles en douane. Aujourd'hui, ces biens sont taxables au premier franc, la France ayant fait le choix de les exclure de la franchise douanière que le droit communautaire autorise. Il sera donc sans doute nécessaire de **renforcer les contrôles douaniers et de développer de nouveaux systèmes de contrôle avec les transporteurs de fret express**, ce qui suppose de pouvoir accéder à leurs systèmes informatiques (les douanes et contributions indirectes britanniques ont par exemple négocié avec les transporteurs, offrant en contrepartie la mise en place de procédures simplifiées d'importation). Des solutions pratiques peuvent être trouvées avec les transporteurs à travers notamment la passation de conventions. Des conventions types pourraient être élaborées au niveau communautaire. Ce système, d'un grand intérêt pratique, favoriserait toutefois les gros transporteurs. Aussi, serait-il souhaitable d'évaluer l'opportunité **d'introduire, en concertation avec les autres États membre, une franchise sur l'importation de biens d'un faible montant**.

Les difficultés pour prélever la TVA sur les services en ligne ou sur les biens " immatériels " sont plus sérieuses

? *La première difficulté concerne la nature même des transactions sur Internet et le régime des biens " dématérialisés "*

Lorsqu'un contrat relatif à un service est passé en ligne mais que la consommation a lieu hors ligne (voyage par exemple), il s'agit d'une traditionnelle prestation de services. En revanche, se pose la question délicate de la qualification juridique des biens ou services qui sont non seulement commandés mais aussi téléchargés en ligne, sans transit physique ou sans prestation hors ligne. C'est le cas notamment des logiciels et des enregistrements de musiques ou de films. Les États-Unis soutiennent qu'il convient de retenir dans ce cas la qualification nouvelle de " biens virtuels " et rejettent la qualification de service. Le terme est utilisé pour qualifier un bien d'une nouvelle nature correspondant à un produit qui est traditionnellement livré sous forme

physique mais qui peut aussi prendre une forme immatérielle. La Commission européenne et le Service de la Législation Fiscale sont plutôt d'avis que les logiciels et autres produits dématérialisés relèvent de la qualification de service dès lors qu'il n'y a pas livraison physique du bien. Les implications de cette qualification sont importantes. La qualification de service emporte notamment des conséquences sur le régime des droits de douane et sur le traitement de la transaction au regard des règles de la TVA.

La **qualification de service semble la plus adaptée**, elle est néanmoins susceptible d'engendrer certains effets pervers en l'état de la législation sur la TVA.

? *Les risques afférents à la mise en œuvre d'une doctrine unilatérale*

Actuellement, les biens " immatériels " sont assimilés à des prestations de service, au titre du " traitement de données et fourniture d'information " (article 259 CGI). Une interprétation unilatérale peut toutefois conduire à un risque de double imposition ou au contraire d'absence de taxation. Cette qualification n'est pas non plus sans inconvénient sur les règles de perception de la TVA, au regard du régime actuel prévu par la 6e directive précitée, dans la mesure où elle oblige l'entreprise étrangère à désigner un représentant fiscal en France.

Il est sans doute **souhaitable sur ce point de rechercher une solution concertée au niveau européen. Ranger clairement les " biens immatériels " dans la catégorie des prestations de service, en retenant le principe de la taxation au lieu de consommation**, permettrait d'harmoniser les règles relatives à la détermination du lieu d'imposition, tout en limitant les risques d'évasion fiscale, et d'assurer une concurrence équitable entre opérateurs. Il conviendrait toutefois de prêter attention à un risque de disparité de traitement des produits culturels selon qu'ils sont qualifiés de bien ou de service, sachant qu'ils bénéficient sous leur forme matérielle d'un taux réduit de TVA, très nettement inférieur au taux de TVA applicable à une prestation de service. En outre, l'obligation imposée aux opérateurs de pays tiers de désigner un représentant fiscal ne doit pas être perçue comme contraire aux engagements pris par les États membres de l'Union dans le cadre des récents accords de l'Uruguay Round sur la libre commercialisation des services de télécommunications à valeur ajoutée. Il serait par exemple préférable de prévoir **qu'un représentant fiscal unique soit désigné dans l'Union** (abandon de l'obligation de désigner un représentant dans chaque État membre), qui pourrait déclarer la TVA dans chacun des États en appliquant les taux en vigueur dans cet État.

Des difficultés résultent enfin de l'application des règles actuelles de territorialité

Lorsque le preneur du service (client) est établi en France, qu'il est assujetti à la TVA (personne physique ou morale), et que le prestataire de service est établi à l'étranger, la taxe est due par le client français, qui doit en principe la déclarer et la payer de sa propre initiative (article 259 B et C du CGI).

Lorsque le prestataire de service est établi hors de l'Union européenne et que l'acheteur n'est pas assujetti à la TVA, le prestataire de service étranger est en principe redevable de la taxe (article 283-1 CGI). Il est tentant pour lui " d'oublier " la TVA française qu'il doit théoriquement acquitter par l'intermédiaire d'un représentant fiscal , ce qui est très fréquent en pratique. À défaut de désignation d'un représentant fiscal, le Trésor est en droit de réclamer la TVA au destinataire de l'opération.

Ces deux cas sont susceptibles de poser des problèmes pratiques sérieux. Lorsque le destinataire est redevable de la taxe, il sera difficile de la prélever sans déclaration spontanée, compte tenu de la difficulté à identifier l'acheteur et la transaction en ligne. Lorsque le prestataire est redevable de la taxe, il sera encore plus difficile de collecter la taxe compte tenu de la localisation de

l'obligation.

Certaines difficultés pourraient résulter des critères retenus pour déterminer le lieu de taxation du service. Pour certains services, il s'agit du lieu d'établissement du fournisseur, en vertu de l'article 9 de la sixième directive précitée. C'est le cas pour les prestations d'agences de voyages qui connaissent un fort développement sur l'Internet. Les risques de délocalisation et de distorsion de concurrence sont réels. Il conviendrait donc sans doute **d'harmoniser les règles de territorialité prévues à l'article 9 de la sixième directive et de prévoir que tous les services sont taxés au lieu de la consommation**. Une telle modification supposerait d'achever l'harmonisation des taux de TVA en Europe pour éviter des distorsions au sein de l'Union.

L'impôt sur les sociétés et le problème de l'interprétation du concept d'établissement stable

En France, les règles de territorialité dans l'imposition des bénéfice des sociétés résultent de l'application combinée du code des impôts (article 209-I CGI) et de conventions internationales destinées à prévenir les risques de double imposition. Une société étrangère n'est soumise à l'impôt sur les sociétés que si elle dispose d'un établissement stable en France et si elle perçoit des revenus de source française. De même, une entreprise française ne sera imposable en France sur ses recettes à l'étranger que si elle n'y dispose pas d'un établissement stable.

La notion d'établissement stable est définie par une convention modèle de l'OCDE comme une installation fixe d'affaires par l'intermédiaire de laquelle une entreprises exerce tout ou partie de son activité. Trois critères doivent donc être réunis : une installation d'affaires, c'est-à-dire des locaux, machines... ; l'installation doit être fixe c'est-à-dire dotée d'un certain degré de permanence ; l'entreprise doit enfin exercer son activité par l'intermédiaire de cette installation.

En pratique, **l'application du concept d'établissement stable aux serveurs Internet est très délicate**. Selon l'interprétation dominante en France, un simple serveur relayant l'offre commerciale d'une entreprise étrangère ne devrait pas être qualifié d'établissement stable si cette entreprise n'a pas de personnels propres en France et que le serveur " ne fait que permettre la connexion, stocker et transmettre les informations et les données " . Cette interprétation est toutefois contestée par certains États qui souhaitent taxer les serveurs (notamment l'Autriche). Cette question est très délicate et appelle une réponse coordonnée au plan international. Il faudra considérer soit que le serveur peut constituer un établissement stable si certains éléments de permanence sont réunis (le critère du personnel est-il dans ce cas adapté ?), soit considérer que le serveur constitue un établissement stable en soi, soit au contraire exclure totalement cette qualification au motif que le serveur peut être déplacé et surtout, qu'à la différence d'un intermédiaire traditionnel, il ne participe pas à la vente.

Ce concept doit donc faire l'objet d'une interprétation claire et harmonisée en prenant en considération les conséquences de l'absence de taxation d'un serveur. En pratique, alors que dans une vente traditionnelle l'intermédiaire commercial étranger est assimilé à un établissement stable et imposable en France, la vente d'un bien immatériel ne permet pas de taxer la marge en France. Il y a donc un risque que les entreprises étrangères échappent à l'impôt en France, voire qu'elles échappent totalement à l'impôt si l'État du lieu d'établissement de l'entreprise renonce à taxer les bénéfices réalisés à l'étranger via l'Internet. Dans le second cas, une sérieuse distorsion des conditions de concurrence s'ajoute à la perte fiscale pour le budget de l'État.

Il importe donc, comme le suggérait le rapport de M. Lorentz sur le commerce électronique, de **trouver une solution à cette réelle difficulté dans le cadre de l'OCDE** en recherchant les possibilités d'éviter que la vente des biens immatériels échappe à toute taxation dans le pays où la marge est réalisée.

Le recouvrement des impôts et taxes se heurte à de sérieuses difficultés

La principale difficulté identifiée concerne le recouvrement des taxes à l'occasion de transactions électroniques dématérialisées et sans intermédiaire : comment identifier les parties ? Auprès de qui procéder au recouvrement des taxes ?

Les caractéristiques d'Internet rendent difficiles l'identification des transactions et le recouvrement des impôts et taxes

Internet revêt un caractère transfrontière et fonctionne sans contrôle central. Les acheteurs et les vendeurs sont en relation directe, sans intermédiaire, y compris le cas échéant pour la livraison d'un bien s'il présente un caractère immatériel (téléchargement d'un logiciel ou d'un enregistrement par exemple). Internet permet en effet la commande et la livraison en ligne de biens sans livraison physique et donc sans possibilité de contrôle douanier. Le paiement lui-même n'est pas nécessairement effectué par l'intermédiaire d'une banque. Il est donc difficile d'identifier les transactions et les opérateurs. Ce point est particulièrement préoccupant pour l'administration fiscale qui impose fréquemment des obligations déclaratives aux intermédiaires et notamment aux banques.

En second lieu, la localisation et l'identification de l'acheteur et du vendeur sont difficiles à établir. Une localisation apparente peut être fictive tant il est facile et peu coûteux de déplacer un serveur Internet. En outre, le lien entre une adresse Internet ou un nom de domaine et l'identité d'une personne ou l'identification d'une entreprise n'est pas assuré. Par ailleurs, l'information sur Internet est volatile et difficilement traçable. Lorsque des données sont conservées, elles le sont souvent dans des États tiers. Or, il va de soi que la détermination de la localisation géographique d'une transaction et son identification sont indispensables pour permettre le prélèvement fiscal.

Évaluer la possibilité d'associer des tiers

S'en remettre entièrement aux déclarations spontanées des parties à la transaction n'apparaît pas une solution très satisfaisante compte tenu notamment des difficultés rencontrées pour les identifier. Diverses **voies devraient être explorées pour associer des tiers au recouvrement des taxes, ou au moins à l'effort d'identification des parties et des transactions**. Ces tiers pourraient être soit les banques et fournisseurs d'accès qui interviennent dans la transaction, soit des services spécifiques de certification fiscale.

L'idée la plus séduisante consiste sans doute à faire **opérer une retenue fiscale par les intermédiaires financiers**. Cette perspective paraît réaliste sur un plan technique lorsque les paiements sont effectués par carte de crédit. Les protocoles de transaction électronique inviolables SET intègrent un système de certification numérique qui associe le titulaire de la carte et le vendeur à la banque. Cette solution suscite toutefois des réserves : elle suppose que les banques acceptent de transmettre ces informations et un encadrement juridique strict pour veiller au respect du secret bancaire ; elle ne serait véritablement opérationnelle que si l'usage de la carte de crédit devenait le principal mode de paiement dans le cadre des transactions électroniques, ce qui n'est pas certain ; enfin, elle conduit les opérateurs à affirmer qu'il suffirait de faire appel à des intermédiaires de paiement dans les États qui exigeront le moins d'informations.

Au total, **il est clair qu'il n'existe pas de solution simple à ces difficultés, et qu'une approche purement nationale est vouée à l'échec dans ce domaine**. Il conviendra donc de poursuivre la réflexion et d'aborder ces différentes questions dans trois enceintes internationales : l'Union

européenne pour la fiscalité indirecte, l'OCDE pour la fiscalité directe, et l'OMC pour les droits de douane. La priorité doit consister à rechercher les moyens d'adapter le cadre juridique actuel afin de permettre le prélèvement des impôts existants et notamment la TVA. Ce n'est que si cette tentative échoue que devra être appréciée la possibilité d'introduire de nouvelles modalités d'imposition. La création d'une taxe forfaitaire, la " bits tax ", a été suggérée. Elle ne paraît pas satisfaisante : elle ne grève pas les transactions mais l'ensemble des messages, sans tenir compte de la valeur ajoutée des contenus véhiculés sur le réseau. Elle constituerait donc un sérieux frein au développement de l'Internet.

Chapitre 5

Noms de domaine et droit des marques

Le Gouvernement des États-Unis a rendu public, le 5 juin dernier, un *Livre blanc* définissant les grandes lignes de la réforme qu'il envisage concernant l'architecture des noms de domaine. Le système des noms de domaine (DNS) est en quelque sorte la " colonne vertébrale " de l'Internet, et les États-Unis en ont à l'heure actuelle la totale maîtrise sur un plan technique. Les principaux éléments de ce document, qui fait suite au *Livre vert* publié en février, seront exposés plus loin. Mais il semble que les autorités américaines soient décidées à mettre en œuvre la réforme du DNS dans les tout prochains mois, ce qui appelle une réaction rapide de la Communauté européenne pour assurer un droit de regard international sur l'évolution des noms de domaine.

Les propositions qui sont présentées dans le présent rapport pourraient inspirer la position que le Gouvernement français défendra au sein de la Communauté européenne, en vue de négociations internationales qui pourraient, par exemple, se dérouler dans le cadre ou avec l'appui de l'Union internationale des télécommunications (UIT) ou de l'Organisation mondiale de la propriété intellectuelle (OMPI) . Ces propositions, qui sont d'ordre juridique et technique, visent à améliorer, au niveau international, le système actuel d'attribution des noms de domaine, en veillant au respect du droit des marques qui assure une protection essentielle pour les entreprises françaises. Certaines suggestions pourraient également s'appliquer au domaine français " .fr ".

Les modalités actuelles d'attribution des noms de domaine sont peu satisfaisantes pour les titulaires de marques et pour les États

Le système actuel des noms de domaine est critiquable à un double titre : il est très peu respectueux du droit des marques, et son évolution est, à l'heure actuelle, essentiellement guidée par les intérêts des États-Unis, en méconnaissant largement la souveraineté des autres États.

Présentation du système des noms de domaine (DNS)

Tout site sur Internet est désigné par un nom de domaine (par exemple " sncf.fr "), qui est en quelque sorte l'équivalent du nom abrégé pour les serveurs télématiques (ex. " 3615 SNCF "). Chaque nom de domaine est associé à une adresse " IP " (*Internet Protocol*), c'est-à-dire à l'adresse numérique attribuée à chaque ordinateur raccordé à Internet (par exemple 147.173.81.1). Tout nom de domaine comprend au moins un suffixe (ex. sncf.*fr*), également appelé " domaine de 1er niveau " ou encore " TLD " (*Top Level Domain*). Ce TLD peut correspondre à un code pays (par exemple, " .fr " pour la France, " .us " pour les États-Unis,...). Mais il peut également s'agir d'un domaine générique appelé " gTLD " (*generic Top Level Domain*) ; ce type de domaine a été développé aux États-Unis mais a acquis en pratique un caractère international. À l'heure actuelle, il existe trois " gTLD " : " .com " pour les entreprises commerciales (ex. *coca-cola.com*), " .org " pour les organismes à but non lucratif et " .net " pour les organismes dont l'existence même est liée à Internet. Il faut ajouter " .int " qui est réservé aux

organisations internationales (ex. *onu.int*).

L'attribution des noms de domaine relève de *l'Internet Assigned Numbers Authority (IANA)*, organisme de droit américain qui a reçu un mandat à cet effet de la part du Gouvernement américain *(Federal Networking Council*) et de *l'Internet Society (ISOC)*, première association mondiale d'utilisateurs d'Internet.

L'attribution des adresses numériques " IP " a été déléguée par l'IANA à trois organisations régionales : le RIPE pour l'Europe, l'APNIC pour l'Asie-Pacifique et l'ARIN pour l'Amérique et les autres pays.

L'attribution des noms de domaine a, quant à elle, été déléguée à divers organismes. Les domaines nationaux sont gérés par des organes publics ou privés désignés par chaque pays (par exemple l'association AFNIC, sous tutelle de l'État, pour le " .fr "). Les domaines " génériques " (gTLD) sont gérés par la *National Science Foundation* américaine. Toutefois, dans la pratique, celle-ci a délégué cette tâche, jusqu'en septembre 1998, à l'entreprise américaine *Network Solutions Inc. (NSI)* pour ce qui concerne l'enregistrement des nouveaux noms de domaine, et à la société ATT pour ce qui concerne la gestion du registre central des noms de domaine *(Domain Names System Root Server)*. La structure de coopération entre ces deux sociétés est appelée *" InterNIC " (International Network Information Center).*

Pour mieux apprécier l'importance des domaines génériques (gTLD), il faut observer que près de deux millions de noms de domaine sont enregistrés sous le gTLD " .com " (entreprises commerciales). On ne peut que constater, par comparaison, la faiblesse relative du nombre des noms de domaine enregistrés dans les domaines nationaux. Ainsi, le " .fr " ne compte que 16 000 noms de domaine et le " .de " (Allemagne) environ 120 000.

Les difficultés liées au développement incontrôlé des domaines génériques internationaux

Le premier problème est une question de principe. Il ne paraît plus justifié aujourd'hui, compte tenu du caractère transfrontière d'Internet, que le système des noms de domaine et particulièrement les domaines génériques soient gérés exclusivement par des entités américaines. En outre, la société commerciale NSI bénéficie, sans aucune justification, d'un monopole sur l'attribution des noms de domaine dans le " .com " et dans plusieurs autres domaines génériques. Cette position dominante est une source importante de revenus pour NSI puisque l'enregistrement et la conservation d'un nom de domaine sont actuellement facturés 70$ (auxquels s'ajoute une redevance annuelle de 35$). Le Gouvernement américain a toutefois annoncé que le monopole de NSI prendrait fin d'ici la fin du mois de septembre 1998.

Le deuxième type de difficultés tient à la mauvaise articulation du système des noms de domaine avec le droit des marques. La jurisprudence récente considère, en règle générale, qu'un nom de domaine est susceptible de porter par lui-même atteinte au droit des marques : c'est-à-dire que le seul fait pour une personne de se faire attribuer un nom de domaine correspondant à une marque dont elle n'est pas propriétaire l'expose à une action en contrefaçon de la part du titulaire de cette marque (voir notamment : TGI Paris, ord. référé, 25 avril 1997, *Framatome c/ Association Internaute* ; TGI Draguignan, 21 août 1997, *Commune de Saint-Tropez c/ Sté Eurovirtuel*). La jurisprudence étrangère va dans le même sens (voir par exemple : Cour de Braunschweig (RFA), 28 janvier 1997, pour le site *" Braunschweig.de "* ; Cour de district de Californie (USA), 23 avril 1996, pour le site *" Juris.com ").*

Cette jurisprudence soulève des difficultés compte tenu du caractère " universel " des noms de domaine enregistrés sous un domaine générique (gTLD), notamment le " .com ". En effet, ce

caractère mondial et général du nom de domaine s'oppose aux principes de territorialité et de spécialité du droit des marques : pour bénéficier d'une protection juridique dans un pays donné, il faut nécessairement y enregistrer sa marque sauf dans quelques pays où le simple usage d'une marque permet d'être protégé, mais là aussi seulement dans le pays concerné. En outre, cette protection ne porte que sur une ou plusieurs classes de produits donnés (sauf pour ce qui concerne les marques " notoirement connues "). De ce fait, il est très fréquent que coexistent des marques homonymes dans des pays différents, et souvent même, dans un pays donné, dans des classes de produits différents (par exemple, la marque " Montblanc " a été déposée par – au moins – deux entreprises différentes mais pour des produits distincts : les stylos pour l'une et les crèmes dessert pour l'autre).

Toutefois, le mode d'attribution des noms de domaine actuel ne permet pas d'assurer cette coexistence des marques homonymes. En effet, NSI pratique la règle du " premier arrivé, premier servi ", c'est-à-dire que la première entreprise qui enregistre un nom de domaine donné (par exemple *societe.com*) fait obstacle à ce qu'une autre entreprise, du même nom ou titulaire de la même marque, qui souhaiterait enregistrer ce nom puisse le faire. Or, compte tenu de la croissance très rapide des enregistrements en " .com " (5 à 7 000 nouveaux noms enregistrés chaque jour), le nombre de noms de domaine disponibles tend à se réduire fortement, d'autant plus que bon nombre d'entreprises pratiquent une politique de " réservation " de noms de domaine, à toutes fins utiles. On estime qu'à ce jour, plus de la moitié des noms de domaine en " .com " ne sont en réalité pas utilisés par leurs titulaires. Il en résulte un véritable " engorgement " du domaine " .com ".

En outre et surtout, la société NSI n'exerce aucun contrôle préalable sur les demandes d'enregistrement de noms de domaine. Contrairement à l'AFNIC (association française qui gère le domaine français " .fr "), NSI ne demande aucun justificatif de propriété industrielle (certificat de marque, extrait " K-bis " du registre du commerce et des sociétés,...). NSI se borne, dans le formulaire d'enregistrement, à faire figurer une clause par laquelle le demandeur déclare qu'à sa connaissance, il ne préjudicie pas aux droits d'un tiers. La portée juridique d'une telle clause contractuelle est évidemment très relative... Il résulte de cette absence de contrôle une forme de " piratage " qui pénalise particulièrement les entreprises titulaires de marques notoires. En effet, un certain nombre de personnes, voyant là une source de profit aussi facile qu'illicite, ont enregistré en " .com " des marques notoires (Mac Donald, Framatome,...) en vue de revendre les noms de domaine aux titulaires des marques correspondantes, moyennant bien sûr une " commission ". En dépit de la jurisprudence favorable aux titulaires de marques, la plupart des entreprises préfèrent reprendre le nom de domaine à l'issue d'une transaction amiable avec le titulaire de celui-ci, estimant cette solution plus rapide, plus discrète et généralement moins coûteuse qu'une procédure judiciaire.

Il faut ajouter qu'aucune convention internationale ni aucune règle jurisprudentielle ne fixe aujourd'hui avec certitude la loi applicable en cas de litige entre deux titulaires de marques homonymes enregistrées dans des pays différents et souhaitant obtenir le même nom de domaine dans le " .com " (ou un autre domaine générique international). Par conséquent, il y a là une grande source d'insécurité juridique. De plus, il est à craindre qu'aussi longtemps que la gestion des domaines génériques sera assurée exclusivement par des organismes américains, ceux-ci appliqueront le droit américain, qui se trouvera ainsi privilégié dans la pratique.

Plus généralement, on constate aujourd'hui que le système d'attribution des noms de domaine a été conçu essentiellement par des informaticiens selon une logique technique. Les considérations juridiques, et notamment l'articulation avec le droit des marques, commencent seulement à être prises en compte et encore avec beaucoup de réticences.

Les réformes proposées par le " Comité international ad hoc "

(IAHC) puis par le Gouvernement américain

Compte tenu des problèmes soulevés par le mode actuel d'attribution des noms de domaine, *l'Internet Assigned Numbers Authority (IANA)* et *l'Internet Society (ISOC)* ont pris l'initiative de constituer un groupe de travail intitulé " Comité international *ad hoc* " (IAHC), dont les recommandations ont été publiées en février 1997 . Le gouvernement américain s'est toutefois opposé à leur mise en œuvre. Il a formulé à son tour une série de propositions dans un *Livre vert* publié en février 1998, dont les principales orientations ont été confirmées dans le *Livre blanc* rendu public au mois de juin.

L'approche de l'IAHC est intéressante dans son principe mais perfectible dans ses modalités

L'IAHC a affirmé que " l'espace de nommage est une ressource collective dont la gestion doit être d'intérêt public ". Le comité en a déduit que la gestion des noms de domaine devait être placée sous le contrôle d'une entité internationale à but non lucratif, qu'il proposait d'installer à Genève. L'IAHC a en outre estimé qu'il convenait de créer sept nouveaux domaines génériques (gTLD) , s'ajoutant à ceux déjà existants, afin d'offrir une alternative au domaine " .com ". L'IAHC proposait que l'attribution des noms de domaines dans ces nouveaux gTLD soit confiée à vingt-huit nouveaux bureaux d'enregistrement, équitablement répartis entre les différentes régions du monde. Ces bureaux, soumis à un cahier des charges commun, seraient en concurrence en termes de tarifs et de délais de traitement des demandes d'enregistrement de noms de domaine. En cas de litige, il était prévu que la loi du pays dans lequel se trouve le siège du bureau d'enregistrement serait applicable. Enfin l'IAHC a élaboré un système très complet de règlement des litiges, notamment en vue de lutter contre le " piratage " sur les noms de domaine .

Les quatre idées principales préconisées par l'IAHC, qui font d'ailleurs l'objet d'un consensus relativement large au sein de la communauté de l'Internet, sont intéressantes et doivent être explorées : le caractère international et à but non lucratif de la structure de régulation des domaines génériques (gTLD) ; la rénovation de la structure actuelle des domaines génériques (gTLD) ; la création de nouveaux bureaux d'enregistrement, répartis dans différents pays, et l'institution d'une procédure de médiation et d'arbitrage.

Toutefois, les modalités techniques préconisées par l'IAHC apparaissent souvent complexes et difficiles à mettre en œuvre, notamment en ce qui concerne la procédure de médiation et d'arbitrage. Surtout, la principale faiblesse de l'initiative de l'IAHC tient à son caractère essentiellement privé et donc à son absence de base juridique en droit international public. Or il est difficile d'admettre que la réforme des noms de domaine, qui affecte le droit des marques et donc la souveraineté des États, soit décidée sans associer les gouvernements. Ceci explique donc largement que le Gouvernement américain ait fait obstacle à la mise en œuvre effective de la réforme élaborée par l'IAHC et qu'il ait souhaité garder un contrôle, au moins à titre transitoire, sur l'évolution du système des noms de domaine.

La réforme envisagée par le Gouvernement américain comporte quelques aspects positifs mais elle manque de légitimité internationale

Le Département du Commerce américain *(National Telecommunications and Information Administration – NTIA)* a publié en février 1998 un *Livre vert* intitulé *Proposition pour améliorer la gestion technique des adresses et noms de domaine sur Internet* . Ce document propose, pour l'essentiel, que l'IANA soit érigée en société à but non lucratif de droit américain, dont le conseil d'administration associerait des représentants des différents acteurs privés de l'Internet, à l'exclusion de tout représentant des États ou organisations internationales. Ce nouvel organisme de régulation du système des noms de domaine resterait provisoirement sous le

contrôle du gouvernement américain. Le *Livre vert* prévoit également la fin progressive du monopole de la société NSI et la mise en concurrence des bureaux d'enregistrement .

À la suite des commentaires qui ont suivi la publication de ce document, le Gouvernement américain a rendu public, le 5 juin, un *Livre blanc* exposant les orientations qu'il a finalement retenues en matière de noms de domaine. L'ensemble des principes du *Livre vert* décrits ci-dessus est repris. Le *Livre blanc* admet toutefois que la détermination de la loi applicable est un problème délicat et qu'il convient que l'organisme de régulation du système des noms de domaine (DNS), qui remplacera l'IANA, essaie de le résoudre en liaison avec l'OMPI. Cette dernière se voit en outre reconnaître un rôle central dans la mise en place de la structure de médiation et d'arbitrage.

Le Gouvernement américain renvoie au futur organisme de régulation le soin de régler ce problème ainsi que tous ceux qui sont posés par le système actuel des noms de domaine. Le *Livre blanc* suggère néanmoins différentes pistes de réflexion .

Comme l'ont relevé à juste titre le Conseil de l'Union européenne et la Commission européenne dans une lettre commune adressée au Gouvernement américain le 16 mars 1998, le principe d'une réforme décidée unilatéralement par les États-Unis n'est pas acceptable pour les pays européens. En effet, la structure de la future autorité de régulation destinée à remplacer l'IANA n'a pas un caractère suffisamment international. Il s'agit d'une entité de droit privé américain, qui se trouve donc de ce fait exposée à n'importe quelle modification de la législation ou de la réglementation décidée unilatéralement par les autorités américaines. En outre, elle n'associe pas de représentants d'autres États ni d'organisations intergouvernementales telles que l'UIT ou l'OMPI. Un tel organisme ne bénéficie donc d'aucune véritable légitimité internationale, en tout cas en droit international public.

Cette affirmation unilatérale de la suprématie américaine sur la gestion des noms de domaine ne peut donc pas être admise. En revanche, certaines orientations du *Libre blanc*, qui ont d'ailleurs de nombreux points communs avec celles de l'IAHC, pourraient être retenues au niveau international. Elles ont donc en partie inspiré les propositions exposées ci-dessous.

Propositions pour rationaliser l'attribution des noms de domaine tout en protégeant les titulaires de marques

Le système des noms de domaine (DNS) doit être régi par trois principes fondamentaux :

1. les noms de domaine sont une ressource publique, qui n'est pas illimitée, et qui doit donc être gérée dans un but d'intérêt général ;

2. quel que soit leur statut juridique (privé ou public), les organes de régulation du DNS doivent avoir un caractère international, comme le DNS lui-même. Les principes essentiels du DNS doivent en outre être définis dans le cadre de l'organisation internationale la plus appropriée ;

3. le DNS doit respecter le droit de la propriété industrielle, notamment le droit des marques.

L'application de ces principes conduit à plusieurs propositions concernant l'organisme de régulation du système des noms de domaine, l'architecture de celui-ci et les mécanismes de règlement des litiges. Ces propositions peuvent également être transposées, dans une large mesure, au domaine français " .fr ".

L'organisme de régulation du système des noms de domaine

La proposition du Gouvernement des États-Unis tendant à confier la régulation du DNS à un organisme privé à but non lucratif (tel qu'une association ou une fondation), de droit américain, ne semble pas pouvoir être remise en cause. Pourtant, compte tenu du caractère international de l'espace de nommage, notamment des domaines " génériques " (gTLD), et eu égard à la mission d'intérêt général qui lui est confiée, il aurait sans doute été préférable que cette régulation soit assurée par une organisation internationale. À défaut, **il est indispensable, à tout le moins, que l'organisme de régulation du DNS dispose d'une sorte de " mandat " international**. Ce mandat définirait le cadre général du DNS en réaffirmant les principes exposés ci-dessus. Il pourrait être accordé à l'organisme de régulation par une organisation internationale telle que l'OMPI (Organisation Mondiale de la Propriété Intellectuelle), l'UIT (Union Internationale des Télécommunications) ou toute organisation appropriée, selon une forme et une procédure qui doivent être définies en concertation avec les autorités américaines (charte, convention, cahier des charges, agrément,...).

Par ailleurs, il est nécessaire que les différentes régions du monde, tout particulièrement l'Europe, soient représentées au sein du conseil d'administration de l'organisme de régulation . Ces représentants peuvent être des industriels et des utilisateurs. Les intérêts publics doivent être également pris en compte, en prévoyant des sièges au sein du conseil d'administration soit pour des organisations internationales telles que l'OMPI ou l'UIT, soit pour des organisations ".régionales." telles que la Communauté européenne.

L'organisme de régulation du DNS prendrait la succession de l'IANA (*Internet Assigned Numbers Authority*) et gérerait le *Domain Names System Root Server* (registre central des noms de domaine), actuellement situé aux États-Unis. Il définirait, dans le cadre général fixé par le " mandat " international précité, la structure des noms de domaine et les principales règles applicables au niveau international. Il serait par ailleurs seul compétent pour accorder et, le cas échéant, retirer l'agrément des " bureaux d'enregistrement ", chargés d'enregistrer les demandes de noms de domaine dans les domaines génériques (gTLD). Par ailleurs, l'organisme de régulation du DNS agréerait des structures de règlement extra-judiciaire des litiges, dont il fixerait les règles communes (voir *infra*).

Les bureaux d'enregistrement et la procédure d'attribution des noms de domaine

Les bureaux d'enregistrement

Les bureaux d'enregistrement (" registrars ") doivent être équitablement répartis à travers le monde comme le proposait l'IAHC. **Il serait sans doute préférable que ces bureaux soient des organismes à but non lucratif,** afin d'éviter les errements liés à une recherche excessive de rentabilité financière, comme le montre aujourd'hui l'exemple de la société NSI. Toutefois, afin de favoriser une certaine émulation entre les bureaux, **il faut permettre à chaque bureau d'enregistrer tout nom de domaine quel que soit le gTLD demandé**. Il serait dangereux qu'un bureau d'enregistrement, même s'il s'agit d'une structure à but non lucratif, dispose du monopole sur un gTLD (comme c'est le cas actuellement pour la société NSI sur le " .com "). En effet, dans ce cas, le règlement d'un litige entre les titulaires de noms de domaine dans le gTLD concerné et les titulaires de marques déposées dans d'autres pays risquerait, *de facto*, d'être soumis à la législation territoriale du pays dans lequel est situé le bureau d'enregistrement. Une telle solution donnerait un avantage injustifié aux entreprises qui ont déposé leur marque dans le pays dans lequel se trouve le bureau d'enregistrement. Il faut donc que les gTLD conservent leur caractère véritablement international, sans pouvoir être rattaché à un pays en particulier. En outre, des monopoles sur tel ou tel gTLD seraient sans doute contraires aux règles de concurrence tant américaines qu'européennes.

Par ailleurs, quelle que soit la solution technique retenue pour la gestion des registres des

domaines génériques (gTLD) (" registry "), il paraît essentiel que celle-ci soit neutre à l'égard des utilisateurs. Le choix d'un gTLD par un demandeur de nom de domaine doit correspondre uniquement à la nature du demandeur (association à but non lucratif – " .org ", organisation internationale " .int ",...) ou à son secteur d'activité (" .com ", " .net ",...). Ce choix ne doit pas être influencé par des tarifs différenciés selon les gTLD, en tout cas pour les domaines destinés aux entreprises commerciales. On pourrait ainsi envisager la création de nouveaux gTLD correspondant à des secteurs d'activité que les entreprises choisiraient en fonction de l'objet principal de leurs sites (voir *infra*).

La procédure d'attribution des noms de domaine

Afin d'assurer la cohérence du système des noms de domaine, il faut exiger un minimum d'harmonisation des " chartes de nommage " des bureaux d'enregistrement, sous le contrôle de l'organisme de régulation du DNS qui peut retirer son agrément aux bureaux ne respectant pas cette charte. Cette remarque pourrait d'ailleurs valoir également, avec des exigences minimales, pour les domaines nationaux (ex. *.fr,.us,...*).

Les bureaux d'enregistrement doivent faire un effort d'information préalable sur les principes du droit des marques auprès des demandeurs de noms de domaine. En revanche, compte tenu du faible nombre de litiges constatés sur l'actuel domaine " .com " et de la forte hostilité de la communauté Internet, **il ne paraît pas utile de pratiquer un contrôle *a priori* sur les demandes d'enregistrement**, qui serait nécessairement lourd et coûteux . Ce type de contrôle paraît d'autant plus difficile à mettre en œuvre que dans certains pays comme les États-Unis, les entreprises ont des " marques d'usage ", qui sont protégées bien que n'ayant pas fait l'objet d'un dépôt formel auprès de l'administration. Les déposants devraient cependant être invités à indiquer sur leur formulaire d'enregistrement s'ils sont titulaires d'un droit sur le signe distinctif correspondant au nom de domaine (marque, nom commercial,...) et à en préciser la nature et les références. **Il s'agirait d'une procédure purement déclaratoire permettant d'établir la bonne ou la mauvaise foi du déposant en cas de litige avec un titulaire de marque**.

Les bureaux d'enregistrement pourraient procéder à la publication en ligne des nouveaux noms de domaine enregistrés afin de faciliter les oppositions éventuelles. Ils devraient également prononcer, après un délai relativement bref (par exemple 6 mois), **la " déchéance " des titulaires de noms de domaine** qui n'ont pas d'utilisation effective des noms enregistrés. Les bureaux d'enregistrement devraient enfin permettre à toute personne intéressée, par une base de données en ligne, de connaître facilement les noms de domaine déjà existants.

Il convient, par ailleurs, que **les pouvoirs publics favorisent la constitution d'un annuaire international (" pages jaunes ") des sites présents sur Internet**, qui complétera utilement les moteurs de recherche et rendra moins crucial le problème du caractère mnémotechnique des noms de domaine, qui est à l'heure actuelle une priorité pour les entreprises.

L'articulation de l'architecture des noms de domaine
avec les principes du droit des marques

Deux solutions radicales paraissent devoir être écartées d'emblée. La première serait la suppression pure et simple des domaines génériques internationaux (gTLD), en ne laissant subsister que les domaines nationaux. Une telle solution paraît peu réaliste aujourd'hui en ce qu'elle irait totalement à l'encontre de la logique internationale caractéristique de l'Internet. La seconde option possible consisterait à considérer un nom de domaine comme une simple adresse électronique, analogue à un numéro de téléphone, et ne constituant pas, par lui-même, un usage de marque susceptible d'être constitutif d'une contrefaçon. Cette solution est cependant contraire à l'évolution de la jurisprudence et à l'esprit de la législation en matière de marques. Elle est en

outre vigoureusement rejetée par les entreprises qui ne veulent pas risquer de voir leur nom ou leur marque utilisés par des tiers sans aucun moyen juridique de les en empêcher.

Dès lors, différentes solutions, essentiellement d'ordre technique, peuvent être proposées afin de faciliter la coexistence de noms de domaine homonymes, grâce à un meilleur respect des principes de territorialité et surtout de spécialité du droit des marques.

Le principe de territorialité

Il paraît difficile, compte tenu du caractère international de l'activité de beaucoup d'entreprises disposant d'un site sur Internet, de leur imposer un nom de domaine correspondant à un pays donné et donc de transposer purement et simplement le principe de territorialité du droit des marques.

Par conséquent, si deux entreprises sont titulaires d'une marque homonyme dans des pays différents, pour des produits similaires, la seconde entreprise souhaitant disposer du nom de domaine correspondant à cette marque pourrait ajouter un spécifiant géographique (par exemple *entreprise.fr.com*) ou libre (*entreprise.sarl.com*). Une autre solution consisterait, pour les deux entreprises concernées, à accepter la mise en place d'une page d'accueil commune mentionnant les deux sites homonymes avec un court descriptif permettant à l'utilisateur de choisir le site auquel il veut accéder .

Le principe de spécialité

La création de nouveaux domaines génériques (gTLD) permettrait de mettre fin à la croissance excessive du domaine " .com ", et surtout de répondre au moins partiellement au principe de spécialité du droit des marques.

Il faut créer de nouveaux gTLD en nombre suffisant pour être relativement précis sur le secteur d'activité, mais sans qu'ils soient trop nombreux afin d'être facilement mémorisables par les utilisateurs d'Internet. C'est pourquoi un nombre de 15 à 20 nouveaux gTLD véritablement " sectoriels " paraît optimal. Ces gTLD pourraient s'inspirer de la nomenclature internationale des classes de produits (42) mais en la simplifiant pour la rendre facilement compréhensible par les utilisateurs (exemple : *.fin* pour les services financiers, *.alim* pour l'alimentaire, *.ind* pour l'industrie, etc.). Le domaine " .com " aurait dès lors vocation à n'être plus, à terme, qu'un gTLD parmi les autres, soit spécialisé (activités de négoce *stricto sensu*), soit " fourre-tout ". Ce domaine ne doit en tout cas plus être privilégié " par défaut " par les logiciels de navigation sur Internet ni par les moteurs de recherche. Bien au contraire, ceux-ci doivent rendre facilement accessible aux utilisateurs la liste des gTLD avec leur signification. Par ailleurs, l'idée de l'IAHC d'un domaine " .nom " pour les pages personnelles paraît devoir être retenue. Enfin, les gTLD actuels (*.org*,*.int* et *.net*) doivent être maintenus.

Cette " sectorisation " par type d'activité des gTLD devrait permettre la coexistence des marques homonymes correspondant à des produits différents, même si elles ont été enregistrées dans le même pays. Toutefois, dans les cas, sans doute assez rares, où les produits, bien que différents, correspondraient au même gTLD (par *exemple.ind*), le deuxième demandeur de nom de domaine pourrait ajouter un spécifiant (libre) (ex. *montblanc.stylos.ind* et *montblanc.dessert.ind*). Il sera également possible de recourir à la solution de la page d'accueil commune renvoyant vers chacun des deux sites.

Il est également possible de résoudre la difficulté du caractère unilingue des intitulés des domaines génériques (.com,.net), qui sont généralement inspirés de l'anglais. **Une solution serait d'attribuer à chaque gTLD un numéro plutôt qu'un nom.** Il appartiendrait alors aux logiciels de navigation, aux fournisseurs d'accès ou aux " serveurs de noms de domaine "

d'assurer la conversion d'un nom de gTLD, tapé par l'utilisateur dans sa langue maternelle (par exemple " .alim " ou " .food " pour le gTLD correspondant au secteur agro-alimentaire) en numéro du gTLD correspondant (par exemple " .1 ").

Il faudra par ailleurs veiller à ce que le Gouvernement américain opère le transfert sous le domaine national " .us " des domaines " .gov " et " .mil ", car il s'agit en réalité de domaines purement américains et non de domaines génériques. En ce qui concerne le domaine " .edu ", on pourrait éventuellement le conserver à titre de véritable domaine générique (gTLD) ouvert aux organismes éducatifs de tous les pays.

La détermination de la loi applicable et le règlement des litiges

Compte tenu du caractère territorial du droit des marques (voir *supra*), il ne paraît pas possible de déterminer une règle simple de résolution des conflits de lois lorsque deux titulaires de marques homonymes déposées dans des pays différents souhaitent disposer du même nom de domaine. Les demandes des deux entreprises sont aussi légitimes l'une que l'autre, même si l'une d'entre elles est propriétaire d'une marque " notoirement connue " au sens de l'article 6 bis de la Convention de Paris du 20 mars 1883. Et toute action judiciaire en contrefaçon contre le titulaire du nom de domaine correspondant à cette marque ne devrait en principe avoir qu'un effet relatif, restreint au pays dans lequel la marque est déposée, ce qui n'a pas grand sens eu égard au caractère international des noms de domaine. Par ailleurs, il n'y a aucune raison de privilégier la loi du pays dans lequel se situe le bureau d'enregistrement ni *a fortiori* celle du pays dans lequel se situe le registre central des noms de domaine, comme le suggère le *Livre blanc* américain. **La solution la plus appropriée de résolution des litiges est donc une procédure extrajudiciaire (médiation et arbitrage).**

Comme sur la question précédente, il paraît souhaitable de s'inspirer des travaux de l'IAHC et de l'OMPI, tout en proposant des améliorations notables, dont certaines sont d'ailleurs demandées par les autorités américaines dans le *Livre vert* et le *Livre blanc* sur les noms de domaine. La procédure de médiation et d'arbitrage " en ligne " doit être plus simple, plus rapide et donc moins coûteuse. Il faut en outre permettre une certaine concurrence, dans le cadre d'un cahier des charges strict, entre les structures d'arbitrage. L'organisme de régulation du DNS, qui agrée ces structures, doit veiller au respect de ce cahier des charges.

Le règlement des litiges serait ainsi confié, par la voie d'une clause incluse dans le contrat d'enregistrement, à un centre d'arbitrage choisi par le bureau d'enregistrement (par exemple – mais pas nécessairement – le centre de médiation et d'arbitrage de l'OMPI). Les parties au litige auraient la faculté de souscrire, au début de la procédure, à une clause compromissoire, par laquelle elles accepteraient de conférer à la médiation le caractère d'un arbitrage, dont la sentence les lierait juridiquement. À défaut de cette clause, les parties resteraient naturellement libres de saisir les tribunaux compétents à l'issue de la procédure de médiation. Afin d'inciter le titulaire du nom de domaine à accepter de recourir à l'arbitrage, le contrat d'enregistrement pourrait prévoir que le refus par le titulaire du nom de domaine de souscrire à la clause compromissoire en cas de litige entraînerait la suspension automatique du nom de domaine, voire même son attribution provisoire au requérant (si celui-ci justifie d'un titre de propriété industrielle sans que le titulaire du nom de domaine puisse en faire autant), jusqu'à l'intervention d'une décision juridictionnelle définitive.

Il appartiendrait aux centres d'arbitrage de définir un certain nombre de principes pour la résolution des conflits, qui seraient annexés à la clause compromissoire. L'organisme de régulation du DNS veillerait à l'homogénéité de ces principes. Ceux-ci pourraient s'inspirer des " lignes directrices " proposées par l'IAHC et l'OMPI. Ils devraient privilégier les titulaires de marques par rapport à ceux qui ne justifient d'aucun droit de propriété industrielle sur le nom de

domaine qu'ils utilisent . Dans le cas où le titulaire du nom de domaine et le requérant seraient tous deux titulaires d'une marque correspondant au nom de domaine litigieux et déposée pour des produits correspondant bien au gTLD en cause si celui-ci est sectoriel (par exemple " .net "), l'arbitre devrait proposer et, en cas d'échec de la tentative de médiation, imposer des solutions permettant la coexistence de noms de domaine identiques : spécifiants relatifs à l'activité (ex. *compagnie.aviation.com* et *compagnie.bus.com*) ou au pays d'origine (ex. *compagnie.fr.com* et *compagnie.us.com*), page d'accueil commune (renvoyant sur les sites homonymes des différentes entreprises), ou toute autre solution technique appropriée. La sentence de l'arbitre lierait le bureau d'enregistrement, qui serait tenu de l'exécuter.

Un tel dispositif, qui est simple, souple et rapide, permettrait de régler les litiges liés au droit des marques en évitant de mettre en place un contrôle *a priori* lors de l'enregistrement des noms de domaine, qui paraît lourd et peu réaliste à l'échelle internationale.

L'assouplissement souhaitable de la " charte de nommage " du domaine français (" .fr ")

La cellule du " NIC-France ", relevant de l'Institut National de la Recherche en Informatique et en Automatismes (INRIA), a assuré la mise en place du domaine " .fr " par délégation de l'IANA. Depuis le 1er janvier 1998, cette gestion a été transférée à une association sous tutelle de l'État, dénommée " AFNIC " (Association française pour le nommage Internet en coopération). Ses adhérents sont essentiellement des prestataires techniques (fournisseurs d'accès et d'hébergement) et des utilisateurs. Il existe aujourd'hui un peu plus de 16 000 sites enregistrés sous le " .fr ". La redevance d'enregistrement est actuellement, en fonction de l'option choisie, d'environ 400 F, à laquelle s'ajoute depuis cette année une redevance annuelle de 100 F.

Deux particularités de l'AFNIC doivent être signalées : la première est l'obligation pour les entreprises désirant obtenir un nom de domaine de passer par l'intermédiaire d'un prestataire technique inscrit auprès de l'AFNIC. La seconde est la " charte de nommage " du domaine " .fr ", qui définit les conditions d'attribution des noms de domaine. Cette charte prévoit d'une part qu'un nom de domaine ne peut être attribué qu'au titulaire du droit de propriété intellectuelle sur le nom correspondant. L'AFNIC exige donc un justificatif officiel (par exemple un certificat de marque ou un extrait " K-bis " du registre du commerce et des sociétés pour la raison sociale). La charte comprend d'autre part un " plan de nommage " qui subdivise le domaine " .fr " en sous-domaines tels que " .asso.fr " pour les associations, " .gouv.fr " pour les administrations, " .tm.fr " pour les marques, etc.

Il semble que l'AFNIC soit l'un des seuls bureaux d'enregistrement nationaux au monde à pratiquer un contrôle préalable très strict sur le droit du demandeur à obtenir un nom de domaine, en exigeant un document justificatif officiel. Ce contrôle préalable et le manque de souplesse de la charte de nommage semblent cependant dissuader un certain nombre d'entreprises françaises de s'enregistrer sous le " .fr ". Cette rigidité pourrait d'ailleurs expliquer, pour partie, que près de 25 000 noms de domaine en " .com " aient été enregistrés par des entreprises françaises qui ont préféré cette solution à celle du " .fr ". Cette forme de " délocalisation " s'explique également par la volonté d'entreprises présentes sur l'Internet de se positionner comme des entreprises internationales plutôt que comme des sociétés françaises.

La rigueur de la " charte de nommage " de l'AFNIC est parfois citée en exemple, notamment dans la mesure où elle évite le piratage de noms de domaine qui existe sur le domaine " .com ". Il paraît néanmoins nécessaire d'introduire davantage de souplesse dans la procédure d'attribution des noms de domaine afin de restaurer l'attractivité du domaine " .fr " pour les entreprises séduites par la souplesse de la procédure d'enregistrement sous le " .com ". Plusieurs solutions sont possibles :

– **l’une des solutions pourrait être de renoncer, purement et simplement, au contrôle préalable actuel et de ne pratiquer qu’un contrôle *a posteriori* en cas de litige.** La procédure déclaratoire et le mécanisme d’arbitrage proposés plus haut pour les domaines génériques (gTLD) pourraient tout à fait être appliqués en France ;

– **une autre solution consisterait à prévoir, au sein du domaine " .fr ", un ou plusieurs sous-domaines " libres " (par exemple " .lib.fr "), pour lesquels aucune pièce justificative ne serait exigée** (sauf celle établissant l’identité du demandeur). Les noms de domaine attribués dans ces conditions pourraient ainsi bénéficier soit à des personnes physiques, soit à des entreprises désirant ouvrir un site promotionnel ne correspondant pas nécessairement à une marque formellement déposée. Un système d’arbitrage en ligne permettrait de régler les litiges éventuels en s’inspirant des propositions exposées précédemment. La création d’un tel espace de liberté et de créativité paraît très important afin de prendre en compte les aspirations des utilisateurs de l’Internet et d’éviter qu’ils ne se détournent du " .fr " au profit des domaines génériques (gTLD).

Quelle que soit la solution retenue, il faut permettre l’enregistrement du nom de domaine, en ligne et sans délai, comme pour le " .com ", même s’il est demandé au titulaire d’adresser des pièces justificatives par courrier. Il ne paraît par ailleurs pas justifié d’exiger que toute demande de nom de domaine soit présentée obligatoirement par l’intermédiaire d’un prestataire technique inscrit auprès de l’AFNIC.

Plusieurs autres propositions sont par ailleurs déjà appliquées par l’AFNIC, notamment l’accès libre, en ligne, au registre des noms de domaine déjà attribués, la " déchéance " du nom de domaine en cas d’absence d’installation effective du site avant l’expiration d’un délai de 6 mois, l’instauration d’une redevance annuelle et l’élaboration d’un annuaire professionnel (type " pages jaunes ").

Quant aux sous-domaines prévus par le " plan de nommage ", ils paraissent dans l’ensemble appropriés. Toutefois, le " .tm " (pour les marques) paraît moins convaincant, car il ne permet pas de résoudre la coexistence de marques homonymes déposées pour des produits différents. **C’est pourquoi on pourrait le remplacer par des sous-domaines sectoriels tels que ceux qui ont été proposés précédemment pour les domaines génériques (gTLD).** On pourrait ainsi avoir un sous-domaine pour les activités financières (" .fin.fr "), un autre pour le secteur agro-alimentaire (" .alim.fr "), etc. Ces sous-domaines pourraient servir non seulement pour les sites correspondant à des marques, mais également pour ceux qui correspondent au nom commercial des entreprises.

En dernier lieu, il convient de mettre un terme rapide à l’exploitation, par des opérateurs privés n’ayant reçu aucun mandat de la part des autorités françaises, des domaines correspondant aux départements d’outre-mer (" .gp " pour la Guadeloupe, " .mq " pour la Martinique,...). L’IANA considère en effet qu’il s’agit de domaines " nationaux ". Le Gouvernement français devrait donc demander à l’IANA de refuser de reconnaître ces opérateurs et de leur attribuer des adresses " IP ". S’agissant de départements français, il n’y a en effet aucune raison que les noms de domaine correspondants ne soit pas enregistrés sous le " .fr ", le cas échéant par l’intermédiaire d’un correspondant de l’AFNIC situé dans chacun de ces départements. En revanche, on peut admettre, si les assemblées territoriales le désirent, que les habitants des territoires d’outre-mer puissent s’enregistrer dans les domaines " nationaux " correspondants (" .pf " pour la Polynésie française, " .wf " pour Wallis et Futuna, etc.). L’AFNIC pourrait apporter son concours technique pour la gestion de ces domaines.

En conclusion, sur la question des noms de domaine, il est proposé, de s’appuyer sur certains des principes affirmés par l’IAHC et le Gouvernement américain, qui font aujourd’hui l’objet d’un

large consensus parmi les acteurs de l'Internet, en y apportant les améliorations nécessaires à une bonne articulation entre le droit des marques et le mode d'attribution des noms de domaine.

Troisième partie

Valoriser les contenus par la protection de la propriété intellectuelle

Le marché des biens et des services protégés par le droit d'auteur représente environ 5 à 7 % du PNB de l'Union européenne. Toutefois, la part de ces services sur l'Internet demeure insignifiante sur un plan économique, alors même que le développement futur des réseaux numériques est très largement conditionné par la mise à la disposition du public de contenus susceptibles de l'intéresser. On constate en effet qu'à l'heure actuelle, tant les éditeurs traditionnels que les producteurs de musique ou d'œuvres audiovisuelles demeurent réticents à proposer des œuvres sur le réseau. Leur prudence est motivée par l'absence de système de paiement pratique et sûr, mais surtout par la peur de la contrefaçon. C'est pourquoi il paraît nécessaire d'améliorer la protection des titulaires de droits, tant en matière de propriété littéraire et artistique que de propriété industrielle, en déployant des moyens efficaces de lutte contre la contrefaçon.

Mais il convient, au préalable, de passer en revue les principales dispositions du droit de la propriété intellectuelle en vue de déterminer les adaptations rendues nécessaires par les spécificités de l'Internet et des réseaux numériques.

L'adaptation du régime de la propriété intellectuelle aux enjeux d'Internet et des réseaux numériques

En ce qui concerne tout d'abord le droit de la propriété industrielle, il ne semble pas qu'une adaptation de son régime juridique s'avère nécessaire, sauf en ce qui concerne la détermination de la loi applicable (conflits de lois et de juridictions) et la lutte contre la contrefaçon (voir *infra*). Le rapport du groupe de travail présidé, aux États-Unis, par M. Bruce Lehman en septembre 1995, dans le cadre de l'" Information Infrastructure Task Force " est d'ailleurs parvenu à la même conclusion. Cette différence de traitement entre la propriété littéraire et artistique et la propriété industrielle s'explique notamment, bien que cela puisse paraître paradoxal, par le caractère territorial plus marqué de la protection du droit des marques et des brevets d'invention : pour bénéficier d'une protection juridique dans un pays donné, il faut nécessairement y enregistrer sa marque ou son brevet, sauf dans quelques pays où le simple usage d'une marque permet d'être protégé, mais là aussi seulement dans le pays concerné . Les disparités entre les législations nationales, qui sont d'ailleurs assez limitées, ne sont donc guère susceptibles d'entraîner des effets pervers ou des délocalisations de sites, sous réserve du problème des noms de domaine qui a été examiné précédemment (partie II du rapport). On peut seulement souhaiter le développement de possibilités d'enregistrement de marques et brevets valables pour plusieurs pays . Mais cette évolution n'est pas liée spécifiquement au développement des réseaux numériques mais plus généralement à l'essor du commerce international. Cette question n'entre donc pas véritablement dans le champ de la présente étude.

En revanche, même si une remise en cause fondamentale du droit de propriété littéraire et artistique n'apparaît pas justifiée par le développement des réseaux numériques, certaines adaptations s'avèrent nécessaires et font d'ailleurs l'objet de négociations internationales et

même d'une proposition de directive communautaire .

L'état de la réflexion internationale

La doctrine est particulièrement féconde depuis quelques années sur la question de **l'adaptation du droit de la propriété littéraire et artistique aux spécificités de l'Internet**. Chaque jugement rendu dans ce domaine donne lieu à d'abondants commentaires de la part d'universitaires et d'avocats. La réflexion est en revanche généralement moins avancée au niveau des pouvoirs publics, qui restent encore relativement indécis sur les modifications à apporter aux législations nationales, même si des avancées conceptuelles significatives ont été réalisées dans les enceintes internationales et au sein de la Communauté européenne.

Les principaux éléments du débat international

L'Organisation mondiale de propriété intellectuelle (OMPI) veille à l'adaptation des conventions internationales existantes pour tenir compte des problèmes soulevés par le développement des réseaux numériques. En particulier, c'est sous son égide qu'ont été conclus deux traités en décembre 1996, sur le droit d'auteur d'une part, et sur les " interprétations et exécutions et les phonogrammes " d'autre part. Un nouveau traité est par ailleurs en cours de négociation actuellement sur les droits des artistes interprètes. Ces nouvelles conventions visent notamment à élargir le champ de protection des œuvres afin d'y inclure les nouveaux supports et modes de transmission, notamment numériques. Toutefois, elles n'ont pas, à ce jour, résolu les difficiles questions liées au champ des exceptions au droit d'auteur sur les réseaux ou à la loi applicable.

Par ailleurs, un accord très important a été conclu, dans le cadre de l'Organisation mondiale du commerce (OMC), sur " les aspects des droits de propriété intellectuelle qui touchent au commerce " (ADPIC). Cette convention a été annexée à l'accord de Marrakech du 15 avril 1994. Elle impose notamment aux 132 États signataires de respecter les principales règles fixées par la convention de Berne du 9 septembre 1886 sur la protection des œuvres littéraires et artistiques, ce qui a pour effet d'accroître sensiblement le nombre de pays appliquant la convention de Berne.

Les négociations internationales ayant conduit à l'adoption des ces conventions ont fait ressortir les spécificités du régime de protection de la propriété littéraire et artistique en France et dans plusieurs autres États européens, par opposition notamment au droit anglo-saxon. Le premier est d'essence humaniste, centré sur la personne même de l'auteur, alors que le second privilégie davantage les considérations économiques, notamment dans la mesure où il refuse de reconnaître le droit moral de l'auteur garanti par l'article 6bis de la convention de Berne sur la protection des œuvres littéraires et artistiques. Il conviendra de prendre en compte cette dimension symbolique, même s'il ne faut pas en exagérer l'importance en termes pratiques, dans la réflexion sur l'adaptation du régime de propriété littéraire et artistique au développement des réseaux numériques.

Ce débat théorique a d'ailleurs un prolongement très concret en matière de titularité des droits, comme on le verra plus loin. De nombreux éditeurs de produits multimédia estiment en effet que la conception française du droit d'auteur rend difficile l'acquisition des droits par l'employeur sur les œuvres de ses salariés et sur les œuvres de commande et qu'ainsi, les entreprises françaises seraient pénalisées par rapport à leurs homologues des pays anglo-saxons.

Cette critique contre le monopole de l'auteur, même salarié, sur son œuvre rejoint paradoxalement un second courant de pensée qui est lui aussi favorable à un amoindrissement du droit exclusif de l'auteur, mais pour des raisons diamétralement opposées à celles des producteurs. Face au désir des auteurs de protéger toujours davantage leurs œuvres contre la

contrefaçon, notamment par des moyens techniques, de nombreux intellectuels redoutent que la logique économique ne restreigne la circulation des idées et l'accès de tous à la culture. Cette préoccupation est partagée par certaines organisations internationales telles que l'UNESCO . Elle est également reprise par des gouvernements qui ont une tradition très forte d'exception au droit exclusif de l'auteur permettant notamment la libre utilisation des œuvres à des fins d'éducation et de recherche, en particulier dans les pays anglo-saxons (exception dite de " fair use ") et dans les pays du nord de l'Europe.

Néanmoins, sur un plan général, un consensus commence à se dégager sur l'idée que les principes fondateurs du droit d'auteur, posés notamment par la Convention de Berne sur la protection des œuvres littéraires et artistiques, ne sont pas véritablement affectés par l'essor des réseaux numériques. En revanche, plusieurs sujets font l'objet d'âpres débats : le premier est celui de la loi applicable. Le second est celui de la titularité des droits, avec notamment les questions liées au statut des auteurs salariés et au respect du droit moral de l'auteur. Ce sujet déborde néanmoins largement le champ de la présente étude sur les réseaux numériques. Seule la problématique générale sera donc exposée ainsi que les pistes de réflexion possibles. Enfin, le troisième grand débat est celui qui est lié au régime des exceptions au droit exclusif de l'auteur sur son œuvre, notamment l'exception de copie privée.

Les solutions ou les pistes de réflexion qui sont proposées dans ce rapport tentent donc de trouver un équilibre entre les aspirations légitimes des auteurs, dont les droits doivent être préservés dans l'environnement des réseaux, l'intérêt économique des entreprises, notamment à l'égard de leurs auteurs salariés, et enfin la préoccupation tout aussi justifiée de ceux qui veulent maintenir une certaine liberté d'accès à la culture et à l'information, et qui souhaitent tirer parti des potentialités offertes par l'Internet à cet égard.

La réflexion au niveau des États

Autant la doctrine universitaire est abondante, autant les documents exprimant officiellement et publiquement les intentions des différents gouvernements quant à l'adaptation de leur régime national de protection de la propriété littéraire et artistique aux spécificités des réseaux numériques sont rares.

Même les rapports officiels demeurent somme toute peu nombreux. On peut signaler, aux États-Unis, le rapport du groupe de travail présidé par M. Bruce Lehman en septembre 1995, dans le cadre de l'" Information Infrastructure Task Force " . Celui-ci concluait que les spécificités de l'Internet impliquent seulement d'adapter certaines dispositions, notamment celles portant sur le droit de distribution, afin d'y inclure la transmission numérique, et sur les exceptions au droit d'auteur (notamment en faveur des bibliothèques et des malvoyants). Ce rapport soulignait également la nécessité de mettre en œuvre les stipulations des deux traités conclus sous l'égide de l'OMPI de décembre 1996 en ce qui concerne les dispositifs techniques d'identification et de protection des œuvres (voir *infra*). L'Agence des affaires culturelles, relevant du gouvernement japonais, est parvenue à des conclusions analogues dans son *Livre blanc* publié en février 1997. Elle a estimé qu'il convenait de préciser davantage la notion de droit de transmission (par câble et sans câble), en tenant compte des notions d'interactivité et de mise à disposition du public, spécifiques à l'Internet. Elle a également rappelé qu'il convenait de transposer les stipulations des deux traités OMPI de 1996. Enfin, au Canada, un important travail a également été réalisé, en mars 1995, par le Comité consultatif sur l'autoroute de l'information . Là aussi, le rapport conclut qu'il n'est pas nécessaire de modifier radicalement le régime du droit d'auteur, même sur la question des exceptions au droit d'auteur. Seule la lutte contre la contrefaçon doit être renforcée.

En France, on peut citer le rapport du professeur Pierre Sirinelli au ministre de la Culture, en

1994 , mais qui portait plus largement sur les changements liés au multimédia et à l'environnement numérique.

Au total, les quelques travaux officiels des gouvernements des pays occidentaux retiennent généralement l'idée que le développement de l'Internet ne justifie que quelques adaptations relativement mineures de leurs législations nationales.

La réflexion au sein de la Communauté européenne

Les États membres de l'Union européenne ont eu l'occasion d'exprimer leurs positions lors des négociations des deux traités OMPI de 1996 et surtout dans le cadre de l'élaboration de la directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Ils ont notamment répondu à la consultation lancée par la Commission européenne suite à la publication, en juillet 1995, du *Livre vert sur le droit d'auteur et les droits voisins dans la société de l'information*. La synthèse de ces réponses a fait l'objet d'une communication de la Commission en novembre 1996 . Ce document a servi de point de départ pour l'établissement de la proposition de directive précitée sur l'harmonisation du certains aspects du droit d'auteur et des droits voisins, présentée par la Commission le 10 décembre 1997. Les travaux de la Commission ont toutefois une portée très générale, qui englobe la plupart des questions liées au droit d'auteur et aux droits dits " voisins ", c'est-à-dire les droits reconnus sur certaines œuvres aux artistes interprètes et aux producteurs, notamment en matière de phonogrammes (disques) et de vidéogrammes (cassettes vidéo). Cependant, la question des réseaux numériques fait l'objet d'une attention particulière de la Commission.

Outre la mise en œuvre des deux traités OMPI sur les mécanismes d'identification et de protection des œuvres (voir *infra*), la Commission souhaite harmoniser l'étendue des droits d'auteur et des droits voisins, notamment le régime des exceptions. À ce premier stade de l'élaboration de la directive, le texte proposé par la Commission distingue trois droits exclusifs pour l'auteur sur son œuvre : le droit de reproduction, le droit de communication au public " y compris le droit de mettre à la disposition de celui-ci des œuvres ou autres objets protégés " et le droit de distribution. Des droits " voisins " sont également reconnus aux artistes interprètes et aux producteurs. Par ailleurs, la proposition de directive énumère, de manière limitative, les exceptions au droit d'auteur et droits voisins que peuvent reconnaître les législations des États membres (voir *infra*). On verra plus loin les implications de ces propositions pour le droit français, du moins pour ce qui concerne l'Internet et les réseaux numériques. Le projet de directive reste en revanche elliptique sur l'étendue exacte de chacune des exceptions listées et délibérément muet, à ce stade, sur la question du droit moral de l'auteur sur son œuvre (droit de paternité, droit de s'opposer à l'altération ou à la déformation de son œuvre,...). La Commission n'a pas davantage pris position concernant l'harmonisation éventuelle des modalités de la gestion collective des droits (par des sociétés de perception et de redistribution des droits d'auteur telles que la SACEM, la SACD,...) . Enfin, l'harmonisation des modes de règlement des conflits de lois et de juridictions est renvoyée à la directive générale sur le commerce électronique, qui est en cours d'élaboration par les services de la Commission.

Il faut par ailleurs rappeler qu'il existe un acquis communautaire non négligeable en matière de droit d'auteur. En particulier, deux directives revêtent, comme on le verra, une importance particulière pour l'Internet et les réseaux numériques : la directive 91/250/CE du Conseil sur la protection juridique des programmes d'ordinateurs du 14 mai 1991 et la directive 96/9/CE du 11 mars 1996 sur la protection juridique des bases de données.

Conserver les principes fixés par la législation française
en matière de propriété littéraire et artistique

Le caractère très général des principes du droit de la propriété littéraire et artistique en France permet, sans grande difficulté, leur application par la jurisprudence. Le régime du dépôt légal, rénové en 1992, ne paraît pas davantage poser de difficultés, sous réserve d'un léger aménagement de ses modalités pratiques. En revanche, en écho au constat fait précédemment au plan international, on verra ensuite que la titularité des droits (notamment sur les œuvres " multimédia ") et le régime des exceptions au droit d'auteur (en particulier la " copie privée ") devront faire l'objet d'adaptations législatives. Le règlement des conflits de lois et de juridictions devra, quant à lui, faire l'objet de conventions internationales.

Le problème de la radiodiffusion de type multichaînes (par exemple les radios spécialisées diffusant des programmes de chansons, avec une qualité de son numérique, facilement copiables par les auditeurs) ne sera pas examiné ici, dans la mesure où il s'agit plutôt d'une question de radiodiffusion, sortant du champ de cette étude sur l'Internet et les réseaux assimilés. En outre, comme l'a indiqué la Commission européenne dans sa communication précitée sur le " suivi du livre vert sur le droit d'auteur et les droits voisins dans la société de l'information ", il est encore trop tôt, en l'état des techniques et du marché, pour se prononcer sur l'impact réel de ce type de radiodiffusion numérique.

Les principes essentiels du droit de propriété littéraire et artistique s'appliquent sans difficulté à l'Internet

Le code de la propriété intellectuelle pose comme principe que l'auteur (ou ses ayants-droit) dispose d'un droit exclusif d'exploitation sur son œuvre. Ce droit se décompose essentiellement en deux prérogatives : le droit de reproduction et le droit de représentation. Cette division simple, à caractère très général, diffère de la solution retenue dans beaucoup d'autres pays (par exemple les États-Unis ou le Japon) dont la législation distingue une grande variété de " sous-droits " : droit de distribution, droit de présentation en public, droit de création des œuvres dérivées, droit de transmission, etc. L'avantage de la solution française est sa faculté d'adaptation grâce à la jurisprudence. Ainsi, les tribunaux n'ont d'ores et déjà eu aucune hésitation à estimer que la numérisation d'une œuvre sur un ordinateur (en la recopiant par exemple à l'aide d'un scanner) constitue une reproduction et que sa mise à la disposition du public à partir d'un site accessible librement sur l'Internet constitue une forme de représentation .

Ces jurisprudences récentes n'ont pas encore été consacrées par la Cour de cassation, mais la doctrine est unanime pour les approuver et il ne fait guère de doute qu'elles seront confirmées. Cette évolution jurisprudentielle paraît en effet tout à fait conforme à l'esprit de la législation, en particulier pour ce qui concerne la reproduction numérique. En ce qui concerne le droit de représentation, la solution retenue par la jurisprudence est plus audacieuse, mais elle est parfaitement logique, bien que le responsable du site n'ait pas toujours une attitude active d'émission et de diffusion vers les utilisateurs et se borne souvent à laisser l'œuvre accessible au public sur son site. Il s'agit bien d'une forme de communication de l'œuvre au public. Peut-être pourrait-on d'ailleurs conforter cette jurisprudence en remplaçant, dans la loi, l'expression " droit de représentation " par la terminologie retenue à la fois dans les conventions internationales et dans la proposition de directive communautaire sur le droit d'auteur, à savoir la notion de " droit de communication au public ". Cette modification textuelle n'est nullement indispensable en droit compte tenu des évolutions jurisprudentielles en cours et de la rédaction de l'article L.122-2 du code de la propriété intellectuelle (CPI) qui définit la notion de " représentation " de manière très large . Mais il demeure que la notion de " communication au public " est plus explicite et paraîtrait plus appropriée au regard des nouvelles technologies de l'information.

En tout état de cause, il ne paraît nullement nécessaire de créer un droit spécifique de " transmission numérique ", de " distribution numérique " ou de " mise à disposition du public sur le réseau ", comme cela paraît envisagé dans certains pays comme les États-Unis ou

le Japon. Bien au contraire, une telle initiative nuirait à l'unité conceptuelle du droit d'auteur et obligerait le législateur à d'incessantes adaptations afin de suivre les évolutions technologiques.

Un autre grand principe du droit d'auteur est celui de la rémunération proportionnelle de l'auteur (ou de ses ayants-droit) au profit généré par l'exploitation de l'œuvre. Certains chefs d'entreprise ont indiqué, lors de leur audition, que ce principe était difficilement applicable sur l'Internet, dans la mesure où un grand nombre de sites sont accessibles gratuitement et qu'en tout état de cause, le régime actuel de facturation des utilisateurs ne permet pas d'individualiser les recettes liées à chaque œuvre. Toutefois, il faut rappeler que l'article L.131-4 du code de la propriété intellectuelle, qui fixe le principe de la rémunération proportionnelle, prévoit un très grand nombre d'exceptions, c'est-à-dire de cas dans lesquels la rémunération peut être forfaitaire. C'est notamment le cas quand " la base de calcul de la participation proportionnelle ne peut être pratiquement déterminée ", ou lorsque " les frais des opérations de calcul et de contrôle seraient hors de proportion avec les résultats à atteindre ", ou également dans les cas où " soit la contribution de l'auteur ne constitue pas l'un des éléments essentiels de la création intellectuelle de l'œuvre, soit l'utilisation de l'œuvre ne présente qu'un caractère accessoire par rapport à l'objet exploité ". Le caractère large de ces exceptions paraît tout à fait couvrir les hypothèses évoquées par les responsables de sites auditionnés, notamment les cas où l'accès au site est gratuit et dépourvu de recettes même indirectes (notamment provenant des annonces publicitaires placées sur le site). En outre, la mise en œuvre progressive des mécanismes de " compteurs électroniques " destinés à enregistrer le nombre de consultations d'une œuvre afin de les facturer à l'utilisateur permettront à terme d'appliquer le principe de la rémunération proportionnelle (voir le paragraphe sur les mécanismes techniques d'identification des œuvres, *infra*).

Ainsi, les principes essentiels du droit de propriété littéraire et artistique ne paraissent pas devoir être remis en cause. Il conviendra toutefois que les titulaires de droits s'organisent pour faciliter l'exploitation de leurs œuvres sur les réseaux numériques, notamment en ce qui concerne la délivrance des autorisations et les modalités de rémunération. En outre, un important effort d'information et de sensibilisation du public paraît indispensable si l'on veut éviter une contrefaçon massive, par simple ignorance des règles du droit d'auteur. C'est là l'un des enjeux principaux de la lutte contre la contrefaçon (voir *infra*).

Les modalités pratiques du dépôt légal pourraient être légèrement adaptées afin d'assurer le respect effectif de cette obligation sur les réseaux numériques

Le champ d'application de la loi du 20 juin 1992 relative au dépôt légal est très vaste, puisque l'article 1er de cette loi prévoit que " les documents imprimés, graphiques, photographiques, sonores, audiovisuels, multimédia, quel que soit leur procédé technique de production, d'édition, ou de diffusion, font l'objet d'un dépôt obligatoire, dénommé dépôt légal, dès lors qu'ils sont mis à la disposition d'un public. " Or il ne fait pas de doute qu'une œuvre placée sur un site Internet doit être regardée comme étant mise à la disposition d'un public au sens de cette loi. Elle est donc soumise à l'obligation de dépôt légal.

Cependant, l'Internet stimule fortement la créativité littéraire et artistique, comme en témoigne la croissance très rapide du nombre des sites et des " pages personnelles ". Il en résulte une multiplication des œuvres mises à la disposition du public et donc en principe assujetties au dépôt légal. Si l'on souhaite que cette obligation reste respectée, il faut en faciliter les modalités d'exécution. **Il serait en particulier indispensable que le dépôt des œuvres puisse désormais se faire en ligne**, en s'inspirant de la procédure qu'a mise en place le " Copyright Office " aux États-Unis (projet " Cords ") . À terme, si le nombre d'œuvres déposées devenait trop difficile à gérer par la Bibliothèque nationale de France et les autres établissements habilités, peut-être

faudrait-il envisager un dispositif de sélection tel que celui que la loi et son décret d'application ont prévu pour les progiciels et autres " produits de l'intelligence artificielle " (voir *infra*).

Par ailleurs, il faudra sans doute adapter le deuxième alinéa de l'article 1er de la loi du 20 juin 1992, qui prévoit que " les progiciels, les bases de données, les systèmes experts et les autres produits de l'intelligence artificielle sont soumis à l'obligation de dépôt légal dès lors qu'ils sont mis à la disposition du public par la diffusion d'un support matériel, quelle que soit la nature de ce support. " Il résulte de cette rédaction que lorsque les œuvres ainsi énumérées ne sont diffusées qu'en ligne, sans support matériel, elles ne sont pas assujetties au dépôt légal. Peut-être serait-il utile de modifier la loi sur ce point afin d'inclure la mise à disposition du public par un réseau numérique " ouvert " (i.e. qui ne soit pas un " intranet "). Toutefois, il faut rappeler que ce type d'œuvres est en tout état de cause soumis à un régime spécifique qui n'assure pas l'exhaustivité du dépôt légal : une commission est chargée de définir des critères de sélection des " produits de l'intelligence artificielle " qui seront conservés au titre du dépôt légal. Or ces critères n'ont toujours pas été définis à ce jour par cette commission. Par suite, seuls les progiciels et les autres produits de l'intelligence artificielle déposés à titre volontaire par les éditeurs sont conservés. Il convient donc, avant toute autre réforme, de mettre en œuvre la loi quitte à l'étendre ensuite aux œuvres dépourvues de support matériel.

Faire évoluer le régime de la titularité des droits, notamment à l'égard des auteurs salariés

L'actualité récente a mis en lumière l'acuité des problèmes liés à la titularité des droits sur les œuvres mises en ligne sur l'Internet, en particulier en ce qui concerne les œuvres réalisées par des auteurs salariés. Cette question a été posée avec vigueur par les entreprises éditrices de bases de données qui ont tenté, en vain, d'obtenir du gouvernement et du Parlement que la loi pose le principe d'une cession automatique à l'employeur des droits d'exploitation des auteurs salariés sur les bases de données à l'élaboration desquelles ceux-ci ont contribué. Les éditeurs d'œuvres " multimédia " émettent le même souhait. Dans le même sens, les entrepreneurs de presse se voient freinés par la jurisprudence dans leurs projets de mise en ligne sur les réseaux de leurs journaux et des articles rédigés par leurs journalistes salariés. Des tribunaux ont en effet jugé que les entreprises de presse ne pouvaient pas procéder à une exploitation radicalement nouvelle des articles, notamment en les diffusant sur l'Internet, sans l'autorisation des journalistes auteurs de ces articles .

À l'appui de leurs revendications, les chefs d'entreprise français, notamment dans le domaine du " multimédia ", se réfèrent fréquemment au droit américain, qui pose comme principe que l'employeur est réputé être l'auteur de toutes les œuvres créées par ses salariés. De même, lorsqu'une entreprise commande une œuvre (" work made for hire "), elle est réputée être titulaire du " copyright " (droit d'auteur) sur cette œuvre.

L'actualité liée à l'exploitation d'œuvres sur l'Internet ne fait que refléter le problème plus général de la titularité des droits de l'employeur à l'égard des œuvres créées par ses salariés. Cette question dépasse donc largement le champ de la présente étude. C'est pourquoi **on se bornera ici à esquisser quelques pistes de réflexion, qui doivent faire l'objet d'une concertation approfondie entre les pouvoirs publics, le patronat et les syndicats.** Il serait d'ailleurs souhaitable à cette occasion de clarifier, dans la législation, la question du droit d'auteur des agents publics sur les œuvres qu'ils ont créées dans le cadre de leur travail. Une réflexion plus large sur la définition même de l'auteur devra également être envisagée.

Il est, en tout état de cause, une solution qui paraît devoir être écartée d'emblée, c'est l'idée de créer un régime spécifique pour les œuvres dites " multimédia ", en s'inspirant de ce qui a été fait pour les œuvres audiovisuelles, les logiciels et les bases de données. En effet, cet " émiettement " progressif du droit d'auteur altère profondément la lisibilité du code de la

propriété intellectuelle et la clarté de ses principes, du fait de l'empilement de régimes dérogatoires. Surtout, ces dispositions propres à des types d'œuvres très particuliers, correspondant à l'état de l'art et de la technologie à un moment donné, sont difficiles à adapter par la jurisprudence à l'évolution extrêmement rapide des technologies de l'information. Les tribunaux paraissent d'ailleurs éprouver d'importantes difficultés pour déterminer le régime juridique applicable aux produits " multimédia ", par exemple les jeux vidéo interactifs, qui comprennent à la fois une partie de logiciel et une partie audiovisuelle . Or la différence est importante pour connaître le titulaire des droits car si le tribunal retient la qualification de logiciel, c'est l'employeur qui sera réputé être titulaire du droit d'auteur (art. L.113-9, CPI), alors que si le juge retient la qualification d'œuvre audiovisuelle, les droits appartiendront conjointement aux auteurs du scénario, de l'adaptation, du texte et des compositions musicales, ainsi qu'au réalisateur, alors même qu'ils seront salariés (art. L.113-7, CPI). Par ailleurs, outre les inconvénients de ces régimes disparates, voire contradictoires, il ne paraît pas possible de définir des critères clairs de l'œuvre " multimédia " dont la caractéristique est précisément d'être complexe et multiforme. C'est pourquoi il paraît important de réduire le nombre de ces régimes d'exception en droit d'auteur et d'essayer de trouver une règle générale de titularité des droits plutôt que de créer une nouvelle dérogation aux contours mal définis en faveur des œuvres dites " multimédia ". Cet effort doit être fait tant au plan national qu'au plan communautaire où l'on ne peut que regretter la multiplication des directives sectorielles (logiciel, bases de données,...).

La première voie qui pourrait être explorée, pour tenter de clarifier la titularité des droits sur les œuvres littéraires et artistiques, est celle de **l'aménagement de la notion d'œuvre collective**. " Est dite collective l'œuvre créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé " (art. L.113-2, CPI). L'exemple classique est celui du dictionnaire ou de l'encyclopédie. On considère également souvent les journaux comme des œuvres collectives. Cependant, de manière générale, la jurisprudence tend à interpréter assez strictement la notion d'œuvre collective, dans la mesure où elle a pour effet de priver les salariés de leur droit d'auteur. Par exemple, comme on l'a vu, la jurisprudence est réticente à considérer que la réutilisation des articles de journal par une entreprise de presse sur son site Internet demeure dans le champ de l'œuvre collective . Les journalistes recouvrent donc leurs droits d'auteur sur leurs articles pris à titre individuel, ce qui peut constituer un obstacle à la diversification des entreprises de presse. Peut-être pourrait-on donc examiner la possibilité de conférer à l'employeur le droit de réutiliser librement les contributions individuelles des divers auteurs ayant participé à l'élaboration de l'œuvre collective, sous réserve d'une rémunération équitable pour ces derniers, dont les modalités pourraient éventuellement être fixées par la loi.

La seconde piste de réflexion possible concerne les œuvres qui n'ont pas un caractère collectif au sens du code de la propriété intellectuelle, et qui peuvent donc être clairement attribuées à un ou plusieurs auteurs individuels. En principe, lorsque ceux-ci sont salariés et alors même que l'œuvre a été créée dans le cadre de leur travail, les droits d'exploitation leur appartiennent sauf si l'employeur a conclu avec eux un contrat de cession des droits. Toutefois, à l'heure actuelle, le code de la propriété intellectuelle interdit la cession globale des œuvres futures (art. L.131-1, CPI). Il n'est donc pas évident qu'un employeur puisse licitement demander à ses salariés de lui céder, par avance, les droits sur toutes les œuvres créées dans le cadre du contrat de travail . En outre et en tout état de cause, l'employeur doit, même dans le cas où il a obtenu la cession des droits, accorder une rémunération spécifique du salarié au titre de son droit d'auteur. Et cette rémunération doit en principe être proportionnelle aux recettes de l'exploitation de l'œuvre, sauf si l'on se trouve dans l'un des cas prévus à l'article L.131-4 du code de la propriété intellectuelle permettant une rémunération forfaitaire (voir *supra*). En tout état de cause, la rémunération au

forfait est interdite si l'employeur a obtenu le droit d'exploiter l'œuvre sous une forme non prévue ou non prévisible à la date du contrat (art. L.131-6, CPI).

L'ensemble de ces dispositions sont, comme on peut le constater, très protectrices de l'auteur salarié. Cependant, il est ressorti des auditions du groupe d'étude qu'elles sont extrêmement contraignantes pour les employeurs et l'on peut douter, de ce fait, qu'elles soient vraiment respectées en pratique. On se trouve donc fréquemment, notamment dans le domaine des œuvres " multimédia " destinées à être mises en ligne, dans une situation peu satisfaisante dans laquelle, bien souvent, les salariés ne perçoivent pas, en réalité, de rémunération proportionnelle aux recettes d'exploitation des œuvres qu'ils ont créées. En outre, les employeurs ne sont jamais certains d'être véritablement titulaires des droits sur les œuvres qu'ils exploitent. Cette insécurité juridique explique l'insistance des entreprises auprès des pouvoirs publics pour que la loi leur reconnaisse la titularité des droits sur les bases de données créées par leurs salariés, en s'inspirant du régime juridique du logiciel.

Il serait souhaitable, en tout état de cause, qu'une solution aussi uniforme que possible puisse être adoptée en matière de titularité des droits des employeurs, surtout compte tenu du caractère composite des œuvres " multimédia ". Diverses solutions peuvent être envisagées. La solution la plus avantageuse pour les employeurs serait naturellement que la loi introduise une présomption de cession à l'employeur des droits d'auteur des salariés sur les œuvres créées par ceux-ci dans le cadre du contrat de travail, comme cela a été fait en matière de logiciel (art. L.113-9, CPI). Un tempérament à ce principe pourrait être apporté en s'inspirant du régime dégagé par la jurisprudence allemande, qui considère que le contrat de travail emporte cession des droits à l'employeur pour l'utilisation des œuvres par l'entreprise ; le salarié conserve néanmoins le droit d'exploiter les œuvres qu'il a créées sous réserve de ne pas porter préjudice à l'entreprise. Il paraît cependant important, si la solution de la présomption de cession des droits était retenue, que la loi veille à la fois au respect du droit moral des auteurs salariés (tout en prévenant les abus de droit motivés par des préoccupations purement financières) et au maintien d'une forme de rémunération équitable au profit de l'auteur salarié (qui n'est d'ailleurs pas prévue en matière de logiciel).

Il n'entre pas dans le champ de cette étude de prendre parti sur l'opportunité d'une forme de cession automatique des droits à l'employeur. La solution adoptée devra résulter d'une concertation entre les acteurs concernés sous l'égide des pouvoirs publics. Mais il paraît indispensable, au minimum, de clarifier les conditions de cession volontaire, par la voie contractuelle, des droits d'exploitation des salariés à leur employeur. **Il faut assouplir les rigidités actuelles du code de la propriété intellectuelle, qui ont été rappelées plus haut, tout en garantissant de manière plus effective la rémunération équitable des salariés au titre de leur droit d'auteur. Ce régime de rémunération pourrait s'inspirer de celui qui est prévu, en matière de brevets, pour les inventions des salariés** (art. L.611-7, CPI). Il faudra, au bout du compte, parvenir, comme en matière de brevets, à une solution équilibrée qui assure à la fois un niveau suffisant de protection des droits des salariés et une plus grande sécurité juridique pour les employeurs. Compte tenu des enjeux financiers très importants du problème de la titularité des droits, notamment dans le domaine du " multimédia ", et eu égard à la dimension très symbolique du droit d'auteur, il serait souhaitable que le Gouvernement prenne l'initiative d'engager au plus tôt la concertation nécessaire entre les acteurs concernés afin d'explorer les différentes pistes de réflexion qui ont été esquissées ci-dessus.

Au-delà des aménagements de la législation existante, il paraît également indispensable que le Gouvernement prenne l'initiative d'une réflexion sur la définition même de l'auteur, notamment dans le cadre salarié. Le caractère complexe des œuvres " multimédia ", qui implique la participation de nombreux salariés (informaticiens, infographistes,...), rend en effet

souvent difficile la distinction entre auteurs et simples auxiliaires techniques. C'est pourquoi il semble nécessaire, dans ce nouvel environnement technologique, d'aider le juge à apprécier, parmi les différents salariés qui ont participé à l'élaboration d'une œuvre collective, ceux qui ont pris une part déterminante dans la conception de l'œuvre et qui, seuls, doivent se voir reconnaître la qualité d'auteur.

Enfin, il faudra résoudre les problèmes liés aux disparités de traitement entre les rémunérations salariées et les rémunérations au titre du droit d'auteur. Ces dernières sont en effet assujetties à des taux de cotisations sociales moins élevés que les salaires et primes assimilées et bénéficient en outre de déductions supplémentaires au titre de l'impôt sur le revenu . On constate d'ailleurs d'ores et déjà des dérives dans certains contrats de commande d'œuvres (notamment musicales ou photographiques), qui conduisent les commanditaires à minorer la part d'honoraires pour accroître artificiellement la part de droit d'auteur bénéficiant d'un régime fiscal et social beaucoup plus favorable. Si ce phénomène devait s'étendre à la rémunération des salariés au titre du droit d'auteur, on pourrait craindre une évasion fiscale considérable. Il faut donc préciser davantage la distinction entre les deux types de rémunération, en essayant de trouver des critères clairs et incontestables pour distinguer ce qui relève de la rémunération du travail et ce qui relève du droit d'auteur. On pourrait également envisager des taux intermédiaires de prélèvements fiscaux et sociaux pour les rémunérations de droit d'auteur qui sont accessoires au salaire (ou aux honoraires pour le contrat de commande), en prévoyant des plafonnements pour prévenir les abus.

Adapter, dans un cadre international,
le régime des exceptions au droit d'auteur

Comme toutes les législations nationales, le droit français prévoit quelques limitations au monopole d'exploitation de l'auteur sur son œuvre, afin de trouver un équilibre entre l'intérêt de celui-ci et l'intérêt général qui s'attache à ce que le public puisse avoir, dans certains cas, accès gratuitement à l'œuvre. C'est ce que l'on appelle les " exceptions au droit d'auteur ". Elles sont énumérées à l'article L.122-5 du code de la propriété intellectuelle. On examinera chacune d'entre elles pour apprécier s'il convient de l'adapter au contexte des réseaux numériques. Il faudra ensuite envisager les éventuelles exceptions nouvelles qui pourraient résulter d'une harmonisation communautaire voire internationale.

Représentation dans le " cercle de famille "

L'article L.122-5 du code de la propriété intellectuelle prévoit que l'auteur ne peut pas interdire " les représentations privées et gratuites effectuées exclusivement dans un cercle de famille ". Cette exception ne semble pas poser de problème particulier sur Internet, même s'il a pu être argué, dans une affaire récente, sur le fondement de cette disposition, que la diffusion d'une œuvre sur un " intranet " (réseau interne d'une organisation telle qu'une entreprise) constituait une représentation privée dans un " cercle de famille ". Il s'agissait toutefois, dans le cas d'espèce, d'un " intranet " professionnel, ce qui aurait dû conduire le juge à écarter le bénéfice de l'exception. Cependant, le juge des référés a admis que le fichier contrefaisant avait un " caractère privé " dès lors qu'il n'était en principe pas accessible au public . Ce raisonnement a été très critiqué par la doctrine, à juste titre, et il paraît peu probable que ce précédent fasse jurisprudence. Le régime de cette exception ne paraît donc pas soulever de difficulté particulière.

Copie privée

? *L'état actuel du droit*

La loi française, comme la plupart des autres législations nationales, interdit à l'auteur de

s’opposer aux " copies ou reproductions strictement réservées à l’usage privé du copiste et non destinées à une utilisation collective " (art. L.122-5, CPI). Cependant, pour les bases de données et pour les logiciels, la copie privée est interdite .

Pour compenser le manque à gagner des auteurs dont les œuvres font l’objet de copies privées, le législateur a introduit différentes formes de " rémunération pour copie privée ". Il a ainsi institué une " redevance " forfaitaire sur différents supports d’enregistrement vierges, notamment les cassettes audio et vidéo (art. L.311-1 et suivants, CPI). Cette redevance est payée par les fabricants ou importateurs de ces supports, et redistribuée aux auteurs, artistes interprètes et producteurs de phonogrammes (disques) et vidéogrammes (cassettes vidéos) par des organismes de gestion collective. Il existe également, depuis 1995, un dispositif un peu analogue pour la reprographie (art. L.122-10, CPI), mais il ne concerne pas véritablement la copie privée au sens strict .

? *Les problèmes posés par l’environnement des réseaux numériques*

Dans l’environnement des réseaux numériques, le régime actuel de l’exception de copie privée soulève deux difficultés. La première, qui concerne également les copies faites sur un support matériel (CD enregistrable, " minidiscs ",...), est que la copie numérique a le même niveau de qualité que l’original, dont elle est une sorte de " clone ". Il n’y a pas de différence entre l’original et la copie, alors que les copies " analogiques " (copie sur une cassette classique par exemple) provoquent une perte sensible de qualité, ce qui en freine la prolifération. Cette sorte d’autolimitation n’existe plus pour les copies numériques et fait donc craindre aux titulaires de droits une multiplication abusive des copies privées sur les réseaux tels que l’Internet.

La seconde difficulté, propre aux réseaux numériques, tient à l’élimination de tout support matériel. Ce phénomène nouveau facilite considérablement la copie privée, comme on peut d’ailleurs le constater d’ores et déjà sur l’Internet, où se développe, sous couvert de copies prétendument " privées ", une importante contrefaçon (voir *infra*). Il faut d’ailleurs rappeler qu’une copie transmise par courrier électronique à un tiers ne constitue pas une copie privée puisqu’elle est destinée à l’usage de quelqu’un qui n’est pas le copiste. En outre, il paraît difficile de définir une assiette pour étendre la perception de la rémunération pour copie privée qui existe pour les titulaires des droits sur les phonogrammes et vidéogrammes. La difficulté de la perception et de la redistribution de cette rémunération pour copie privée, qui n’existe que dans une minorité de pays dans le monde, est accrue par le caractère international de réseaux tels que l’Internet.

Compte tenu des spécificités des réseaux numériques, une solution séduisante consisterait à supprimer l’exception de copie privée. En d’autres termes, toute copie d’une œuvre faite depuis un site numérique et toute reproduction ensuite de cette copie initiale devrait être expressément autorisée par le titulaire des droits sur l’œuvre, même si ces copies sont destinées à l’usage privé du copiste. Le contrôle de cette interdiction de reproduction pourrait, à terme, être assuré par des mécanismes techniques de protection de l’œuvre (voir *infra*). Cette solution est naturellement défendue par les titulaires de droits, notamment par une grande partie des sociétés d’auteurs, qui redoutent que l’exception de copie privée leur cause un préjudice considérable compte tenu des particularités des réseaux qui viennent d’être rappelées.

Cependant, cette solution radicale se heurte à l’opposition de principe de tous ceux qui estiment que le droit de faire des copies pour son usage privé est un droit inaliénable du citoyen. Ce droit bénéficierait même, semble-t-il, d’une protection constitutionnelle aux États-Unis et dans certains pays du Nord de l’Europe. En outre, le rétablissement intégral du droit exclusif de l’auteur sur l’œuvre, qui était traditionnellement tempéré par l’exception de copie privée, limiterait l’accès des plus défavorisés à la culture et à l’information. La logique économique se

trouverait donc en opposition avec le droit à la culture. Il est important néanmoins de relativiser un peu cette argumentation, en rappelant notamment qu'un nombre important d'auteurs acceptent spontanément que leur œuvre soit copiée librement (à condition que ce soit dans un but non commercial), en particulier sur l'Internet. De nombreux logiciels sont ainsi mis gracieusement à la disposition des utilisateurs (" freeware "), par exemple le logiciel de navigation " Netscape ". En outre, il existe différents moyens d'accéder gratuitement ou presque à l'information, notamment par l'intermédiaire des bibliothèques. Mais ces arguments ne suffisent pas à désarmer les partisans de l'exception de copie privée, qui craignent malgré tout une restriction de l'accès aux œuvres, surtout compte tenu du développement des dispositifs techniques de protection et d'identification des œuvres.

La forte sensibilité de ce sujet, et son importance tant économique que symbolique, ont conduit la Commission européenne à ne pas le traiter dans la proposition de directive sur l'harmonisation du droit d'auteur qu'elle a présentée en décembre 1997. Mais elle n'a pas renoncé à lancer des négociations sur ce point au niveau communautaire.

? *Les solutions envisageables*

Une solution purement française au problème de la copie privée sur les réseaux numériques présenterait peu d'intérêt pratique compte tenu du caractère international de l'Internet. On peut toutefois avancer une solution de compromis, qui pourrait peut-être recevoir l'aval des autres États membres de la Communauté européenne, voire d'autres pays encore. **Elle consisterait à poser comme principe légal que la copie privée, c'est-à-dire strictement réservée à l'usage privé du copiste et non destinée à un usage collectif, est autorisée, sauf interdiction expresse du titulaire des droits sur l'œuvre, notifiée au copiste lors de la copie initiale sur le site par un message explicite.** Le respect de cette interdiction peut bien sûr ensuite être assuré par un dispositif technique empêchant la copie. La copie privée n'est licite qu'à la condition que l'œuvre ait été mise à la disposition du public sur un site dans des conditions régulières, c'est-à-dire que le responsable du site soit titulaire des droits d'exploitation sur le réseau. En outre, il est bien évident que le choix du titulaire des droits de permettre, à titre gratuit ou onéreux, la consultation d'une œuvre sur son site et, le cas échéant, la reproduction de celle-ci sur le disque dur de l'utilisateur par téléchargement relève de son droit exclusif. Le régime de la copie privée s'applique principalement aux copies " subséquentes ", c'est-à-dire celles qui sont faites par l'utilisateur à partir de l'exemplaire qu'il a téléchargé sur son ordinateur. Ces copies peuvent être faites notamment sur des disquettes, des CD enregistrables ou par des sorties d'imprimantes. On peut toutefois s'interroger davantage sur le statut juridique de la " capture d'écran " que permettent d'opérer certains logiciels de navigation sur l'Internet, c'est-à-dire la copie sur le disque dur (ou sur l'imprimante) du document qui apparaît à l'écran, sans que le responsable du site en soit informé. Il semble logique qu'une telle copie puisse bénéficier du régime qui vient d'être proposé pour l'exception de copie privée.

Les titulaires de droits pourraient être incités à ne pas interdire la copie privée par une extension des dispositifs légaux de rémunération pour copie privée décrits plus haut. On pourrait en effet imaginer qu'ils reçoivent dans ce cas, par l'intermédiaire d'organismes de gestion collective, une rémunération pour copie privée. Celle-ci pourrait être perçue sur les nouveaux supports d'enregistrement (CD enregistrables, " minidiscs ", et même éventuellement les disquettes et disques durs). L'avantage d'une assiette la plus large possible serait qu'elle permettrait un taux de perception très faible et découragerait donc la fraude. Naturellement, seuls les titulaires de droits s'engageant à ne pas interdire ni restreindre (notamment en exigeant un paiement) la copie privée pourraient bénéficier de la rémunération forfaitaire à ce titre .

La solution proposée présente l'avantage de maintenir la présomption du caractère licite de la copie privée, sous réserve qu'elle soit destinée exclusivement à l'usage privé du copiste. Mais

elle permet en même temps aux titulaires de droits de l'empêcher lorsque les reproductions privées risqueraient d'occasionner un préjudice considérable, ce qui concerne essentiellement les œuvres faisant l'objet d'une exploitation commerciale, ce qui est loin d'être le cas de toutes celles qui sont protégées par le droit d'auteur. Il appartient aux titulaires de droits de faire un arbitrage entre la rémunération que leur assurent les éventuels moyens de protection technique dont ils disposent et celle qu'ils peuvent percevoir au titre de la rémunération forfaitaire pour copie privée. Certaines sociétés d'auteur, notamment le Groupement européen des sociétés d'auteurs et de compositeurs (GESAC), qui regroupe les principales sociétés d'auteurs européennes, se sont d'ailleurs déclarées favorables, à titre transitoire, au maintien de l'exception de copie privée sous réserve d'un mécanisme de rémunération forfaitaire pour copie privée . Le GESAC précise qu'il n'envisage un tel système qu'à titre temporaire, en attendant que les dispositifs techniques de protection et d'identification des œuvres soient opérationnels et permettent l'application du droit exclusif. Cependant, la solution proposée ci-dessus pourrait, de manière pérenne, permettre une rémunération pour copie privée tout en laissant la faculté aux auteurs qui le souhaitent d'interdire individuellement la copie privée, ce qui les exclurait naturellement du mécanisme global de rémunération pour copie privée.

Par ailleurs, cette solution serait conforme à l'esprit des deux traités de l'OMPI précités de décembre 1996 pour ce qui concerne les mécanismes de protection des œuvres. En effet, on voit mal sinon quel pourrait être l'intérêt de tels mécanismes s'ils ne peuvent empêcher la copie privée, qui n'est définie que par son seul usage, lequel est difficilement vérifiable.

Courte citation et autres exceptions prévues par la législation française

L'article L.122-5 du code de la propriété intellectuelle autorise, sans que l'auteur puisse s'y opposer, " les courtes citations justifiées par le caractère critique, polémique, pédagogique, scientifique ou d'information de l'œuvre à laquelle elles sont incorporées. " Cette exception ne paraît pas poser de difficulté dans l'environnement des réseaux numériques. Ce droit de citation ne peut en aucun cas permettre la mise en ligne d'extraits d'œuvre (par exemple de chansons) à des fins commerciales. Il s'agit d'une exception, qui est donc d'interprétation stricte, et qui se définit par la finalité de la citation qui est précisément encadrée par le code de la propriété intellectuelle. En revanche, on peut imaginer que ces extraits ne concernent pas nécessairement des œuvres littéraires mais également d'autres types d'œuvres, par exemple sonores ou audiovisuelles, mais toujours en respectant les conditions énoncées par la loi. Quant aux autres exceptions légales (diffusion de discours destinés au public et parodie), elles ne paraissent pas poser de problème pour leur application sur l'Internet.

Copie technique

Le code de la propriété intellectuelle ne prévoit, dans sa rédaction actuelle, aucune exception pour les reproductions techniques nécessitées par les transmissions numériques (copie sur le serveur du site et du fournisseur d'accès, sur la mémoire vive et sur le disque dur de l'ordinateur de l'utilisateur,...). Il existe pourtant un relatif consensus sur la nécessité d'une telle exception pour permettre la circulation des œuvres sur les réseaux numériques. La difficulté tient à la définition exacte de sa portée.

Les fournisseurs d'accès souhaiteraient naturellement que le champ de cette exception soit relativement large afin d'inclure la reproduction sur les " caches " de leurs serveurs, c'est-à-dire le stockage temporaire des pages Internet les plus consultées par leurs abonnés, afin d'éviter des connexions inutiles aux sites concernés. Les " caches " permettent à la fois un accès plus rapide aux pages stockées pour les abonnés et une économie sur le recours aux liaisons numériques internationales. Il existe, de la même façon, des " caches " dans l'ordinateur de l'utilisateur (principalement dans la mémoire vive mais parfois aussi sur le disque dur) ; ces " caches " sont

gérés par le logiciel de navigation de l'utilisateur.

Cependant, comme le font valoir à juste titre les titulaires de droits, le recours aux " caches " réduit le nombre d'accès directs aux sites et empêche le décompte des consultations des œuvres sur ceux-ci, d'autant plus qu'il arrive fréquemment qu'une page soit stockée pendant plusieurs heures voire plusieurs jours. Par suite, les " caches " risquent d'empêcher la mise en place des mécanismes techniques d'identification des œuvres et des " compteurs électroniques " (voir *infra*). Plus généralement, les " caches " limitent le contrôle des titulaires de droits sur leurs œuvres. Il serait donc excessif de permettre, par une exception trop large, une pratique favorable aux fournisseurs d'accès mais potentiellement très préjudiciable aux titulaires de droits.

Les critères de la " copie technique " retenus dans la proposition de directive communautaire sur l'harmonisation du droit d'auteur paraissent imprécis et peu opérants (" actes de reproduction provisoires... qui font partie intégrante d'un procédé technique ayant pour unique finalité de permettre une utilisation d'une œuvre ou d'un autre objet protégé, qui n'ont pas de signification économique indépendante "). Si l'on veut encadrer précisément le champ de cette exception, il faut distinguer la copie technique " volatile " de celle qui est " temporaire ".

On pourrait considérer que **l'exception au droit d'auteur ne doit s'appliquer qu'à la " copie technique volatile ", c'est-à-dire faisant partie intégrante d'un procédé technique ayant pour unique finalité de permettre l'utilisation en ligne d'une œuvre ou d'un autre objet protégé, *et dont l'existence n'excède pas la durée de la transmission***. Cette exception ne s'appliquerait donc qu'aux reproductions sur les ordinateurs de routage, sur la mémoire vive de l'ordinateur de l'utilisateur, etc, sans possibilité de conservation au-delà de la transmission ou de l'utilisation autorisée par le titulaire des droits. Les autres copies, y compris celles faites sur les " caches " des fournisseurs d'accès, demeureraient donc soumises au droit exclusif de l'auteur. Le fait de n'admettre que cette exception restreinte, dont le principe est accepté par la plupart des titulaires de droits, serait évidemment défavorable aux fournisseurs d'accès. Mais cette solution les inciterait à coopérer avec les titulaires de droits pour la mise en place de systèmes assurant un contrôle et, le cas échéant, une rémunération suffisants sur leurs œuvres. Des accords cadres pourraient également prévoir une rémunération forfaitaire des titulaires de droits au titre des copies réalisées sur les " caches ".

Compte tenu de l'importance technique et économique des " caches " pour le développement de l'Internet, on pourrait également envisager **une seconde exception, en faveur de la " copie technique temporaire ", c'est-à-dire celle faite sur les " caches " des fournisseurs d'accès.** Ce type de copie pourrait être défini comme faisant partie intégrante d'un procédé technique ayant pour unique finalité de permettre l'utilisation en ligne d'une œuvre ou d'un autre objet protégé par les abonnés d'un fournisseur d'accès, *et dont l'existence n'excède pas la durée autorisée par le titulaire des droits par les dispositifs techniques appropriés* (*i.e.* spécifications techniques concernant la durée maximale du " cache ", que le titulaire des droits peut interdire) . Toutefois, en contrepartie de cette exception qui leur est favorable, il serait normal que les fournisseurs d'accès acceptent le principe d'une **" rémunération pour copie technique " forfaitaire au profit des titulaires de droits**. Le mécanisme de celle-ci pourrait s'inspirer de celui retenu pour la " rémunération pour copie privée " (voir *supra*) : une redevance forfaitaire serait perçue sur les abonnements aux fournisseurs d'accès et serait redistribuée aux titulaires de droits selon les mêmes modalités que pour la copie privée.

Bibliothèques et enseignement

Certains plaident en faveur de l'extension à l'Internet de l'exception anglo-saxonne de " fair use " (*i.e.* utilisation de la copie à des fins non commerciales, notamment pour la recherche ou l'éducation). Ce courant de pensée rencontre même un certain écho en France et dans les

enceintes internationales, comme en ce qui concerne l'exception de copie privée (voir *supra*). Une telle exception ne s'inscrit pas du tout dans la tradition française en matière de propriété littéraire et artistique. Les autorités américaines elles-mêmes se montrent d'ailleurs prudentes sur ce sujet. Elles envisagent même de limiter le nombre de copies numériques que les bibliothèques pourraient être autorisées à effectuer dans le cadre du " fair use ", afin d'éviter que la prolifération de copies, qui sont en réalité identiques à l'original, ne cause un trop grand préjudice aux titulaires de droits.

En France, il conviendrait que les pouvoirs publics incitent les titulaires de droits à passer des accords cadres avec les bibliothèques et les établissements d'enseignement, leur consentant des conditions tarifaires privilégiées, sur le modèle de ce qui s'est fait récemment avec le ministère de l'Éducation nationale pour la Banque de programmes et de services (BPS) et de ce qui est en cours de négociation avec la Bibliothèque nationale de France pour la consultation d'œuvres numérisées sur son réseau interne. Ce n'est que si cette voie contractuelle s'avérait insuffisante pour permettre un large accès de tous à la culture que le Gouvernement devrait envisager la création d'une exception au droit d'auteur en faveur des bibliothèques et des établissements d'enseignement, mais en la restreignant aux œuvres mises en ligne sur les réseaux numériques.

Harmonisation communautaire et internationale du régime des exceptions

Le caractère international de l'Internet rend nécessaire une harmonisation progressive des exceptions au droit d'auteur. Toutefois, compte tenu du caractère très sensible et de la portée symbolique du régime des exceptions au droit d'auteur, l'harmonisation des législations nationales sur ce point sera très certainement lente et difficile, même à l'échelle communautaire. Par suite, compte tenu du fait que chaque site est accessible depuis n'importe quel pays, **il est impératif que chaque État impose aux responsables de sites résidant sur son territoire de prévoir un dispositif technique limitant le bénéfice des exceptions au droit d'auteur** (notamment celles liées au " **fair use ") aux utilisateurs résidant dans ce pays.** De tels dispositifs de filtrage d'accès en fonction du lieu de résidence de la personne qui consulte le site existent d'ailleurs d'ores et déjà sur certains sites même si leur efficacité n'est pas encore totale.

Harmoniser les règles relatives aux conflits de lois et de juridictions, notamment en matière d'atteintes aux droits de propriété intellectuelle

L'harmonisation des règles relatives aux conflits de lois et de juridictions, en matière de titularité des droits et de responsabilité contractuelle

En matière de responsabilité contractuelle (contrats de cession de droits ou d'autorisation d'exploitation), le principe est celui de l'autonomie de la volonté des parties. Les règles du droit international privé sont clairement fixées (voir en ce qui concerne les transactions commerciales, partie II, *supra*) et la propriété intellectuelle ne paraît pas connaître de spécificités particulières sur ce point.

En ce qui concerne la titularité des droits sur une marque ou un brevet, la loi applicable ne peut être que celle du pays dans lequel a été déposé la marque ou le brevet en cause.

Pour ce qui est de la détermination du titulaire des droits sur une œuvre, la loi applicable est celle du pays d'origine de l'œuvre, qui est appréciée par le juge essentiellement d'après le lieu de première publication de l'œuvre. Lorsque l'œuvre a fait l'objet d'une publication sur un support matériel (livre, CD-rom, ...) avant sa mise sur le réseau, le tribunal applique les critères

traditionnels en s'inspirant notamment de l'article 5 de la convention de Berne. En revanche, lorsque ce n'est pas le cas, il est plus difficile de déterminer le lieu de la première publication et aucune jurisprudence ne semble encore exister sur ce point. Il paraît dangereux de retenir comme seul critère le lieu de la première " injection " de l'œuvre sur le réseau, c'est-à-dire le site sur lequel l'œuvre a été mise pour la première fois à la disposition du public. Il est nécessaire que le tribunal détermine le véritable pays d'origine de l'œuvre en prenant en compte les circonstances de l'affaire et notamment le lieu de résidence habituelle du ou des auteurs. Il faut en effet éviter que le critère du lieu géographique d'injection de l'œuvre sur le réseau ne permette des fraudes à la loi tendant, par exemple, à privilégier les pays dans lesquels les droits des auteurs salariés sont peu ou pas protégés.

En ce qui concerne la protection du droit moral de l'auteur, la jurisprudence de la cour de cassation a estimé qu'elle relève de l'ordre public international . Elle s'impose donc à tout tribunal français même lorsque la loi française n'est normalement pas applicable en l'espèce. Cette solution doit être maintenue, surtout eu égard aux risques importants de déformation ou de mutilation des œuvres sur les réseaux numériques.

L'harmonisation des règles relatives aux conflits de lois et de juridictions, en matière d'atteinte au droit de propriété littéraire et artistique

? *L'état actuel du droit*

Lorsqu'un site numérique met à la disposition du public un contenu contrefaisant, on pourrait estimer, en première analyse, qu'il est régi par la loi du pays dans lequel il est situé (loi du pays d'émission) et qu'il n'y a pas lieu de prendre en compte la législation d'autres États. Toutefois, comme cela a été rappelé à plusieurs reprises, ce site est accessible depuis l'ensemble des pays du monde. Or, la jurisprudence traditionnelle s'inspire plutôt du principe posé par l'article 5 §2 de la convention de Berne sur la protection des œuvres littéraires et artistiques : elle considère que la loi applicable en cas d'atteinte au droit d'auteur est celle du pays dans lequel la protection est réclamée, c'est-à-dire celui dans lequel est subi le préjudice. Si l'on transpose cette solution aux sites numériques, il s'agirait donc du (ou des) pays de réception, au moins pour la réparation du préjudice subi dans ce (ou ces) pays du fait de la contrefaçon.

La solution concernant la juridiction compétente n'est pas très différente. Il est bien sûr toujours possible de saisir celle de l'État dans lequel réside le défendeur, c'est-à-dire l'auteur de la contrefaçon (*i.e.* le pays d'émission) , mais il est également possible de saisir celle de l'État (ou des États) dans lequel le fait dommageable est constaté (*i.e*. le pays de réception).

Il faut ajouter que, dans la plupart des législations, notamment dans la loi française (art. L.335-2, CPI), la contrefaçon constitue non seulement une faute de nature à engager la responsabilité civile du contrefacteur, mais également un délit pénalement réprimé. Or, en France comme dans beaucoup de pays, il suffit, en matière pénale, que l'un des éléments constitutifs de l'infraction soit situé sur le territoire national pour que les règles pénales soient applicables (art. 113-2, code pénal) et pour que le juge national soit compétent. En d'autres termes, sur le plan pénal, c'est la loi du pays de réception qui est applicable (voir quatrième partie, *infra*).

On peut donc déduire de l'état actuel de la jurisprudence, tant en matière civile qu'en matière pénale, qu'un titulaire de droits victime d'une contrefaçon peut saisir, outre bien sûr le tribunal du pays d'émission, le tribunal de tout État dans lequel il aura subi un préjudice (pays de réception). En principe, chacun de ces tribunaux appliquera sa loi nationale compte tenu des règles jurisprudentielles rappelées plus haut. Le tribunal du lieu d'émission pourra faire cesser la contrefaçon et prononcer des sanctions immédiatement exécutoires à l'encontre du contrefacteur (sans que se pose le problème de l'*exequatur),* ce qui rend cette solution particulièrement

attractive pour la victime. Toutefois, dans beaucoup de cas, il pourra s'agir d'un pays éloigné, dont les coût de procédure (honoraires d'avocats, frais de justice,...) sont élevés. Surtout, il est à craindre que les sites contrefaisants se concentrent dans des pays dont la législation ou les tribunaux sont peu protecteurs de la propriété intellectuelle. Quant à la solution consistant à saisir le tribunal du pays de réception, elle présente l'inconvénient que chacun d'entre eux ne sera en principe compétent que pour réparer la part de préjudice subi dans le pays considéré. La victime devra donc multiplier les procédures dans les différents pays dans lesquels elle a subi un préjudice, ce qui n'est guère satisfaisant. En outre, le titulaire de droits lésé risque d'avoir des difficultés pour obtenir, dans le pays d'émission (i.e. où réside le contrefacteur), l'*exequatur* des jugements rendus dans les pays de réception.

Si l'on se place maintenant du point de vue du responsable du site, qui peut être en situation régulière au regard de sa loi nationale (par exemple si la copie qu'il a faite bénéficie d'une exception au droit d'auteur), il faut reconnaître que la jurisprudence actuelle est très protectrice de leurs intérêts. Il est peu probable, en effet, que l'*exequatur* du jugement rendu dans le pays d'émission sera accordée à la victime si l'atteinte au droit de propriété intellectuelle qui lui est reprochée ne constitue pas une contrefaçon au regard de la loi du pays d'émission.

? *Les solutions envisageables*

L'état actuel du droit est, au total, relativement protecteur pour les responsables de sites, mais il risque de favoriser la délocalisation des sites contrefaisants vers les pays peu protecteurs de la propriété intellectuelle. Ce phénomène de délocalisation, qui se développe dans d'autres domaines (voir quatrième partie, *infra*), risque de prendre une ampleur considérable en matière de propriété intellectuelle, compte tenu des dérives que l'on constate déjà aujourd'hui dans le domaine analogique et qui ont d'ailleurs été formellement reconnues par les gouvernements en préambule de l'accord " ADPIC " précité du 15 avril 1994. Il serait donc tout à fait contraire à la logique de cet accord que d'admettre que le caractère contrefaisant du contenu d'un site accessible depuis tout pays ne doit être apprécié qu'au regard de la loi du pays d'émission, avec le risque de délocalisation qu'implique cette solution. Il faut rappeler en outre que la France est l'un des pays au monde les plus protecteurs de la propriété intellectuelle, et qu'elle serait donc particulièrement affectée par une telle solution.

Il paraît donc très largement préférable de s'en tenir à la solution vers laquelle s'oriente la jurisprudence actuellement, c'est-à-dire **la loi et le tribunal du (ou des) pays de réception, pour la part du préjudice subi dans chacun d'entre eux**. La victime conserve naturellement la faculté, si elle a une chance de succès, de saisir également le tribunal du lieu d'émission. Il est toutefois important d'essayer de remédier aux inconvénients de cette solution qui ont été décrits plus haut, en facilitant l'*exequatur* (voir *infra*), et en évitant d'obliger la victime à multiplier les procédures dans les différents pays de réception.

Il faudrait ainsi donner au titulaire de droits lésé la faculté de saisir un tribunal, autre que celui du lieu d'émission, qui serait reconnu compétent pour réparer l'intégralité du préjudice subi au plan mondial. Ce tribunal devrait être celui qui présente le lien le plus étroit avec le préjudice . On pourrait présumer qu'il s'agit de celui dans lequel la victime a sa résidence habituelle (s'il s'agit d'une personne physique) ou son principal établissement (s'il s'agit d'une personne morale). Il ne s'agirait que d'une présomption simple, qui pourrait s'effacer si les circonstances particulières de l'affaire ou le choix des parties désignaient un autre tribunal comme étant celui qui présente le lien le plus étroit avec le préjudice (par exemple si l'essentiel du préjudice était subi dans un seul pays).

Toutefois, compte tenu des disparités existant entre les législations nationales en matière notamment d'exceptions au droit d'auteur (voir *supra*), il ne paraît ni possible ni souhaitable de

ne retenir qu'une seule loi applicable. **Le tribunal saisi devrait donc faire une application distributive des lois des différents pays de réception pour la part du préjudice subi dans chacun d'entre eux.** Ainsi, lorsque le contenu en cause est licite au regard d'une législation nationale, par exemple grâce au régime des exceptions au droit d'auteur, le tribunal n'accorderait aucune indemnité au titulaire de droits au titre de ce pays. La souveraineté des États et les traditions nationales en matière de propriété intellectuelle seraient ainsi préservées, tout en limitant les inconvénients pour la victime puisqu'elle n'aurait qu'un seul tribunal à saisir et donc une seule *exequatur* à solliciter. Quant à la difficulté pour le tribunal de connaître les lois étrangères, elle pourrait être surmontée grâce à l'aide d'organisations internationales telles que l'OMPI, qui pourrait jouer un rôle précieux sur ce point, mais également l'OMC, qui a d'ailleurs d'ores et déjà entrepris un important de travail de collecte d'informations sur les législations nationales en matière de propriété intellectuelle, dont elle a restitué les premiers résultats aux États membres .

Cette démarche internationale pourrait fort utilement être complétée, voire précédée par une avancée européenne, à la fois dans le cadre de la directive en cours d'élaboration sur le droit d'auteur et dans celui de la renégociation des conventions régissant les conflits de lois et de juridictions (en particulier celle de Bruxelles sur les règles de compétence entre juridictions). Des progrès pourraient tout d'abord être réalisés dans le domaine des conflits de juridictions. Ainsi, les deux solutions proposées ci-dessus dans un cadre international pourraient être d'ores et déjà appliquées au niveau de l'Union européenne voire de l'Espace économique européen. Outre l'accélération des procédures d'*exequatur*, **la victime pourrait donc saisir le tribunal de l'État européen ayant le lien le plus étroit avec le préjudice, qui serait compétent pour réparer l'intégralité du préjudice subi en Europe (U.E. ou E.E.E.). On pourrait toutefois présumer dans ce cadre que, lorsque le contenu contrefaisant est émis depuis un pays européen, le pays qui a le lien le plus étroit avec le préjudice est le pays d'émission (et non celui de la résidence de la victime).** Il ne s'agirait, là aussi, que d'une présomption simple. En outre, il faudrait considérer que le pays d'émission est celui dans lequel l'éditeur du contenu en cause a sa résidence habituelle, s'il s'agit d'une personne physique, ou son principal établissement dans l'Union européenne, s'il s'agit d'une personne morale. Il paraît en effet dangereux de se borner à ne retenir que le lieu dans lequel est physiquement réalisée l'injection du contenu sur l'Internet, ce qui pourrait conduire à des phénomènes de délocalisation (" *forum* shopping ").

À plus long terme, des progrès pourraient également être réalisés, au sein de l'Union Européenne, en matière de loi applicable. Mais des avancées décisives ne seront possibles sur ce point que lorsque le processus d'harmonisation des législations nationales sera parvenu à un niveau suffisant pour éviter les risques de délocalisation des sites numériques vers certains États membres, notamment en ce qui concerne les exceptions au droit d'auteur. Il faudrait parvenir, en matière de propriété intellectuelle, à un espace européen juridique " unique " en termes de loi applicable. **Ainsi, les principes exposés ci-dessus pour la répartition des compétences de juridiction entre pays européens pourraient également s'appliquer en matière de conflit de lois,** c'est-à-dire application de la loi du pays d'émission, lorsque le responsable du contenu réside dans un pays européen, ou sinon application de la loi du pays présentant le lien le plus étroit avec le préjudice (voir *supra*). Il conviendrait alors, par cohérence, que cette règle de conflit de lois s'applique également à l'aspect pénal du droit de la propriété littéraire et artistique.

L'harmonisation des règles relatives aux conflits de lois
et de juridictions, en matière d'atteintes au droit des marques

Dès lors qu'une marque n'est protégée que dans le (ou les) pays dans lesquels elle a été déposée (sous les réserves que l'on a vues plus haut), le responsable d'un site ne doit en principe en faire usage que dans les pays où il l'a enregistrée. Toutefois, il conviendrait que la jurisprudence ou, si

nécessaire, la loi elle-même, pose le principe que **le fait qu'un site présente un produit ou un service sous une marque qui, dans certains pays, appartient à d'autres titulaires que le responsable du site ne saurait constituer en lui-même une contrefaçon.** C'est le fait de commercialiser ces prestations dans le (ou les) pays en cause qui serait illicite, que ce soit par des ventes ou des démarches publicitaires.

Il résulte de ce caractère territorial du droit des marques que **la loi applicable pour apprécier le caractère contrefaisant de l'activité d'un site ne peut être que celle du pays dans lequel la marque litigieuse a été enregistrée, c'est-à-dire la loi du pays de réception**. L'application de cette loi peut conduire à interdire au responsable du site de commercialiser les produits contrefaisants dans le pays en cause, mais elle ne peut en aucun cas lui interdire cette commercialisation dans d'autres pays .

En termes de compétence juridictionnelle, il paraît évident que le tribunal du lieu de résidence du défendeur, c'est-à-dire du responsable du site (*i.e.* pays d'émission), est compétent. Mais on peut également admettre, suivant le raisonnement qui vient d'être exposé, la compétence du tribunal du pays dans lequel a été enregistré la marque (*i.e.* pays de réception). Il serait possible d'aller plus loin en conférant au titulaire de droits lésé la faculté, comme cela a été proposé en matière de propriété littéraire et artistique, de saisir **le tribunal du pays présentant le lien le plus étroit avec le préjudice subi en reconnaissant que celui-ci est compétent pour réparer l'intégralité du préjudice subi au plan mondial, sous réserve de l'application distributive des lois des différents pays dans lesquels la marque a été contrefaite** (voir *supra*). Le régime des présomptions pourrait être identique à celui qui a été proposé ci-dessus pour les œuvres littéraires et artistiques.

En conclusion, les principales adaptations du droit de la propriété intellectuelle qui paraissent nécessaires aujourd'hui concernent la détermination de la loi applicable et l'harmonisation du régime des exceptions au droit d'auteur, notamment pour ce qui concerne la copie privée. Il convient également d'engager au plus tôt une réflexion, dont la portée dépasse la question des réseaux numériques, sur la titularité des droits de l'employeur sur les œuvres créées par ses salariés.

La lutte contre la contrefaçon

Ce chapitre est consacré principalement à la contrefaçon en matière de propriété littéraire et artistique, mais les solutions proposées sont transposables dans une large mesure à la propriété industrielle, notamment au droit des marques. Des précisions seront apportées sur ce point lorsque cela s'avérera nécessaire .

Les titulaires de droits (auteurs, éditeurs, producteurs,...) sont très attachés au renforcement de la lutte contre la contrefaçon sur les réseaux numériques et en tout premier lieu sur l'Internet, et ils exercent une forte pression sur les différents gouvernements pour que ceux-ci renforcent l'arsenal répressif en la matière. Le risque de contrefaçon est en effet beaucoup plus élevé dans ce nouvel environnement dans la mesure où la copie numérique d'une œuvre est en réalité identique à l'original. En outre, il est extrêmement aisé, sur un plan pratique, de télécharger une copie, depuis un site numérique, sur le disque dur d'un ordinateur et de la dupliquer pour la retransmettre ensuite, via le réseau, à un grand nombre de personnes. On commence d'ailleurs à voir se développer sur l'Internet des plates-formes d'échanges et de diffusion de copies d'œuvres contrefaites (notamment dans le domaine musical, par exemple les œuvres de Jean-Michel Jarre qui sont particulièrement prisées des internautes). Ce phénomène n'est pas véritablement quantifié à l'heure actuelle mais les titulaires de droits redoutent le développement à large échelle de cette forme de contrefaçon.

Trois grandes difficultés rendent malaisée la lutte contre la contrefaçon sur les réseaux numériques :

– le caractère immatériel et généralement fugace des actes de contrefaçon, qui rend difficile leur constatation et donc la preuve devant le juge ;

– la rapidité de diffusion et de dissémination des copies contrefaisantes qui peut générer en très peu de temps (quelques heures suffisent) un préjudice considérable au titulaire des droits ;

– le caractère international des réseaux numériques qui fait souvent obstacle, à l'heure actuelle, à l'exécution à l'étranger des jugements rendus en matière de contrefaçon.

Ces difficultés appellent trois types de réponses : une plus grande responsabilisation des acteurs, une amélioration des procédures judiciaires et une coopération internationale accrue.

La responsabilisation des acteurs et l'identification des œuvres

Les principaux titulaires de droits, notamment les entreprises internationales d'édition ou de production (phonogrammes, audiovisuel,...) et les sociétés de gestion collective (SACEM, SACD, SCAM,...) ont engagé depuis quelques années, au plan international, un travail très important en vue de se donner les moyens de lutter efficacement contre la contrefaçon. Outre leur collaboration avec les gouvernements et les organisations internationales concernées (OMPI et OMC) pour améliorer le cadre juridique (voir *infra*), ces professionnels développent des dispositifs techniques pour protéger leurs œuvres contre la contrefaçon. Cette action se fait naturellement en partenariat avec les fabricants de logiciels et de matériels informatiques. Il convient d'encourager ces initiatives et d'inciter l'ensemble des acteurs concernés à coopérer entre eux de manière encore plus étroite en dépit d'intérêts économiques parfois divergents.

L'une des manières les plus efficaces pour les titulaires de droits de lutter contre la contrefaçon consiste à assurer la protection de leurs œuvres par des moyens techniques. Il faut distinguer deux types de dispositifs :

– les mécanismes de *protection* des œuvres visent à protéger une œuvre contre la contrefaçon en contrôlant à la fois l'accès à l'œuvre (en le subordonnant à une autorisation préalable ou à un paiement) et son utilisation (nombre de consultations ou de copies possibles). Ces dispositifs comportent en général un logiciel qui contrôle l'accès à l'œuvre qui est elle-même cryptée. Plusieurs entreprises, françaises et étrangères, commercialisent déjà ce type de techniques. Le développement de leurs ventes reste toutefois entravé par les restrictions à l'exportation de logiciels de cryptographie par les gouvernements et par les difficultés du paiement par voie électronique. Il serait souhaitable de lever ces deux obstacles à l'essor des dispositifs de protection technique (voir deuxième partie, *supra*) ;

– les mécanismes *d'identification* des œuvres ont pour objet d'apposer sur chaque œuvre (et sur chacun de ses éléments divisibles) un code d'identification indélébile et standardisé au plan international. Ce code constitue une sorte de " plaque minéralogique " de l'œuvre. Il peut être utilisé pour retrouver l'origine d'une contrefaçon, notamment s'il est complété par un identifiant propre à chacune des copies mises en circulation sur le réseau. Ce code peut également permettre la mise en place de " compteurs électroniques ", placés soit sur les sites, soit même sur les ordinateurs des utilisateurs, pour mesurer le nombre de consultations des œuvres et déclencher la facturation correspondante.

Les dispositifs techniques de protection des œuvres

La plupart des professionnels considèrent que les dispositifs de protection des œuvres

permettront une lutte relativement efficace contre la contrefaçon, à condition que l'utilisation et même la fabrication ou la vente de matériels destinés à contourner ces dispositifs soient réprimées pénalement. C'est d'ailleurs ce qu'ils ont obtenu à l'article 11 du traité sur le droit d'auteur et à l'article 18 du traité sur les interprétations et exécutions et les phonogrammes, adoptés lors de la conférence diplomatique tenue en décembre 1996 sous l'égide de l'OMPI, qui ont été signés par la France le 9 octobre 1997 . L'obligation pour les États de l'Union européenne d'introduire ces incriminations dans leurs législations nationales est également prévue dans la proposition de directive de la commission européenne du 10 décembre 1997 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information. Il serait souhaitable que la France introduise les dispositions correspondantes dans le code de la propriété intellectuelle dès que la position communautaire sur ce sujet aura été définitivement arrêtée.

Il faut noter que le Congrès des États-Unis examine actuellement un projet de loi qui met en œuvre le traité OMPI sur ce point. Ce texte se heurte toutefois à une vive hostilité des fabricants de matériel informatique qui ne veulent pas encourir de sanction dans le cas où ils commercialiseraient des appareils susceptibles de permettre le contournement des dispositifs de protection des œuvres, même si cela n'est pas la fonctionnalité principale de l'appareil en cause. Le Congrès s'oriente donc vers une incrimination très précise qui viserait uniquement ceux qui ont mis en vente des appareils principalement destinés à permettre le contournement des mécanismes de protection et qui ont assuré la promotion ou la publicité de ces appareils en faisant état de cette fonctionnalité. Cette solution de compromis semble dangereuse car elle permettrait aux industriels de fabriquer des matériels permettant le contournement des mécanismes de protection sous la seule condition que ce ne soit pas la fonction principale de l'appareil et que le vendeur n'en fasse pas un argument publicitaire. **Il conviendrait au contraire d'interdire strictement toute vente, distribution, fabrication ou importation d'un matériel permettant, dans son usage normal, le contournement des mécanismes de protection, et de sanctionner les fabricants et vendeurs de tels matériels.**

Les dispositifs techniques d'identification des œuvres

Les mécanismes de protection ne sauraient s'appliquer à toutes les œuvres, à la fois pour des raisons techniques et pour des raisons économiques (coûts de ces dispositifs). Ils ne sont en outre jamais totalement inviolables. Il est donc nécessaire de les compléter par des mécanismes d'identification des œuvres qui ont une finalité plus large. Ces derniers peuvent servir, comme cela a été indiqué, à des fins d'information du titulaire de droits et de l'utilisateur, mais également dans un but de facturation, d'enquête sur les réseaux de contrefaçon, de statistiques,...

Les milieux professionnels concernés reconnaissent l'importance et l'utilité des mécanismes d'identification. Il faut à cet égard souligner l'important travail accompli par les acteurs français dans ce domaine, notamment les sociétés de gestion collective (dans le cadre de la Confédération internationale des sociétés d'auteurs et compositeurs – CISAC), l'AFNOR et le ministère de la Culture. Ils ont obtenu que les normes techniques internationales (ISO) en matière de transmission d'images numériques fixes (norme JPEG) et d'images numériques animées multimédia (normes MPEG 2 et 4) incluent le principe d'un code d'identification international de l'œuvre. Les modalités d'attribution de ces codes à chaque œuvre sont également en bonne voie d'être définies et le sont d'ailleurs déjà pour certains types d'œuvres (code ISRC pour les phonogrammes, code ISAN pour les œuvres audiovisuelles,...). Par ailleurs, les matériels informatiques conformes aux normes JPEG et MPEG empêcheront la modification ou l'altération de ces codes. En outre, comme pour les mécanismes de protection, les deux traités OMPI précités de décembre 1996, ainsi que la proposition de directive européenne sur le droit d'auteur, imposent aux États membres de prévoir des sanctions appropriées à l'encontre des personnes qui suppriment ou modifient sans autorisation une information relative au régime des

droits, ou encore qui communiquent au public une œuvre pour laquelle cette même information a été supprimée ou modifiée sans autorisation.

Il faut ajouter que les titulaires de droits s'organisent au plan international pour mettre en place des réseaux de bases de données qui permettent, à partir du code d'identification, de retrouver les caractéristiques de l'œuvre et surtout les titulaires de droits. On peut citer en particulier le projet " Common Information System " (CIS) lancé par la CISAC, qui regroupe 159 sociétés d'auteurs appartenant à 87 pays. Dans le cadre de ce projet, les bases de données concernant les œuvres musicales et les œuvres audiovisuelles sont désormais interconnectées au niveau international . En revanche, les travaux avancent plus difficilement concernant les œuvres littéraires et les arts visuels (notamment la photographie). Il importe, sur un plan plus général, de veiller à ce que le réseau des bases de données relatives aux titulaires de droits reste ouvert à de nouveaux acteurs économiques, afin **d'éviter tout risque d'abus de position dominante de la part des sociétés de gestion collective**, qui serait contraire aux règles de concurrence, notamment communautaires.

Ces réalisations techniques en matière d'identification des œuvres apparaissent très prometteuses. Cependant, il faudra que les pouvoirs publics veillent au maintien d'une certaine harmonisation de ces mécanismes d'identification, en particulier quant aux règles d'attribution des codes à chaque œuvre. Mais il n'est pas nécessaire pour autant que les codes soient attribués par des administrations publiques, et ce n'est d'ailleurs pas le choix des professionnels. **Il s'agit davantage de faciliter la coopération des acteurs concernés,** comme le font d'ailleurs déjà dans une large mesure la commission européenne (dans le cadre du programme " Imprimatur " notamment) et le ministère de la culture en liaison avec l'AFNOR. **Il paraît, en revanche, tout à fait prématuré, à ce stade du développement technique, de rendre obligatoire cette identification des œuvres**. On pourra éventuellement l'envisager à plus longue échéance, ce qui impliquera sans doute une modification de la Convention de Berne, car la protection juridique du droit d'auteur serait alors subordonnée à une formalité obligatoire, ce qui est exclu dans la rédaction actuelle de cette convention.

En ce qui concerne l'utilisation des codes d'identification, notamment à des fins de facturation, un important travail technique demeure nécessaire. Un système de contrôle étroit de la consultation des œuvres par chaque utilisateur, par le biais des " compteurs électroniques ", ne devrait donc pas être possible avant plusieurs années. **Il conviendra toutefois que les pouvoirs publics veillent au respect de la vie privée des utilisateurs, en encadrant l'utilisation faite par les titulaires de droits des données recueillies par les " compteurs ".**

Il faudra également être attentif à ce que la logique essentiellement économique des systèmes de facturation liés aux mécanismes d'identification des œuvres, qui sous-tend également le développement des mécanismes de protection, n'en vienne pas à supprimer toute liberté de circulation des œuvres sur le réseau, comme on l'a vu à propos du régime des exceptions au droit d'auteur.

La coopération des acteurs

Les premiers acteurs de la lutte contre la contrefaçon doivent être les titulaires de droits eux-mêmes. Il leur appartient de s'organiser et de coopérer entre eux pour assurer la défense de leurs intérêts. Des efforts importants ont d'ailleurs déjà été réalisés dans ce sens. On peut citer en particulier la mise en place de " SESAM ", en juillet 1996 par les principales sociétés de gestion collective (ADAGP, SACD, SACEM, SCAM et SDRM). Cette nouvelle société de gestion collective constitue une sorte de " guichet unique " destiné à faciliter l'octroi des autorisations d'exploitation aux personnes qui souhaitent utiliser des œuvres déjà existantes pour les intégrer dans une nouvelle œuvre ayant un caractère multimédia (i.e. combinant de la musique, du texte

et/ou des images). Cette démarche destinée à faciliter l'utilisation des œuvres, en simplifiant la procédure d'autorisation et de perception des rémunérations, est intéressante et doit être poursuivie.

La logique de " guichet unique " n'implique pas nécessairement une extension de la gestion collective des droits, même si celle-ci doit être encouragée dans la mesure où elle facilite grandement la tâche de l'utilisateur pour l'obtention de l'autorisation et pour le paiement de la rémunération. En revanche, **il paraît indispensable que des organismes professionnels collectifs tels que " SESAM " développent une large fonction d'information en direction des publics concernés**. Ainsi, les titulaires de droits doivent, en coopération avec les fournisseurs d'accès d'hébergement, améliorer le niveau d'information du public sur les principes du droit d'auteur et notamment sur le principe de l'autorisation préalable. Diverses initiatives peuvent être envisagées en ce sens : mise en place d'un site d'information générale sur le droit d'auteur, qui pourrait s'inspirer de ce que pratique l'Agence de protection des programmes (APP) et auquel les fournisseurs d'accès et d'hébergement pourraient renvoyer leurs abonnés ; fiches d'information simples sur les procédures d'autorisation destinées aux personnes souhaitant créer un site ou une page personnelle, et qui pourraient être diffusées par l'intermédiaire des fournisseurs d'accès et d'hébergement ; etc.

Au-delà de cette information générale, il serait utile de développer une fonction d'orientation des demandes d'autorisation pour l'exploitation " en ligne " (sur un site) d'œuvres existantes. Dans un premier temps, l'organisme collectif (par exemple SESAM) pourrait se borner à orienter le demandeur vers la société de gestion collective concernée ou à aider le demandeur à déterminer le titulaire des droits sur l'œuvre pour laquelle est sollicitée l'autorisation. Mais à plus long terme, on peut imaginer que cet organisme indique au demandeur, moyennant une rémunération modique, en fonction du code d'identification de l'œuvre, le ou les titulaires de droits à contacter, grâce à la mise en place progressive des bases de données des titulaires de droits, dans le cadre notamment du " Common Information System " (CIS) (voir *supra*). Ce rôle d'information et d'orientation est essentiel si l'on veut que les personnes de bonne foi qui souhaitent utiliser une œuvre sur leur site ou leur page personnelle acquièrent le réflexe de solliciter l'autorisation préalable du titulaire des droits correspondants. Il est à noter que cette difficulté d'identification du titulaire des droits n'existe pas en matière de marques grâce au registre tenu par l'Institut national de la propriété industrielle, qui est facilement accessible par le public par voie télématique.

À l'égard des personnes qui commettent délibérément des actes de contrefaçon, **il paraît indispensable que les titulaires de droits regroupent davantage leurs moyens pour assurer une veille permanente sur le réseau et pour prendre les mesures appropriées (mise en demeure et, le cas échéant, poursuites judiciaires).** Les sociétés de gestion collective jouent déjà un peu ce rôle, mais à une échelle encore modeste. Des organismes comme l'Agence de protection des programmes (pour les logiciels mais plus généralement pour tout type d'œuvres) ou l'Union des fabricants (pour les marques et les produits) ont mis en place des équipes de veille chargées de rechercher les sites contrefaisants sur l'Internet et de leur adresser des mises en demeure. Ces organismes font également procéder à des constats par des agents assermentés ou par des huissiers (voir *infra*) en vue de procédures judiciaires. En matière d'œuvres musicales, les titulaires de droits américains, notamment les principaux producteurs de phonogrammes, ont par exemple mis en place une structure commune de lutte contre la contrefaçon sur l'Internet. Il faut souhaiter que ces exemples soient davantage suivis en France et surtout que les titulaires de droits acceptent de coopérer sur ce point en mettant les moyens nécessaires en commun. Là aussi, des organismes collectifs tels que SESAM peuvent jouer un rôle important.

Afin d'inciter les titulaires de droits à créer des organismes professionnels communs chargés de

lutter contre la contrefaçon, notamment sur les réseaux numériques, on pourrait envisager de leur conférer plusieurs avantages. Le premier est déjà prévu à l'article L.331-1 du code de la propriété intellectuelle qui dispose que " les organismes de défense professionnelle régulièrement constitués ont qualité pour ester en justice pour la défense des intérêts dont ils ont statutairement la charge. " Le second avantage existe également mais pourrait être étendu au domaine de la propriété industrielle : il s'agit de la possibilité de disposer d'agents assermentés habilités à constater les contrefaçons (voir *infra*). Le troisième avantage serait nouveau et viserait à privilégier ces organismes professionnels dans le cadre de " l'autorégulation " du réseau (voir *infra*).

La responsabilisation des acteurs et l'autorégulation

Dans le cadre de l'autorégulation (ou de la " corégulation ") du réseau Internet, il est essentiel que les fournisseurs d'accès et d'hébergement coopèrent avec les titulaires de droits pour lutter contre la contrefaçon sur les réseaux numériques. C'est pourquoi les titulaires de droits victimes d'une contrefaçon doivent adresser des mises en demeure non seulement au responsable du site contrefaisant, mais également au fournisseur d'hébergement du site en cause et même aux principaux fournisseurs d'accès afin que ceux-ci coupent l'accès à la page ou au site concerné à titre préventif. Leur refus serait en principe de nature à engager leur responsabilité pour complicité de contrefaçon. Toutefois, ce point n'a pas encore été clairement tranché par la jurisprudence française. Une clarification législative pourrait éventuellement être envisagée, en s'inspirant des exemples étrangers (voir *infra*, quatrième partie).

Aux États-Unis, un projet de loi portant spécifiquement sur la responsabilité des fournisseurs d'accès et d'hébergement en matière de contrefaçon est en cours d'examen par le Congrès. Il devrait sans doute être adopté d'ici la fin de l'année. Dans le projet soumis à la discussion (en date du 1er avril 1998), les *fournisseurs d'accès* ne sont pas considérés comme contrefacteurs s'ils ont transmis ou stockés à titre intermédiaire et temporaire (" cache ") un contenu contrefaisant, à condition qu'ils ne soient pas à l'origine de son émission, qu'ils n'en conservent pas une copie et que la transmission et le stockage résultent d'un procédé automatique. Ils doivent cependant respecter les instructions du site émetteur fixant la durée maximale de conservation de la page sur le " cache " (voir *supra*). Quant aux *fournisseurs d'hébergement*, ils ne peuvent pas davantage être poursuivis pour contrefaçon lorsqu'ils ont hébergé un contenu contrefaisant, à condition, d'une part, qu'ils n'aient pas connaissance (" actual knowledge ") du caractère contrefaisant de celui-ci et que ce caractère ne soit pas " apparent ", et d'autre part qu'ils ne perçoivent pas une rémunération provenant directement d'une activité contrefaisante qu'ils ont la possibilité de contrôler. Ils doivent en revanche retirer un contenu présumé contrefaisant s'ils sont requis à cet effet par un titulaire de " copyright " (droit d'auteur). Dans ce cas, leur responsabilité ne peut pas être engagée par l'éditeur du contenu en cause. En contrepartie, une personne arguant délibérément d'un " copyright " qu'elle ne possède pas engage sa responsabilité vis-à-vis de l'éditeur de contenu lésé. Les fournisseurs d'hébergement ne sont pas tenus de procéder à une recherche systématique des contenus contrefaisants, ni d'intervenir sur les contenus protégés par la loi, c'est-à-dire en pratique la correspondance privée (courrier électronique). Par ailleurs, ils conservent naturellement la faculté de dégager leur responsabilité en invoquant l'exception de " fair use ". En revanche, ils sont tenus de communiquer l'identité du responsable du site à tout titulaire de droits qui en fait la demande en vue d'une action en contrefaçon. Des règles analogues à celles prévues pour les fournisseurs d'hébergement sont instituées à l'égard des moteurs de recherche.

Le projet de loi américain apparaît très favorable aux fournisseurs d'accès, qui ne sont donc pas tenus de faire droit à des demandes tendant à bloquer l'accès de leurs abonnés à des pages présumées contrefaisantes. Cette obligation ne pèse que sur les fournisseurs d'hébergement. Une

telle solution n'est pas acceptable pour la France, compte tenu du fait qu'un grand nombre de sites contrefaisants sont situés à l'étranger, ce qui signifie que les fournisseurs d'hébergement échappent de fait à la compétence des juridictions françaises (voir *supra*). Il est donc indispensable de conserver le principe résultant de la jurisprudence traditionnelle, selon lequel toute personne qui s'est rendue complice, en connaissance de cause, d'une contrefaçon engage sa responsabilité civile et pénale. Par conséquent, tant les fournisseurs d'hébergement que les fournisseurs d'accès (sans parler bien évidemment des éditeurs de contenus eux-mêmes) doivent se doter des moyens de traiter rapidement les réclamations en contrefaçon émanant des titulaires de droits de propriété intellectuelle. Il leur appartient d'en apprécier le caractère sérieux afin de ne pas engager leur responsabilité vis-à-vis du site concerné pour coupure abusive de l'accès à celui-ci. On peut laisser le soin à la jurisprudence de déterminer l'étendue exacte des obligations de " diligence " des fournisseurs d'accès et d'hébergement, faisant tomber la présomption de mauvaise foi en cas de contrefaçon. Il est également envisageable d'introduire dans le code de la propriété intellectuelle une disposition analogue à celle proposée dans la quatrième partie du rapport, **limitant la responsabilité pour contrefaçon des fournisseurs d'accès et d'hébergement aux cas où ils n'ont pas accompli les diligences " normalement exigibles " de leur part pour faire cesser une contrefaçon dont ils avaient connaissance.** Cette disposition pourrait également s'appliquer aux moteurs de recherche et plus généralement à toute personne permettant de localiser un contenu contrefaisant sur l'Internet, notamment par des liens hypertextes.

L'organisme de corégulation des professionnels français de l'Internet (voir la quatrième partie, *infra*) pourrait recommander aux fournisseurs d'accès et d'hébergement de présumer qu'une réclamation en contrefaçon à l'encontre d'un site a un caractère sérieux dès lors qu'elle émane d'une société de gestion collective ou d'un organisme professionnel de lutte contre la contrefaçon et, par suite, de couper préventivement l'accès à la page ou au site concerné. Les titulaires de droits indépendants seraient ainsi fortement incités à adhérer à ce type d'organismes, tout en conservant naturellement la possibilité de présenter directement leurs réclamations en adressant aux fournisseurs d'accès et d'hébergement les pièces justificatives. Les organismes de lutte contre la contrefaçon pourraient également assurer la représentation des auteurs et de leurs ayants-droit au sein de l'organisme d'autorégulation, par exemple dans le cadre de commissions spécialisées en matière de propriété littéraire et artistique et de propriété industrielle.

Cette forme d'autorégulation, alliée à un renforcement des procédures judiciaires d'urgence (voir *infra*), pourrait suffire à assurer une protection efficace des titulaires de droits contre la contrefaçon.

L'amélioration des procédures judiciaires

Les titulaires de droits ont, pour la plupart, souligné que la législation française était l'une des plus protectrice des victimes de contrefaçon, que ce soit en termes de procédure ou de sanction. Pour autant, des améliorations semblent nécessaires pour répondre aux spécificités des réseaux numériques.

La constatation des actes de contrefaçon

Outre la possibilité, de droit commun, de faire constater les contrefaçons par des officiers ou agents de police judiciaire, les titulaires de droits ont la faculté de recourir à des agents assermentés spécialement habilités à cet effet. L'article L.331-2 du code de la propriété intellectuelle permet aux sociétés de gestion collective, au Centre national de la cinématographie et aux " organismes professionnels d'auteurs " de désigner des agents qui, après agrément par le ministre de la culture, peuvent être assermentés et ainsi habilités à constater les actes de contrefaçon. Les sociétés de gestion collective et des organismes tels que l'Agence de protection

des programmes, déjà citée, disposent d'ores et déjà de nombreux agents assermentés, dont cependant peu encore sont formés au nouvel environnement des réseaux numériques. L'accroissement du nombre d'agents compétents dans ce nouveau domaine est indispensable et implique donc un effort particulier de la part des titulaires de droits et de leurs organismes professionnels de lutte contre la contrefaçon.

Un effort de rigueur paraît s'imposer dans la procédure d'agrément de ces agents, en préalable à l'augmentation sensible de leur nombre. En effet, à l'heure actuelle, aucune condition particulière n'est fixée par les textes quant à la moralité, à la compétence professionnelle et à la nature des fonctions de ces agents. Ces agents ne disposent par ailleurs d'aucune garantie d'indépendance par rapport aux organismes qui les emploient, ce qui pourrait à terme poser des problèmes quant à l'impartialité de leurs constats. En outre, la législation est très imprécise sur la notion d'organismes professionnels d'auteurs susceptibles de disposer de ces agents, ce qui ouvre la voie à d'éventuelles dérives. Il est donc impératif de renforcer le cadre réglementaire de ces agréments en complétant l'article R.331-1 du code de la propriété intellectuelle sur ces différents points. On pourrait ainsi, par exemple, envisager de conférer aux agents assermentés le statut de salarié protégé dans le cadre du code du travail. Il serait par ailleurs utile que le ministère de la culture tienne un registre des agents assermentés, qui soit accessible au public par exemple par l'intermédiaire du site du ministère de la culture. On pourrait peut-être aussi envisager une forme d'agrément simplifié des organismes professionnels de lutte contre la contrefaçon en vérifiant notamment leur objet et la nature de leurs adhérents (auteurs ou titulaires de droits).

À l'heure actuelle, ces agents assermentés ne sont compétents qu'en matière de propriété littéraire et artistique. Il n'existe pas d'équivalent en matière de propriété industrielle. Les titulaires de droits dans ce domaine doivent donc recourir soit à des huissiers soit à des agents de la Direction générale de la consommation, de la concurrence et de la répression des fraudes (DGCCRF). **On pourrait envisager de créer une nouvelle catégorie d'agents assermentés, agréés à cet effet par le ministre chargé de l'industrie, en s'inspirant du régime décrit ci-dessus**. Ces agents pourraient être employés par des organismes professionnels de lutte contre la contrefaçon tels que l'Union des Fabricants.

Ces agents assermentés pourraient, outre leur rôle en matière d'établissement de la preuve de la contrefaçon, apporter leur concours aux tribunaux. Certains magistrats ont en effet émis le vœu de pouvoir faire appel, dans le domaine des nouvelles technologies de l'information, à des " consultants judiciaires ". Ceux-ci pourraient à la demande du juge, lors de l'audience, apporter des explications techniques sans qu'il soit nécessaire de recourir à la procédure plus lourde des experts judiciaires. Ces " consultants " pourraient également participer à des actions de formation des magistrats dans ces nouveaux domaines.

Les procédures d'urgence

En matière de propriété littéraire et artistique, le titre troisième du livre III du code de la propriété intellectuelle fixe des règles en matière de saisie-contrefaçon qui permettent une mise en œuvre facile de celle-ci grâce à des procédures très simples (saisie des exemplaires contrefaisants par le commissaire de police – art. L.332-1, CPI). Cependant, ces dispositions visent la saisie " d'exemplaires " contrefaisants, ce qui suppose un support matériel alors que les copies illicites circulant sur les réseaux numériques sont par nature immatérielles et insaisissables. Ces dispositions paraissent donc difficilement applicables sur l'Internet.

Il reste la voie du référé, qui a d'ailleurs déjà été utilisée à plusieurs reprises par les titulaires de droits, tant en matière de propriété littéraire et artistique que de propriété industrielle . Le juge des référés a fait montre dans ces premières affaires d'un souci de pragmatisme et de pédagogie.

Il n'a pas hésité à prononcer, sur le fondement des textes actuels, des injonctions tendant au retrait des contenus contrefaisants (œuvres ou marques). Il lui est même arrivé d'ordonner la publication sur le site contrefaisant d'un texte relatif à la contrefaçon avec un renvoi vers le site de l'Agence de protection des programmes (APP) . Cette procédure de référé est jugée relativement satisfaisante par les titulaires de droits.

Cependant, outre la voie de l'autorégulation déjà évoquée (*i.e*. coupure préventive, à la demande d'un titulaire de droits, d'une société de gestion collective ou d'un organisme professionnel d'auteurs, de l'accès à un site contrefaisant par les fournisseurs d'accès et d'hébergement), **il paraît utile que soit conférée au président du tribunal de grande instance la possibilité d'ordonner, à titre conservatoire, le retrait d'un contenu présumé contrefaisant et la coupure de l'accès audit contenu à tout fournisseur d'accès ou d'hébergement** (voir également *infra*, quatrième partie). On pourrait sur ce point s'inspirer des dispositions de l'article L.332-1 du code de la propriété intellectuelle (ordonnance sur requête). Il appartiendrait au demandeur de notifier ladite ordonnance aux fournisseurs concernés, et l'on pourrait même envisager qu'il soit autorisé à y procéder par courrier électronique. La méconnaissance de cette ordonnance pourrait être passible de sanctions pénales spécifiques en plus de celles prévues au titre de la contrefaçon.

L'efficacité des sanctions prononcées par le juge

Le pouvoir d'ordonner à tout fournisseur d'accès ou d'hébergement la coupure de l'accès au contenu contrefaisant, proposé ci-dessus à titre de procédure d'urgence, pourrait être conféré également au juge du fond dans les mêmes conditions. Comme précédemment, il ne serait pas nécessaire d'appeler à l'instance l'ensemble des fournisseurs d'accès et d'hébergement puisqu'il suffirait que le demandeur leur notifie le jugement pour que celui-ci leur soit opposable (sous réserve de tierce opposition). On pourrait également compléter l'article L.335-5, CPI, en donnant la faculté au tribunal d'ordonner la fermeture définitive d'un site contrefaisant et d'interdire à son responsable d'en ouvrir un autre pour une activité similaire. Par ailleurs, il faudrait également préciser à l'article L.335-6 du code de la propriété intellectuelle que le tribunal peut ordonner la publication du jugement sur tout support, y compris sur un site numérique.

On pourrait également envisager, eu égard au risque souligné en introduction, spécifique aux réseaux numériques, d'un préjudice considérable dans un délai très court, d'alourdir les sanctions pénales prévues en cas de contrefaçon, bien qu'un effort en ce sens ait déjà été consenti par le législateur en 1994 . On peut d'ailleurs relever que c'est la voie suivie par les États-Unis avec la loi dite " No Electronic Theft Act ", adoptée en novembre 1997, qui prévoit une peine de cinq ans d'emprisonnement et une amende pouvant atteindre 250 000 $ en cas de copie électronique illicite, même sans but lucratif, occasionnant un manque à gagner de plus de 1 000 $ au titulaire du " copyright " (droit d'auteur sur l'œuvre).

Toutefois, il est clair que la principale difficulté pour l'exécution des jugements résulte de l'insuffisante coopération judiciaire internationale, qui limite fortement les moyens d'action des titulaires de droits français à l'encontre des sites contrefaisants situés à l'étranger.

La coopération internationale

La coopération internationale des autorités politiques et judiciaires est une condition essentielle de la réussite de la lutte contre la contrefaçon. Le risque est grand, sinon, de voir se développer des " paradis numériques " dans des États peu protecteurs de la propriété intellectuelle. Cette coopération au plan judiciaire, d'ailleurs nécessaire sur un plan plus général en matière de réseaux numériques (voir *infra*, quatrième partie), est indispensable pour permettre l'exécution des jugements. Elle implique également, comme on l'a vu, une harmonisation des règles de

conflits de lois et de juridictions en matière de contrefaçon.

La protection de la propriété intellectuelle a fait l'objet très tôt d'une coopération internationale relativement avancée, avec notamment la convention de Paris sur la protection de la propriété industrielle (20 mars 1883) et la convention de Berne sur la protection des œuvres littéraires et artistiques (9 septembre 1886), qui font depuis lors l'objet de révisions régulières. Cette volonté de coopération a d'ailleurs conduit à la création, en 1967, de l'Organisation mondiale de la propriété intellectuelle (OMPI), qui prend régulièrement l'initiative de conférences diplomatiques qui peuvent déboucher sur la signature de conventions internationales, telles que les deux traités déjà cités conclus en décembre 1996 sur le droit d'auteur.

La volonté de lutter contre la contrefaçon a par ailleurs été réaffirmée dans le cadre de l'Organisation mondiale du commerce (OMC). Elle a conduit à l'adoption en 1994 de l'accord " ADPIC " (Aspects des droits de propriété intellectuelle qui touchent au commerce), déjà mentionné. Cet accord prévoit notamment que les législations des États parties doivent comporter des procédures permettant une action efficace contre les atteintes aux droits de propriété intellectuelle. Il s'agit là, compte tenu du nombre important d'États signataires (132), d'un important progrès dans la coopération intergouvernementale pour lutter contre la contrefaçon.

Cette coopération entre les États doit être poursuivie dans toutes les enceintes appropriées, notamment celles de l'OMPI, de l'OMC et de l'OCDE. L'un des points qui demeure le plus préoccupant est, comme cela a été indiqué plus haut, la difficulté de l'exécution des jugements rendus en matière de contrefaçon. Les prochaines négociations internationales devront donc viser, en plus de l'harmonisation progressive des législations en matière de propriété intellectuelle, à simplifier les procédures d'*exequatur*, qui permettent l'application d'un jugement dans un pays étranger. Les solutions retenues pourraient notamment s'inspirer des règles prévues par les conventions de Bruxelles (27 septembre 1968) et de Lugano (16 septembre 1988) concernant la reconnaissance et l'exécution des jugements entre les pays appartenant à l'Espace économique européen. **Cette simplification de l'*exequatur*, qui pourrait prendre la forme d'une procédure d'urgence dans le pays d'émission, pourrait au moins concerner la partie du jugement prononçant l'injonction tendant à faire cesser l'émission du contenu contrefaisant vers le pays de réception en cause** (à charge pour le site d'adopter les dispositifs techniques nécessaires pour filtrer les demandes d'accès en provenance de ce pays). La procédure simplifiée pourrait également concerner les dommages et intérêts.

Cette simplification de la procédure *d'exequatur* devrait être plus facile dans un domaine tel que la propriété intellectuelle, dans laquelle existe une longue tradition de coopération internationale. Elle pourrait préfigurer des améliorations de la coopération judiciaire internationale dans d'autres matières (voir la quatrième partie, *infra*).

En conclusion, l'adaptation du régime de la propriété intellectuelle et la lutte contre la contrefaçon sur les réseaux numériques constituent, au-delà de leur importance culturelle, un enjeu économique extrêmement important. Ces adaptations conditionnent le développement de l'Internet, comme en atteste l'attentisme prudent des éditeurs d'œuvres littéraires et artistiques à l'heure actuelle. Il convient donc que les gouvernements favorisent la coopération des différents acteurs. Il faudra surtout qu'ils harmonisent leurs législations autant qu'il sera possible et surtout facilitent l'exécution des jugements rendus en matière de contrefaçon, notamment en clarifiant les règles de conflits de lois et de juridictions.

Quatrième partie

Lutter contre les contenus et comportements illicites

Pour certains, l'Internet et les réseaux numériques sont des espaces privilégiés pour la délinquance et la criminalité, des outils nouveaux de déviances ; espace virtuel, le monde en réseau assurerait ainsi l'impunité des coupables.

L'imaginaire collectif s'empare alors de cette crainte diffuse face à un phénomène encore mal connu et justifie un repli frileux voire un interventionnisme restrictif.

Il faut apprécier la réalité de l'enjeu de façon sereine plutôt qu'émotionnelle.

À l'instar de toute technologie de communication à son stade initial de développement, l'Internet et les réseaux sont susceptibles de véhiculer des activités délictueuses ou contestables.

La criminalité informatique est une notion floue qui recouvre des réalités multiples : sans vouloir dresser un catalogue exhaustif des attitudes répréhensibles, on estime qu'elles sont de deux types : les infractions commises contre le réseau lui-même, les infractions commises grâce au réseau. Dans le premier cas, il s'agit d'atteintes aux systèmes informatiques eux-mêmes (intégrité des données, confidentialité, accès non autorisé...) et il est clair que les progrès des techniques offrent aux criminels des moyens d'action nouveaux et efficaces ; dans le deuxième cas, il s'agit d'infractions classiques qui existaient déjà en dehors du réseau.

Il n'y a donc pas véritablement une criminalité *sui generis*, sectorielle, spécifique au cyberespace et fondée sur de nouveaux types d'atteintes ou de comportements.

Il est très difficile d'avoir une connaissance statistique précise de la criminalité informatique, ces infractions n'étant pas systématiquement dénoncées à l'autorité judiciaire, probablement pour préserver la crédibilité du système de sécurité et l'image de la société victime. Ainsi, la direction centrale de la Police judiciaire a-t-elle diligenté 400 enquêtes au cours de l'année 1997 alors que France Télécom avoue connaître environ 900 attaques de son système informatique par week-end. De plus, ces chiffres ne concernent que les atteintes au réseau lui-même et non les infractions de droit commun réalisées à l'aide du réseau, dont l'ampleur est aujourd'hui totalement ignorée.

Le dispositif textuel, code pénal ou lois spécifiques, est globalement suffisant pour sanctionner la plupart des infractions relatives aux droits des personnes, des données ou du consommateur. Faisant écho à une analyse doctrinale développée par la majorité des juristes depuis deux ans, les premières décisions de jurisprudence n'ont pas consacré une vision " anarchique " des réseaux et, tant en matière pénale qu'au civil, les juges ont souhaité transposer au réseau les règles de droit traditionnelles.

Cette analyse a été confirmée lors du dernier sommet G7-P8 à Washington, en décembre 1997 : le communiqué suivant la réunion des ministres de la Justice et de l'Intérieur affirme que " les législations s'appliquent à l'Internet et à d'autres réseaux mondiaux... Chaque pays doit être doté d'une législation interne qui permette de qualifier d'infraction l'usage litigieux de réseaux et de recueillir en temps utile les preuves des délits liés aux technologies de l'information ".

Ce qui est nouveau, c'est d'une part, la plus grande facilité avec laquelle ces infractions peuvent être commises et diffusées dans le monde du fait de la structure du réseau et de son mode de fonctionnement et, d'autre part, les difficultés rencontrées dans l'application des textes du fait de la fugacité extrême des contenus et de la dimension internationale d'Internet.

L'objectif est donc de proposer des solutions concrètes pour que la règle de droit soit respectée, et que l'espace nouveau d'expression humaine que constitue Internet et les réseaux ne soit pas symbole de transgression facile et non sanctionnée.

Il importe dès lors de préciser le champ d'application de la loi pénale et civile et la compétence du juge français, de clarifier les responsabilités des acteurs et d'accroître l'efficacité de l'intervention de la police et du juge.

Cependant, la lutte contre l'illégalité sur Internet ne saurait se résumer à une action répressive : ce monde est trop décentralisé, trop international pour que la réponse législative ou réglementaire de sanction *a posteriori* soit la seule ; il convient de la combiner avec l'autorégulation des acteurs, c'est-à-dire la participation active et préventive de ceux-ci au respect de l'État de droit sur les réseaux.

Préciser la loi applicable et la compétence du juge français

Une des premières questions qui se pose concernant Internet est celle de la détermination de la loi applicable. Celle-ci qui définit l'illégalité potentielle d'un site ou d'un comportement et les acteurs doivent être éclairés à ce sujet. Par ailleurs, la victime doit savoir quelle juridiction saisir. Si peu de difficultés existent au plan pénal, des adaptations sont sans doute nécessaires en matière civile.

En matière pénale

Les règles générales de compétence du droit français permettent en théorie d'appréhender la plupart des contenus ou comportements délictueux sur Internet.

Selon le code pénal, dans sa rédaction applicable au 1er mars 1994 , la loi française est applicable aux infractions commises sur le territoire de la République (art.113-2) ; l'infraction est réputée commise sur le territoire dès qu'au moins un de ses éléments constitutifs a lieu dans l'espace maritime, terrestre ou aérien de la République française (art.113-2). Pour un acte de complicité commis de France, bien que le crime ou le délit ait été commis à l'étranger, le complice pourra être poursuivi en France si le fait principal est puni par la loi française et étrangère (art.113-5).

Il résulte de ces dispositions que la loi pénale française s'appliquera clairement dans le cas d'un message litigieux disponible sur le réseau Internet, quelle que soit sa source dans le monde, **et accessible de France** dès lors que la réception par l'utilisateur sur le territoire français est bien un élément constitutif de l'infraction en application de l'article 113-2 du code pénal. Un tel mécanisme aboutit en réalité à dissocier le lieu de la réalisation matérielle de l'infraction de celui où elle produit ses effets, et donne au juge national une compétence très large.

En outre, la loi pénale française est applicable aux infractions commises hors du territoire de la République dans les situations suivantes :

– pour les crimes commis par un Français (art.113-6) ;

– pour les délits punis par la législation du pays où ils ont été commis par un Français (art.113-6).

Enfin, une jurisprudence constante (Cass. Crim. 5-8 1920 Bull. no 355 ; Cass. Crim. 15-01 1990 Bull. no 22) considère que la juridiction française est compétente pour connaître des faits commis par un étranger dès lors que ces faits forment un tout indivisible avec les infractions imputées en France à cet étranger et dont elle est également saisie.

Le code de procédure pénale définit, en outre, les règles de compétence territoriale (art 43 : compétence du procureur de la République ; art 52 : compétence du juge d'instruction ; art 382 compétence du tribunal correctionnel ; art 522 : compétence du tribunal de police). En principe, le tribunal compétent est celui du lieu de l'infraction – commission ou constatation des faits –, celui de la résidence du prévenu ou du lieu d'arrestation, voire du lieu de détention. Le domicile de la victime ne constitue un critère de compétence que dans des hypothèses tout à fait exceptionnelles, comme par exemple l'abandon de famille (art 382 du code de procédure pénale).

En matière civile

Compétence juridictionnelle

Les règles françaises internes de compétence territoriale ont été étendues par la jurisprudence à l'ordre international. La victime peut saisir, à son choix, le tribunal français du domicile du défendeur (article 42 du nouveau code de procédure civile), celui du fait dommageable ou dans le ressort duquel le dommage a été subi (article 46 NCPC) ou encore un tribunal français (sans autre précision), dès lors que le demandeur ou défendeur est de nationalité française ou a son domicile en France (articles 14 et 15 du code civil étendu à ce dernier cas par l'article 4§2 de la convention de Bruxelles). Les conventions de Bruxelles (27 septembre 1968) et de Lugano (16 septembre 1988) prévoient également que la victime peut saisir à son gré, soit une juridiction de l'État du domicile du défendeur (art. 2), soit celle du lieu où le fait dommageable s'est produit (article 5.3).

Le lieu de l'événement causal ne correspond pas toujours au lieu de survenance du dommage (cas où l'information est mise sur le réseau dans un pays et lue dans un autre pays). Il peut par ailleurs y avoir une pluralité des lieux du dommage.

Les tribunaux français peuvent être saisis par la victime d'un délit commis " en ligne " dès lors que la victime pourra établir que l'information pouvait être consultée en France et qu'elle a causé un dommage sur le territoire national. C'est ce qui a été récemment jugé par une décision en matière de droit d'auteur du tribunal de commerce de Paris (3 mars 1997 *Sté Ordinateur Express/Sté ASI*) selon laquelle le lieu où a été constaté l'infraction détermine la juridiction compétente. En d'autres termes, le lieu du délit n'est pas celui du serveur contrefacteur mais celui où a été subi le préjudice.

Droit applicable

En matière contractuelle, la détermination de la loi applicable relève de l'expression de la volonté des parties. En l'absence de prévision contractuelle, le tribunal saisi du litige recherchera le pays avec lequel le contrat présente les liens les plus étroits (voir *supra* deuxième partie).

En matière délictuelle, la loi applicable est déterminée selon les règles de conflits de lois de l'État dont la juridiction est saisie sauf lorsqu'une convention détermine la loi applicable à la matière en cause.

Il existe une grande divergence entre les règles de conflit des États, y compris au sein de l'Union européenne.

On citera par exemple, en matière de diffamation, les divergences entre les règles allemandes qui obéissent au principe de l'ubiquité (la loi applicable peut être celle de tout pays où soit l'événement causal, soit le dommage s'est produit, solution très favorable à la victime), celles du Royaume-Uni (qui ne permet l'action que si elle est admise à la fois par la loi du pays où le fait s'est produit et par la loi anglaise) et celles de la France.

En France, la jurisprudence considère que la loi applicable est celle du lieu dans lequel le fait dommageable s'est produit, ce lieu s'entendant aussi bien comme celui du fait générateur du dommage que comme celui du lieu de réalisation de ceux-ci (Cass. Civ. 14-01-97 Bull no 97504). En matière de délits internationaux commis par voie de presse, la loi du lieu de diffusion du message est souvent assimilée au lieu où le fait générateur s'est produit (CA Paris, 7 mars 1988 *SA Information et Revistas / NMPP*).

Cette règle s'applique à Internet. Par un jugement en date du 21 août 1997, le TGI de Draguignan a ainsi reconnu applicable la loi du territoire de réception.

Face à la multiplicité et à la diversité des systèmes juridiques étrangers, un risque d'absence d'unité de la loi applicable apparaît, les contradictions existant entre les lois pouvant aboutir à une inexécution de la décision à l'étranger.

Application de la décision

Il convient que la décision se voie conférer une force exécutoire à l'étranger, notamment pour obtenir l'interdiction d'un site contrevenant. Chaque système juridique étatique fixe à cet égard des conditions qui lui sont propres pour la reconnaissance et l'exécution de décisions étrangères.

Le droit français prévoit cinq critères pour apprécier la régularité d'une décision étrangère :

– l'autorité étrangère doit être compétente au regard du droit français ;

– la décision doit être conforme au système français de conflits de lois ;

– la décision étrangère doit être compatible avec l'ordre public français ;

– la décision ne doit pas entrer en conflit avec une décision déjà efficace en France ;

– les droits de la défense doivent être respectés.

Si le principe veut que la décision étrangère ne devienne exécutoire qu'à l'issue d'une procédure d'*exequatur*, la convention de Bruxelles, applicable à la quasi-totalité des États d'Europe occidentale, prévoit en son article 26 al. 1er que les décisions rendues dans un État contractant sont reconnues dans les autres États contractants, sans qu'il soit nécessaire de recourir à aucune procédure. Seule l'exécution forcée dépend d'une décision d'*exequatur* préalable, une procédure simplifiée étant prévue (article 31) par voie de requête présentée au président du TGI.

Conclusion

La multiplication des cas d'application extraterritoriale de la loi liée au caractère transnational du réseau et la diversité des systèmes juridiques existant dont l'application peut être simultanément revendiquée rendent difficile l'application des règles traditionnelles du droit international privé.

Cependant, il n'est sans doute pas opportun aujourd'hui d'imaginer une solution spécifique pour les réseaux compte tenu du caractère encore limité de leur développement. Par ailleurs, les informations concernées sont celles du droit commun.

Les travaux internationaux actuels sur les règles de droit international privé en matière délictuelle qui doivent conduire à l'élaboration d'une " nouvelle " convention de Rome (Rome 2) retiennent de nouvelles orientations : conformément à celles-ci, la loi applicable serait celle du pays qui a les liens les plus étroits avec le dommage, une présomption désignant celui de la résidence habituelle de la victime ; les mêmes règles devraient s'appliquer pour le choix du tribunal compétent ; le tribunal du lieu de domicile serait en outre compétent pour réparer

l'intégralité du préjudice subi car, *in fine*, c'est bien au domicile de la personne lésée que l'intégralité du dommage est subi. Il reste que les problèmes d'*exequatur* resteront importants sauf à imaginer des solutions spécifiques pour les réseaux.

À l'avenir, une convention internationale pourrait en conséquence être envisagée pour déterminer la loi applicable, le tribunal compétent et les règles d'*exequatur*.

Clarifier les responsabilités des acteurs

La responsabilité des acteurs de l'Internet est une des questions-clé de la régulation de ce nouvel espace. En effet, comme le souligne le professeur Trudel, responsable du laboratoire de droit public de Montréal, le monde des réseaux est un monde de communication et non seulement de diffusion, ce qui rend la réglementation étatique particulièrement difficile à mettre en œuvre et plus que jamais nécessaire l'autorégulation des acteurs ; il ajoute cependant : " les internautes ont beau proclamer que le Net est un espace de liberté, le droit les rejoint lorsqu'il faut que quelqu'un réponde des informations préjudiciables ayant circulé sur le réseau. Il est tout à fait prévisible que la régulation émergera des demandes visant à repartir et à préciser les responsabilités respectives des acteurs de la communication électronique ".

Ces demandes existent aujourd'hui, la plupart des acteurs ne pouvant plus gérer l'incertitude juridique qui leur semble s'attacher à leurs activités. Il est donc opportun, si l'on veut construire un espace de confiance, de formuler des réponses.

La question se pose au plan mondial. Elle n'est pas sans conséquences économiques pour les acteurs et le développement du marché. Les réponses données doivent être efficaces, légitimes et adaptées à un environnement en perpétuelle évolution.

Enfin, derrière la responsabilité, c'est toute une approche, une éthique de ce nouvel espace qui est en cause : le monde de l'Internet et des réseaux est à imaginer, à bâtir et les choix qui seront faits doivent permettre d'en faire un nouvel espace de " civilité mondiale " et non de délinquance.

Comment apprécier cette question dans le cas français ? Le droit positif actuel de la communication ne saurait fonder l'intégralité de l'analyse relative à la responsabilité pénale. Les premières affaires évoquées devant le juge ouvrent certaines pistes qui confirment l'inspiration des exemples étrangers. Il convient dès lors de formuler des recommandations qui reposent tant sur une clarification des règles applicables et que sur la reconnaissance du rôle d'un organisme de corégulation.

L'inadéquation de la responsabilité en cascade au monde des réseaux

En tant que services de communication audiovisuelle au public, au sens de l'article 43 de la loi du 30 septembre 1986, les opérateurs de services offerts sur Internet sont tenus à une obligation de déclaration auprès du Conseil supérieur de l'audiovisuel (CSA) et du procureur de la République, et doivent comporter un directeur de la publication. L'article 93-3 de la loi du 29 juillet 1982 dispose que lorsqu'une infraction de presse, prévue par la loi du 29 juillet 1881 , est commise par un moyen audiovisuel, le directeur de la publication est poursuivi comme auteur principal et, à titre subsidiaire, l'auteur puis le producteur .

Ce régime s'est progressivement étendu à des infractions de droit commun (une vingtaine), commises par voie de presse écrite ou audiovisuelle, telles que les infractions de mise en péril de mineurs .

Ces dispositions ne sont applicables que lorsque la " publication " est réalisée en France ; la

jurisprudence, dans le cas des journaux imprimés ou publiés dans un pays étranger, a considéré que la responsabilité éditoriale ne s'appliquait pas (crim. 15 février 1894) même s'ils étaient disponibles en France ; pour Internet, ces dispositions seraient donc applicables aux seuls services édités en France.

Pour toutes les autres infractions qui seraient commises sur ou par les réseaux, le régime de responsabilité est celui du droit commun ; c'est-à-dire " que nul n'est responsable que de son propre fait " (article 121-1 du code pénal) et qu'" il n'y a pas de crime ou de délit sans intention de le commettre " (article 121-3 du code pénal). La responsabilité peut être engagée en qualité d'auteur ou en tant que complice si cette personne a, sciemment, par aide et assistance, facilité la préparation ou la commission du délit (article 121-7 du code pénal).

La transposition du régime de la responsabilité éditoriale " en cascade " au monde de l'Internet et des réseaux a suscité beaucoup de controverses, tant auprès des acteurs privés qu'au sein de la doctrine. Il est certain que ce régime qui avait été conçu pour protéger la liberté d'expression du journaliste et faciliter l'établissement de la preuve ne répond guère à la logique et aux pratiques de ce nouveau monde.

Il est tout d'abord difficile de fixer, *a priori*, une chaîne de responsabilité d'acteurs, aux fonctions stables et déterminées, alors que ceux-ci peuvent, sur les réseaux, exercer pratiquement toutes les fonctions ; certes, il y a des métiers distincts (fournisseur d'accès, hébergeur, éditeur de contenus...) mais ceux-ci ne sont pas liés de façon permanente à un type d'acteur. Il faut donc raisonner par fonction et déterminer au cas par cas, le schéma de responsabilité.

À ce stade, plusieurs fonctions peuvent être identifiées :

– éditeur de contenus : création et production de contenus mis à disposition du public ;

– hébergement de site : fonction consistant à gérer les ressources informatiques connectées à l'Internet ;

– fournisseur de services : fonction d'intermédiation entre un éditeur de contenus et l'abonné ;

– opérateur de bouquet ou ensemblier : assemblage en une offre commerciale unique de plusieurs contenus ou services ;

– fournisseur d'accès : commercialisation de la prestation technique d'interconnexion d'équipements privés d'abonnés avec infrastructure IP ;

– transporteur : opérateur technique assurant l'interconnexion entre réseaux.

Un même acteur peut exercer plusieurs fonctions ; la plupart des fournisseurs d'accès sont ainsi hébergeurs, voire éditeurs de contenus. Les fonctions " d'intermédiation technique " sont, en général, considérées comme celles d'accès et d'hébergement.

Cependant, l'analyse fonctionnelle peut, elle-même, devenir caduque en fonction de l'évolution des techniques.

Par ailleurs, **la multiplicité des services offerts par Internet ne correspond pas à la logique simple et univoque de la responsabilité éditoriale " en cascade "**.

En effet, si les sites Web " classiques " mettant de l'information en ligne (type les Echos, le Monde...) peuvent être proches de l'activité éditoriale classique, que penser des forums de discussions, des services de messagerie électronique, des pages personnelles des abonnés, des services de commerce électronique... ? En réalité bien que partageant l'espace réseau, ces

activités ne s'inscrivent pas dans une communauté éditoriale contrôlée par un éditeur, le fournisseur d'accès. Par exemple, AOL peut-il être réellement déclaré responsable des pages personnelles de ses abonnés ou des propos racistes prononcés dans l'un des nombreux forums qu'il propose ? Son offre commerciale et marketing fondée sur une présélection de sites qu'il édite lui-même ou sur lequel il renvoie le transforme-t-il toujours en un directeur de la publication ?

De même, le fonctionnement spécifique et original de l'Internet, fondé sur les liens hypertexte qui crée une arborescence de l'information au plan mondial n'est pas celui d'un contrôle du contenu mais d'une facilité élargie de consultation et d'accès. La pratique enfin des " caches " qui dupliquent automatiquement, sur le serveur du fournisseur d'accès, les sites les plus demandés par les abonnés afin de diminuer le temps de connexion est-elle celle d'un choix éditorial qui rendrait le fournisseur d'accès responsable des contenus litigieux stockés sur le cache ? Toutes ces remarques, ces questions montrent bien que l'espace réseau n'est pas un simple espace nouveau de diffusion d'information mais un espace de communication, interactif, multiforme, commercial ou non, qui s'éloigne de l'édition classique de contenus et rend difficile la fixation d'un régime unique de responsabilités, fondé le principe de la cascade.

L'existence de sites à vocation commerciale justifierait pour certains la suppression de la cascade et l'application d'un régime de responsabilité de droit commun : doit-on incriminer pour appel à la haine raciale des galeries marchandes, des serveurs de données comme la météo, données statistiques... ?

L'hétérogénéité des acteurs, enfin, et notamment le rôle des particuliers ne correspond pas au monde éditorial classique : sur les réseaux, n'importe quel acteur, opérateur économique important, individu ou association peut se livrer aux mêmes activités. Or, la réglementation en matière de presse et d'audiovisuel était conçue pour des entités d'une certaine taille sur lesquelles pèsent des obligations, non seulement en fonction de l'importance des fautes commises mais surtout en contrepartie du profit retiré de leurs activités (théorie du risque-profit). Comment faire peser des obligations identiques sur des acteurs aussi différents que ceux de l'Internet et qui n'obéissent pas tous à cette logique de profit ?

Ces quelques points montrent bien que le monde des réseaux est complexe, constitue beaucoup plus qu'un simple nouveau support et que cette logique du support, initiée par la presse, transposée à l'audiovisuel puis à la télématique trouve aujourd'hui ses limites.

Comment dès lors apprécier les responsabilités ?

Les enseignements de la jurisprudence et des exemples étrangers

La jurisprudence relative à la télématique et aux premières affaires constatées sur Internet ainsi que les orientations qui se dessinent à l'étranger consacrent des principes convergents : droit commun de la responsabilité, contrôle et connaissance.

La jurisprudence

Les poursuites en matière de presse et de télématique ne sont pas nombreuses et le sont essentiellement à l'initiative des victimes ; le parquet n'est guère actif dans ces domaines tant par souci de préserver la liberté d'expression que par méconnaissance des pratiques et contenus sur les réseaux ; les poursuites sur le fondement de l'article 227-24 du code pénal sont relativement rares, les tribunaux se livrant au surplus à une interprétation restrictive de cet article en exigeant, en plus de la violence et du caractère pornographique du message, une atteinte grave à la dignité humaine.

La jurisprudence intervenue en matière de télématique a permis de dégager cependant certains principes : elle a reconnu la responsabilité du fournisseur de service quant au contenu. (Cass. crim, 15 novembre 1990, Ulla, Cass. Crim. 17 novembre 1992 PPX et Neron) ; elle a exclu la responsabilité du centre serveur et celle du transporteur (affaire Midratel 1992). Cette exonération de responsabilité est toutefois subordonnée à l'absence de connaissance du délit ou de violation de l'engagement contractuel avant ou au moment de la commission des infractions.

Par ailleurs, la notion " d'insuffisance nécessairement volontaire des mesures de contrôle " d'accès aux mineurs (3615 ALINE TGI de Paris, 9 octobre 1997 et Donadio TGI de Nanterre 12 février 1998), établissant l'existence du caractère intentionnel du délit, a été retenue.

L'ensemble de cette jurisprudence est cependant intervenue sur le fondement du droit commun et non sur celui de la responsabilité en cascade.

Concernant le réseau Internet, une vingtaine d'affaires sont intervenues depuis deux ans, notamment en matière de droit d'auteurs (voir *supra* troisième partie), certaines d'entre elles ayant posé la question de la responsabilité des acteurs. Les contentieux ont été en majorité portés devant le juge civil et introduits, dans la plupart des cas, selon la procédure du référé. Les décisions illustrent déjà certains points de discussion.

La plupart des actions ont été engagées à l'encontre des auteurs principaux, entreprises éditeurs de sites, personnes privées éditeurs de " home pages ".

Dans l'affaire *UEJF c/ Costes* (TGI Paris, 10/07/1997), il était reproché au fournisseur d'hébergement d'avoir rendu possible la diffusion d'écrits à caractère raciste. L'assignation a été déclarée nulle en raison d'un vice de procédure.

Dans l'affaire *Queneau* (TGI Paris, 5 mai 1997, précité), l'*association Mygale de l'université de Paris VIII*, a été poursuivie pour contrefaçon en tant qu'hébergeur sans que le juge puisse se prononcer sur la responsabilité de celle-ci.

Dans l'affaire *Yves Rocher* (TGI, 16 avril 1996) dans le cas d'une brochure mise sur le réseau exprimant les griefs de M. Yves Rocher à l'encontre du groupe BNP-BANEXI, le juge a déclaré que si une personne prend l'initiative de diffuser des informations manifestement illicites, elle ne peut pas se retrancher derrière la nature de l'Internet pour mettre devant le fait accompli les personnes auxquelles cette divulgation porte préjudice. Le juge a considéré que le prévenu aurait du être en mesure de " justifier des efforts et démarches accomplis pour faire cesser l'atteinte au droit d'autrui ou en limiter les effets ".

Au titre des condamnations pénales, il convient de mentionner la condamnation intervenue sur le fondement de l'art. 226-19 du code pénal pour diffusion de données nominatives portant sur les mœurs d'une personne (TGI de Privas septembre 97, *Ministère public et Mlle S c/ M. F*). Il s'agissait en l'espèce d'une diffusion de photos à caractère pornographique accompagnées de commentaires. Une autre condamnation est intervenue sur le fondement de l'art. 227-23 du code pénal pour recel d'images pédophiles, la réception d'images pornographiques de mineurs ayant été constatée à l'issue d'une enquête du SRPJ (TGI Le Mans 16 février 1998 *Procureur. République c/ Philippe H.*).

Dans l'affaire *UEJF C/ Calvacom* (TGI Paris, 12/06/96), le plaignant, après avoir constaté qu'était disponible sur Internet des messages et documents négationnistes avait assigné neuf fournisseurs d'accès en référé afin qu'il leur soit ordonné sous astreinte d'empêcher leurs clients d'accéder à ces messages. La demande a été rejetée comme trop générale et imprécise. Les défendeurs ont fait valoir que leur responsabilité ne saurait être recherchée en leur qualité de fournisseur d'accès, leur seule éventuelle responsabilité devant être limitée aux pages Web et

forums de discussion dont ils sont les concepteurs, les animateurs ou qu'ils hébergent volontairement pour le diffuser. Il est à noter que le juge a donné acte des engagements des fournisseurs d'accès d'effectuer une surveillance des services hébergés et d'adapter leurs contrats de diffusion de sorte à interdire la diffusion de messages contraires aux lois françaises.

Par une ordonnance de référé du TGI de Paris en date du 9 juin 1998 " *Estelle LEFEBURE C/ Valentin LACAMBRE et autres* " relative à une affaire concernant la violation du droit à l'image, le juge a considéré que pour pouvoir s'exonérer de sa responsabilité, le fournisseur d'hébergement devra justifier du respect des obligations mises à sa charge spécialement quant à l'information de l'hébergé sur l'obligation de respecter les droits de la personnalité, le droit des auteurs, des propriétaires de marques, de la réalité des vérifications qu'il aura opérées, au besoin par des sondages, et des diligences qu'il aura accomplies dès la révélation d'une atteinte au droit des tiers pour faire cesser cette atteinte ; le juge a également considéré que le fournisseur d'hébergement avait obligation de veiller à la bonne moralité de ceux qu'il héberge, au respect par ceux-ci des règles déontologiques régissant le Web et au respect par eux des lois, des règlements et des droits des tiers.

La plus importante affaire a donné lieu à ouverture d'une instruction pénale (*affaire World net/ France net*, 7 mai 1996) qui est toujours en cours. Il a été reproché à deux fournisseurs d'avoir hébergé des images à caractère pédophile et de les avoir mises à la disposition de leurs abonnés.

Depuis cette instruction, aucune information judiciaire n'a été ouverte à l'encontre de fournisseurs d'accès, ce qui relève soit des efforts de ces acteurs pour limiter les atteintes, soit de la politique pénale, le parquet disposant d'un pouvoir d'appréciation sur l'opportunité des poursuites.

Aucune décision n'a mis en œuvre le régime de la responsabilité en cascade.

Il ressort de cette analyse jurisprudentielle, notamment en matière de télématique, que la responsabilité éditoriale n'a pas servi à construire le schéma de responsabilité des nouveaux services télématiques, et que toute responsabilité doit être liée à la connaissance et au degré de contrôle effectif sur le contenu.

L'enseignement des exemples étrangers

Les travaux menés depuis 1996 par un certain nombre de pays se sont plus centrés sur la question de l'autorégulation et de ses techniques que sur celle de la responsabilité des acteurs. Ce sujet est, en effet, apparu comme complexe, nécessitant une compréhension globale du fonctionnement du réseau, peut-être aussi trop politique et de nature à jeter une ombre sur ce nouvel espace. Le traité de l'OMPI relatif au droit d'auteur de décembre 1996 n'aborde ainsi pas ce point et les premiers travaux canadiens se bornent à une analyse sectorielle de la responsabilité, incrimination par incrimination, sans approche globale et synthétique (rapport de juillet 1997).

L'OCDE, de même, au sein de laquelle la France avait lancé une initiative de coopération internationale sur les contenus en octobre 1996, a refusé d'inscrire ce point comme axe de travail en 1997.

Cependant, le rôle des intermédiaires techniques a fait l'objet, soit de recommandations, soit de réglementations, à la suite des premières affaires judiciaires concernant ces derniers et des pressions fortes des opérateurs de télécommunications. De même, certains des codes de conduite élaborés par les professionnels eux-mêmes s'attachent à définir la responsabilité des acteurs à l'égard du contenu. De ces diverses initiatives il semble se dégager un consensus, surtout en Europe, qui consacre le droit commun de la responsabilité, les notions de connaissance et de

capacité de contrôle.

La déclaration ministérielle rédigée à l'occasion de la *conférence européenne de Bonn en juillet 1997* affirme ainsi : " Les ministres soulignent que les règles relatives à la responsabilité pour le contenu devraient être fondées sur un ensemble de principes communs propre à assurer le respect des règles du jeu. En conséquence, les intermédiaires tels que les opérateurs de réseau et les fournisseurs d'accès ne devraient pas, en général, être responsables du contenu. Ce principe devrait être appliqué de telle façon que les intermédiaires tels que les opérateurs de réseau et les fournisseurs d'accès ne soient pas soumis à des règles qui ne sont pas raisonnables, qui sont disproportionnées ou discriminatoires. En aucun cas, il ne faudrait attendre des services hébergeant un contenu appartenant à des tiers qu'ils exercent un contrôle préalable sur le contenu qu'ils n'ont pas de raison de croire illégal. Il devrait être tenu dûment compte du fait pour de tels intermédiaires d'avoir ou non des moyens de connaître et une possibilité de contrôler le contenu, qui sont raisonnables. Les ministres estiment qu'il convient que les dispositions relatives à la responsabilité donnent effet au principe de la liberté d'expression, respectent l'intérêt public et privé et n'imposent pas de charges disproportionnées aux acteurs. "

L'approche est donc claire : favorable aux transporteurs, elle s'écarte de tout schéma automatique de responsabilité lui préférant une approche *a posteriori*, au cas par cas, en fonction de la connaissance et des moyens de contrôle sur le contenu. Elle souscrit de plus à une stricte logique économique.

L'Allemagne de même, dans la loi multimédia du 1er août 1997, dissipe les inquiétudes des différents acteurs en établissant clairement la responsabilité sur le contenu de l'offreur de services Internet : celui qui produit le contenu est responsable ; celui qui utilise des contenus étrangers est coresponsable si le contenu lui est connu et qu'il lui est techniquement possible de l'éliminer de son offre de services dans des conditions raisonnables ; l'offreur d'accès enfin, qui se borne à assurer le transit des contenus n'est pas responsable de ceux-ci.

En *Belgique*, la réflexion a été mené par le Conseil supérieur de l'audiovisuel de la communauté française : celui-ci a exprimé sa préférence, dans un avis du 28 mars 1997, pour une responsabilité de droit commun des différents intervenants de l'Internet plutôt que pour une responsabilité en cascade ; la responsabilité devrait être proportionnée au rôle concret joué par chacun d'entre eux ; à titre d'exemple, le Conseil considère que le fournisseur d'accès qui ne peut assurer aucun contrôle *a priori* sur les ressources de l'Internet ne saurait être inquiété du fait qu'il aurait omis d'exercer un tel contrôle.

En *Suède*, un projet de loi de mai 1997 dispose que les fournisseurs " d'électronic notice-boards " (babillards), s'ils sont prévenus de l'existence de messages justifiant des sanctions pénales, doivent agir pour empêcher toute dissipation ultérieure desdits messages.

En *Suisse*, enfin, le groupe de travail sur l'Internet aboutit à la conclusion que " lorsque le fournisseur d'accès dispose d'indices concrets fondés sur ses propres recherches ou sur celles de tiers permettant de présumer l'éventuel caractère illicite de contenus de réseaux déterminés, il procédera ou fera procéder immédiatement à des investigations afin de déterminer si un blocage s'impose. Lorsque le fournisseur d'accès apprend, de façon certaine, l'existence de contenus de réseaux illicites, notamment réprimés par le droit pénal, il prendra immédiatement les mesures raisonnablement exigibles et techniquement réalisables afin de bloquer l'accès à ces contenus de réseaux ".

Toutes ces initiatives convergent même si elles peuvent différer dans leurs modalités précises ; face à leur multiplication et au nom de la bonne réalisation du marché intérieur, la Commission européenne (DG XV) prépare une directive sur la responsabilité des acteurs ; la rédaction de ce

texte devrait être achevée en 1998.

Les *États-Unis* n'ont jusqu'à présent pas formulé de recommandations générales sur la responsabilité, se cantonnant surtout au domaine du droit d'auteur (après l'échec du Communication Decency Act, annulé par la Cour Suprême américaine en juin 1996). La jurisprudence cependant dégage quelques pistes malgré d'évidentes contradictions. Dans l'affaire Cubby, Inc v. Compuserve, il ainsi été jugé que Compuserve n'était pas responsable de propos diffamatoires prononcés dans un de ses forums dès lors que cette société n'avait pas connaissance et ne saurait avoir connaissance de ceux-ci et que l'on ne pouvait lui demander d'examiner chaque publication qu'elle transporte pour relever d'éventuelles diffamations. Dans une autre affaire en revanche (Statton Oakmont, Inc v. Prodigy), il a été jugé que le fournisseur d'accès était responsable de propos diffamatoires dans un forum dès lors qu'il exerçait un contrôle éditorial sur ceux-ci à l'aide de logiciels de filtrage et de personnels dédiés.

Au *Canada*, enfin, les premières décisions de jurisprudence et les travaux menés dans le cadre du groupe de travail sur le commerce électronique semblent plutôt privilégier le droit commun comme fondement de la responsabilité des acteurs.

La proposition en matière pénale

Face aux incertitudes du droit applicable et en accord avec les évolutions internationales, les fournisseurs d'accès français, dans le cadre de leurs travaux sur l'autorégulation, ont dégagé les règles minimales que doivent respecter leurs abonnés ; cette approche " contractuelle " s'est traduite par l'adoption en 1997 du code de conduite de l'AFA (association de fournisseurs d'accès) qui dispose :

– que les membres de l'AFA ne sont pas auteurs ou producteurs des contenus mis en ligne par des tiers ;

– qu'ils ne le sont également pas pour les pages personnelles de leurs abonnés, mais s'engagent à détecter les contenus éventuellement illégaux par des techniques de lignes d'appel, de surveillance des pages les plus consultées et de filtrage des mots suspects ;

– pour les forums, l'AFA considère que ses membres peuvent agir *a posteriori* et suspendre la diffusion de forums contraires à leurs conditions d'utilisation.

Certains utilisateurs comme l'association IRIS dénoncent cet interventionnisme, préjudiciable selon eux aux libertés publiques en confiant, même avec une base contractuelle, un pouvoir exorbitant aux fournisseurs d'accès ; ils ajoutent que si l'unanimité peut se faire concernant des images pédophiles, il est beaucoup plus difficile de se prononcer sur une atteinte éventuelle aux droits d'auteur et que dans ce cas, l'intervention du juge doit être privilégiée.

Il est donc temps de clarifier le schéma des responsabilités des acteurs.

Un consensus existe quant aux objectifs de ce schéma

Ce consensus est le suivant :

– le régime adopté doit être lisible et simple ;

– il doit offrir une sécurité juridique aux acteurs en déterminant clairement le champ de leurs responsabilités ; c'est une condition obligatoire pour le développement de l'Internet en France ;

– il doit répondre au principe d'équité en vertu duquel une personne ne doit être responsable que des choses qu'elle est en mesure de contrôler ;

– le régime doit être efficace en responsabilisant les acteurs afin de prévenir les infractions et en permettant de lutter effectivement contre les contenus illégaux ; il doit inciter à une logique vertueuse des comportements et non dissuader, de crainte de voir leur responsabilité engagée, tout contrôle des contenus par les acteurs ;

– le régime doit permettre à la France d'être compétitive au plan mondial et en cohérence avec les systèmes étrangers ;

– il doit enfin assurer la neutralité du support en évitant la dichotomie des régimes applicables pour la diffusion d'un même message sur des supports différents.

Les solutions déjà discutées

Tant la doctrine, dans l'attente de décisions judiciaires des juges du fond, que les pouvoirs publics ou les acteurs se sont intéressés à la question de la responsabilité des acteurs et ont formulé des propositions. Aucune ne semble à ce jour entièrement satisfaisante :

? *Déresponsabilisation des intermédiaires techniques*

Certaines propositions visent à prévoir explicitement l'exclusion de la responsabilité des fournisseurs d'accès considérés comme de simples intermédiaires techniques. Telle était l'inspiration des amendements (dits " Fillon ") introduits dans le projet de loi de réglementation des télécommunications en juillet 1996. Ceux-ci envisageaient d'introduire un article 43-2 à la loi du 30 septembre 1986 prévoyant l'exonération de la responsabilité pénale des fournisseurs d'accès – définis comme les personnes dont l'activité est d'offrir un service de connexion à un ou plusieurs services de communication audiovisuelle – pour les infractions résultant du contenu des messages diffusés par un service de communication audiovisuelle sauf " s'il est établi qu'ils ont, en connaissance de cause, personnellement commis l'infraction ou participé à sa commission ".

Cette disposition ne modifiait pas le droit positif puisqu'elle se limitait à dire expressément ce qui se déduisait de l'interprétation de plusieurs textes, la culpabilité des fournisseurs d'accès ne pouvant être établie qu'à partir de la preuve de leur participation à la commission de l'infraction.

Il apparaît cependant que ce type de mesure risque de déresponsabiliser les acteurs et de faciliter de ce fait la commission des infractions.

? *Adaptation de la responsabilité éditoriale en cascade*

Il a été suggéré d'adapter la liste des acteurs susceptibles d'entrer dans la chaîne de responsabilité en incluant les hébergeurs et les fournisseurs d'accès. Il était à cet égard avancé qu'à l'instar de l'article 42 de la loi du 29 juillet 1881 incluant les imprimeurs et les distributeurs, ces catégories d'acteurs ne contribuaient pas directement à la réalisation du contenu mais participaient à sa mise à disposition du public. Cette proposition présentait en outre l'avantage de faciliter les poursuites, les hébergeurs et les fournisseurs d'accès, localisés en France, étant plus facilement identifiables que les auteurs étrangers.

Une telle proposition ne saurait toutefois être admise : facilitant les poursuites sur le territoire national, elle induirait un inévitable risque de délocalisation et nuirait à la compétitivité et l'image de la France dans le monde ; en outre si la directive européenne en préparation privilégiait le régime de droit commun, une solution différente handicaperait lourdement notre pays pour le développement d'Internet ; enfin, une telle proposition, faisant peser sur les prestataires techniques une présomption de responsabilité, exigerait de leur part la mise en place de systèmes de contrôle n'entrant pas dans le champ de leur mission, impliquant d'importantes

charges financières et favorisant la mise en place d'une forme de censure privée.

? *Généralisation du droit commun en supprimant la responsabilité en cascade*

Certains auteurs préconisent, enfin, l'exclusion de la responsabilité en cascade lui préférant l'application du droit commun qui offre des solutions globales et évolutives.

L'application du régime de droit commun présente en effet l'avantage d'une plus grande simplicité. Tous les acteurs (auteur, fournisseur de service, hébergeur, fournisseur d'accès, transporteur) sont susceptibles d'être poursuivis comme auteurs principaux, coauteurs ou complices dès lors qu'ils ont sciemment mis à disposition du public des contenus illicites. Ils sont ainsi exposés aux même sanctions. La détermination de la responsabilité repose ainsi sur l'examen des moyens ou des possibilités d'intervention techniques à la disposition de l'opérateur (mise en œuvre d'un contrôle), la connaissance de l'infraction et la mise en œuvre de moyens propres à faire cesser la diffusion de messages litigieux. Il est avancé au surplus que le régime de la responsabilité en cascade est lié à une logique éditoriale qui ne prévaut pas sur Internet.

Toutefois, de par la nature même des infractions visées (diffamation, incitation à la haine raciale...), cette responsabilité n'est susceptible d'être mise en jeu que pour les services offrant un contenu rédactionnel touchant à la liberté d'opinion. Il convient en effet de rappeler que le domaine d'application de la responsabilité éditoriale est par nature limité à certaines infractions qui sont peu susceptibles d'être commises sur des sites ayant une vocation purement commerciale. L'absence de contenu rédactionnel dans la plupart des services offerts sur Internet n'est par conséquent pas à même de justifier la suppression du régime de la responsabilité éditoriale sur ce support.

De plus, cette solution conduirait à ce que deux régimes de responsabilité distincts en fonction du support puissent être mis en œuvre pour un contenu identique : imaginons une publication de presse comportant une diffamation ; la société éditrice met en ligne le message diffamatoire ; le directeur de la publication de presse papier serait dans cette hypothèse pénalement responsable du contenu de la publication de presse alors que pour le service en ligne, cette responsabilité pèserait sur le journaliste en tant qu'auteur.

La proposition

Cette proposition apparaît plus comme une clarification des règles existantes que comme une modification substantielle de celles-ci.

L'objectif serait de **maintenir la responsabilité éditoriale pour ce qui la concerne, c'est-à-dire la fonction d'édition de contenus, mais de retenir un régime de responsabilité de droit commun pour toutes les autres fonctions exercées sur le réseau** et notamment les fonctions d'intermédiation technique ou d'ensemblier.

Concrètement, un fournisseur d'accès ne serait donc *a priori* responsable que de ses propres contenus, édités par lui-même, mais non de ceux auxquels il donne accès ou qu'il héberge ; il ne serait ainsi ni le directeur de la publication des pages personnelles de ses abonnés, ni responsable des propos émis dans les forums.

De même, les liens hypertexte ne le rendraient pas responsable de l'ensemble des contenus auxquels ils renvoient.

De même, les reproductions temporaires de type " cache " ne devrait pas le rendre responsable du contenu de celles-ci.

La seule difficulté de cette solution est qu'elle impose de définir, ce qui n'a jamais été fait, l'édition de contenus ; une définition peut être proposée : il s'agit de la création et de la production d'un message mis à disposition du public.

Il conviendrait d'introduire cette définition dans la loi du 29 juillet de 1982 en introduisant un dernier alinéa à l'article 93-3 ainsi rédigé : " Ne sont tenus pour responsables sur le fondement des alinéas précédents que les personnes qui créent ou produisent un contenu mis à disposition du public. "

En revanche, une responsabilité de droit commun devrait s'appliquer pour les prestations autres qu'éditoriales, rendant possible la poursuite des fournisseurs d'accès sur le terrain de la complicité.

Il conviendra alors de préciser les conditions d'engagement de celle-ci : le principe de connaissance est à cet égard essentiel, établissant l'intention délictueuse ; la capacité de contrôle et les mesures prises par le fournisseur en cas de contenus litigieux le sont également. En réalité, comme le suggère le professeur Vivant, il convient d'analyser le triptyque " Savoir/ Pouvoir/ Inertie " : l'intéressé savait-il ou aurait-il dû savoir ? Avait-il les moyens d'empêcher ? N'a-t-il rien fait pour limiter l'atteinte ?

On pourrait dès lors, en s'inspirant du régime de responsabilité des élus pour faits d'imprudence ou de négligence, prévu par la loi du 13 mai 1996, considérer que, pour les services mentionnés au 1er de l'article 43 , les personnes qui ne créent ni ne produisent des contenus mis à disposition du public peuvent être tenues responsables sur le fondement de l'article 121-7 du code pénal si elles ont agi en connaissance de cause et si elles n'ont pas accompli " les diligences normales " pour faire cesser l'infraction.

L'organisme de corégulation dont il est envisagé la création (voir *infra*) doit aider à la détermination de ces diligences normales, exigibles de chacun des acteurs professionnels ou personnes privées.

Enfin, dans l'hypothèse où serait envisagé un régime spécifique pour les opérateurs de service en ligne (voir *infra* cinquième partie), ces dispositions auraient vocation à y être incluses.

La responsabilité civile

Parallèlement aux règles de responsabilité pénale, les acteurs de l'Internet demeurent soumis à la responsabilité civile sur le fondement de l'article 1382 du code civil en matière délictuelle et sur le fondement des articles 1137 et 1147 du code civil en matière contractuelle.

Transporteur ou opérateur de télécommunications

L'opérateur est défini par l'article 1er de la loi du 26 juillet 1996 comme " toute personne physique ou morale exploitant un réseau de télécommunications ouvert au public et fournissant au public un service de télécommunications ".

Sa responsabilité contractuelle ne pourra être engagée qu'en cas de non-respect ou de défaillance dans la fourniture des moyens de transport et non à raison du contenu de l'information véhiculée. En effet, le principe de neutralité posé par l'article L. 32-11, 5e alinéa, du code des postes et télécommunications, dans sa rédaction issue de la loi du 26 juillet 1996, limite les possibilités de mise en cause de la responsabilité des opérateurs à raison du contenu informationnel qu'ils véhiculent.

Fournisseur d'hébergement

Il gère techniquement des ressources informatiques connectées à l'Internet et met ses ressources à disposition de l'abonné. Il accueille des sites d'éditeurs de contenu avec lesquels il est contractuellement lié, " duplique " des sites extérieurs, met en œuvre des serveurs " proxy " et des serveurs de " news ".

La doctrine dominante tend à exclure la responsabilité des contenus informationnels qu'ils n'ont pas conçus et qu'ils se limitent à héberger. Ceci est raisonnable et en cohérence avec les principes dégagés plus haut sur la responsabilité pénale. Il doit peser toutefois sur le fournisseur d'hébergement un devoir de vigilance sur les contenus qu'il lui est proposé de mettre en ligne, ce que la plupart des professionnels ne contestent pas.

Il appartiendra à la jurisprudence, compte tenu de ces indications, de dégager les standards d'un comportement " raisonnable " attendu du professionnel.

Le fournisseur d'hébergement engage en outre sa responsabilité contractuelle en cas d'inexécution ou de défaillance dans sa prestation technique d'hébergement.

Fournisseur d'accès

Sa fonction essentielle est celle d'un prestataire de services de nature technique, chargé de mettre en relation ses abonnés avec les sites ou les autres utilisateurs. Le fournisseur d'accès peut cependant, dans certains cas, avoir un rôle d'éditeur de contenus (AOL par exemple).

Une distinction est à opérer selon la fonction exercée : en cas d'activité exclusivement technique, la responsabilité civile ne devrait pas être engagée sauf en cas de connaissance ou de possibilité de maîtrise de l'information mise en cause ; par ailleurs, l'absence de fourniture à l'abonné de dispositif de contrôle technique prévu à l'article 43-1 de la loi du 30 septembre 1986 peut constituer une faute civile ; enfin, la responsabilité civile des fournisseurs d'accès peut être limitée, dans les contrats d'abonnement, par des clauses limitatives ou exonératoires de responsabilité. La plupart des contrats d'abonnement proposés aujourd'hui stipulent que le fournisseur d'actes n'est pas responsable des contenus accessibles par son intermédiaire et n'exerce aucun contrôle sur ceux-ci.

Fournisseur de services

Cet acteur du réseau peut, selon le cas, être éditeur de contenus, propriétaire du serveur ou fournisseur d'accès.

En qualité de professionnel, sa responsabilité contractuelle ou délictuelle peut être engagée pour les informations fausses ou répréhensibles qu'il diffuse. Compte tenu de la jurisprudence dégagée sur les agences de renseignement, il est tenu de vérifier ces informations.

Éditeur de contenus

Sa responsabilité civile est engagée en cas de contenus illicites de nature à porter tort à un tiers.

L'utilisateur

L'internaute est à la fois consommateur et diffuseur d'informations. Il est tenu de respecter les droits d'autrui (droit de propriété intellectuelle, respect de la vie privée) ainsi que le libre accès aux informations des personnes qui sont sous sa garde, sauf à voir sa responsabilité civile mise en jeu.

En tant qu'auteur de contenus informationnels (forums, courrier électronique, pages personnelles...), il assume envers les tiers la responsabilité civile des informations qu'il diffuse.

L'appréciation de la faute civile du consommateur sera cependant appréciée moins sévèrement par les tribunaux que celle des professionnels de l'information. Dans une affaire récente (Trib. Com. du Mans 16 février 1998), un utilisateur a cependant été condamné à 6 mois d'emprisonnement dont 3 avec sursis pour recel d'objet provenant de la diffusion d'images d'un mineur à caractère pornographique et abus de confiance ; le juge a considéré que le prévenu avait par ses paiements contribué à l'entretien de réseaux pédophiles alors que son instruction et son niveau de responsabilité auraient dû lui permettre de prendre conscience du caractère répréhensible des scènes téléchargées sur l'ordinateur qu'il détournait de son usage professionnel, en sa qualité de directeur de cabinet du président du Conseil général.

Enfin, lorsqu'il intervient dans un cadre contractuel, l'internaute peut engager sa responsabilité s'il méconnaît les conditions du contrat.

Faciliter l'action de la police et de la justice

Internet et les réseaux apparaissent souvent comme des espaces dans lesquels il est difficile de veiller à l'application des règles de droit. La dimension internationale, l'absence de point de contrôle central du réseau, les techniques d'acheminement des messages par paquets, les facultés d'anonymat,... en un mot, les spécificités d'Internet rendraient illusoire, selon certains, toute tentative d'identification ou de poursuite de l'auteur de faits délictueux. La police et la justice seraient donc désarmées.

Une telle analyse n'est pas exacte : il ne faut pas négliger tout d'abord, les faits délictueux commis sur le territoire national, sans implication extra-territoriale, pour lesquels les services enquêteurs peuvent agir sans difficulté majeure ; par ailleurs, l'anonymat qui protégerait l'auteur de messages illicites est très relatif ; en réalité, comme on a pu le voir dans la première partie de ce rapport, il n'y a pas de réel anonymat sur le réseau et les " traces " laissées par les utilisateurs au cours de leur navigation permettent souvent de remonter à la source de l'infraction ; enfin, et peut-être surtout, la dimension internationale du réseau ne saurait constituer un obstacle dirimant, interdisant les enquêtes et les poursuites, sauf à accepter la création de " paradis virtuels ", constitutifs de dangers pour l'ordre public international ; un tel constat est apparu clairement aux États du G7/P8 en décembre 1997 lors du sommet de Washington et les a conduit à adopter dix principes et un plan d'action pour lutter contre la criminalité de haute technologie.

Il apparaît néanmoins nécessaire de renforcer les moyens d'action de police et de la justice, au plan national et international, afin d'améliorer l'efficacité de leur action sur les réseaux.

Renforcer l'identification des acteurs

Si l'anonymat est une illusion sur les réseaux, il est souvent difficile de déceler l'identité réelle de la personne physique ayant commis l'infraction ; il paraît donc essentiel d'améliorer la " traçabilité " des messages et l'identification des acteurs afin de pouvoir engager une action en responsabilité. À ce titre, le fournisseur d'accès apparaît comme un maillon-clé dans la chaîne de transmission de l'information.

Diverses solutions peuvent être proposées :

– **obligation pour tout service de communication au public de faire figurer sur son site l'identification de l'éditeur de contenu et ses coordonnées** : cette disposition existe déjà pour les services télématiques de l'article 43 de la loi du 30 septembre 1986 et est sanctionnée pénalement à l'article 76-2 de la même loi (amende 10 000 à 40 000 francs). Cette mesure est de nature à offrir une plus grande transparence des services offerts au public et à faciliter l'identification de la personne pénalement responsable. Elle devrait concerner tous les sites, professionnels ou individuels dès lors qu'ils mettent de l'information à disposition du public.

Elle pourrait être sanctionnée par une contravention de la quatrième classe (amende de 5000 francs), ce qui nécessiterait une modification des peines actuellement prévues pour les services de l'art. 43 ;

– **identification des abonnés** : la connaissance des abonnés est essentielle pour faciliter l'action de la police en cas d'infraction. Chaque fournisseur d'accès devrait être en mesure de fournir l'identité de ses clients, dans le cadre d'une enquête, aux services de police et de justice . Ceci devrait le conduire à demander l'identité de ses clients lors d'une demande d'abonnement, ce que certains pratiquent déjà. Pour s'assurer de la véracité des éléments fournis, il conviendra de prévoir un délit de fausse déclaration, infraction exposant le contrevenant aux même sanctions que celles prévues par l'article 781 du code de procédure pénale, cet article incriminant la fourniture de renseignements d'identité imaginaires susceptibles de provoquer des mentions erronées au casier judiciaire. L'infraction pourrait être sanctionnée par une contravention de la quatrième classe. Il conviendra de rappeler, dans les contrats d'abonnement, que toute fausse déclaration constitue une infraction pénale. De telles dispositions ne remettent pas en cause l'anonymat qui restera possible pour la messagerie électronique vis-à-vis des tiers grâce à la technique des pseudonymes. Une difficulté doit être évoquée : celle des abonnements gratuits, souvent anonymes, qui facilitent la commission d'infractions en l'absence de toute localisation de l'utilisateur ; il parait difficile de les interdire, ce que peuvent cependant souhaiter les fournisseurs d'accès, dès lors que cette pratique commerciale est coûteuse ; l'obligation de fournir l'identité des abonnés à la police en cas d'enquêtes devrait cependant inciter les fournisseurs à pratiquer certaines vérifications pour l'ouverture complète d'un abonnement (envoi d'une lettre de confirmation, paiement par chèque) ;

– **suppression de la déclaration obligatoire auprès du procureur de la République** : il ne paraît pas souhaitable de maintenir l'obligation de déclaration prévue à l'article 43 de la loi du 30 septembre 1986. La plupart des observateurs constatent que cette formalité est peu respectée, la majorité des acteurs de l'Internet méconnaissant cette obligation ; elle semble surtout peu adaptée à des éditeurs individuels en nombre potentiellement important ; enfin, les renseignements qu'elle contient sont stockés mais sont peu exploités par les autorités dépositaires ;

– **conservation des données de connexion par les fournisseurs d'accès** : les données de connexion que le fournisseur d'accès collecte aujourd'hui automatiquement lorsqu'il met un utilisateur en contact avec le réseau ont une grande valeur informationnelle pour les services d'enquête ; figurent ainsi le " login " utilisé, les heures de début et de fin de la connexion, le numéro IP de l'appelant et les sites visités. Ces données sont stockées par les fournisseurs d'accès pendant des périodes très variables, selon l'importance des flux de clients qu'ils ont à gérer. L'important est que ces données ne soient pas détruites trop vite afin de faciliter les poursuites et l'établissement de la preuve des infractions. Dans le cas des universités par exemple, considérées par la police comme les cibles ou les lieux " rebond " privilégiés pour la commission d'infractions, les données de connexion ne sont gardées que deux jours.

Le délai de prescription légale des délits est de trois ans ; la durée de conservation des données relatives aux appels téléphoniques par France Télécom est de un an ; la CNIL recommande un délai maximal d'un an ; cette durée de conservation semble raisonnable mais devra être expertisée. Le non-respect de cette obligation de conservation des données pourrait être sanctionné par une contravention de la cinquième classe.

Il paraît irréaliste d'étendre cette mesure aux messages électroniques qui sont régulièrement effacés par les serveurs, compte tenu de leur nombre ; pour les forums de discussion, des moteurs de recherche comme " Déjà news " conservent pendant plusieurs années les messages émis.

Augmenter les pouvoirs et les compétences du juge

Le dispositif textuel est, on l'a dit, globalement suffisant pour sanctionner les contenus et pratiques litigieuses sur Internet et les réseaux. Il peut cependant être complété sur quelques points afin d'accroître l'efficacité du dispositif répressif.

Établissement de nouvelles peines

? *Compléter la loi du 5 janvier 1988 sur la protection des systèmes informatiques*

La loi du 5 janvier 1988, dite loi Godfrain, a introduit un certain nombre de dispositions pénales destinées à protéger les systèmes informatiques ; les articles L. 323 et suivants du code pénal sanctionnent ainsi :

– le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données ;

– le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données ;

– le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient.

La loi Godfrain, intervenue très tôt, est un modèle d'innovation juridique et est couramment appliquée pour lutter contre les formes classiques ou nouvelles de criminalité informatique (lutte contre les virus, les bombes logiques...) ; elle permet sans nul doute de sanctionner les " chevaux de Troie ", logiciels espions ayant pour but de surveiller un site, un système informatique ; en revanche, son applicabilité à des logiciels de contrôle des réseaux communément utilisés par les administrateurs (Satan, TCP Dump...) mais aussi dévoyés par les pirates est plus douteuse, dès lors que ces dispositifs sont situés en dehors du système informatique attaqué. En outre, elle n'incrimine les producteurs de logiciels ayant facilité la commission de telles infractions de piratage (comme les logiciels de génération de numéros de cartes bancaires) qu'au titre de la complicité par fourniture de moyens.

Afin de renforcer ces mécanismes, il peut être envisagé, à l'instar du droit suisse (article 144 du code pénal), de créer une infraction visant à condamner la fabrication, la mise à disposition ou l'importation de logiciels qui sont destinés à être utilisés dans le but de commettre des infractions.

? *Le " spamming "*

Le " spamming " consiste à envoyer des messages de façon continue et non sollicitée à un utilisateur, soit pour des raisons commerciales (publicité) soit dans l'intention de nuire ; une boîte aux lettres peut être ainsi inondée de prospectus, l'accès à un système informatique bloqué par un logiciel qui lui envoie 10 000 " gros mots " à la minute. Le débat est intense aux États-Unis et les tentatives se multiplient pour limiter ces pratiques ; un projet de loi, introduit par le sénateur Mc Cain (Arizona) et approuvé par le Sénat le 12 mai 1998, vise d'une part à obliger les publicitaires à s'identifier, d'autre part à informer les consommateurs qu'ils peuvent, sans frais, demander à ne plus recevoir de tels messages publicitaires.

En France, le " spamming " à vocation commerciale n'est pas incriminable en tant que tel et il appartient surtout aux acteurs privés d'en fixer les limites par des procédés d'autorégulation ; par ailleurs, la qualification de démarchage pourrait être retenue dans ce cas (voir *supra* deuxième partie). Le " spamming " dans l'intention de nuire, quant lui, doit pouvoir être sanctionné, soit

par la loi Godfrain (article 323-2 du code pénal relatif à l'atteinte volontaire au fonctionnement du système), soit, éventuellement, en élargissant l'application de l'article 222-16 du code pénal qui sanctionne les " appels téléphoniques malveillants " à d'autres types d'envois effectués dans l'intention de nuire.

? *Peines complémentaires*

Pour renforcer la répression des infractions, il pourrait être envisagé d'interdire à un responsable de site illégal d'exercer certaines fonctions ; à ce titre, l'article 131-6-11° du code pénal qui permet au tribunal d'infliger à tout prévenu majeur la peine d'interdiction d'exercer une activité professionnelle ou sociale pendant 5 ans au plus, est adaptée bien que les conditions fixées à son application paraissent restrictives : il n'existe pas toujours, en effet, un lien entre l'infraction commise et l'activité professionnelle du prévenu qui est souvent un particulier ; le prévenu n'a pas toujours utilisé ses facilités professionnelles pour commettre l'infraction ; enfin, le législateur a exclu du champ de cet article les délits de presse.

En réalité, il serait opportun de prévoir des interdictions plus larges que l'interdiction professionnelle, telles que l'interdiction d'émettre des messages de communication au public et de réserver ces peines aux infractions les plus graves comme celles des articles suivants du code pénal : l'article 227-23, 227-24 (protection des mineurs) ou 227-18 (provocation à l'usage de stupéfiants).

? *Circonstances aggravantes*

L'établissement de circonstances aggravantes liées à l'utilisation de services de communication au public pour la commission de certaines infractions n'apparaît pas souhaitable. Cette solution a été retenue par la loi du 17 juin 1998 relative à la prévention et à la répression des atteintes sexuelles commises contre les mineurs. Ayant constaté que l'essor des réseaux informatiques (minitel, Internet) permettait à certains individus de commettre plus facilement des infractions à connotation sexuelle, notamment contre les mineurs, le texte prévoit d'ériger l'utilisation d'un moyen de télécommunication pour la diffusion de messages à destination d'un public non déterminé en circonstance aggravante du proxénétisme, de la corruption de mineur, du délit de diffusion d'images de mineurs présentant un caractère pornographique et, enfin, de l'atteinte sexuelle sur mineur sans violence.

Une telle approche ne saurait se généraliser ; en effet cette disposition, de par le caractère large des termes utilisés, est de nature à jeter le discrédit sur Internet en assimilant le réseau à l'utilisation d'une arme alors même qu'il constitue un espace neutre dans lequel toute forme d'activité humaine, positive ou négative, peut se développer. En outre, la dissociation des principes de répression en fonction du mode de commission technique du fait délictueux principal n'apparaît pas souhaitable.

? *Publicité des décisions*

Afin de rendre les sanctions sur Internet plus effectives, il peut être envisagé une publicité des jugements sur le réseau.

En matière civile, le juge peut ainsi ordonner la publicité de la décision à titre de réparation. On notera à cet égard que dans une décision en date du 3 mars 1997, " *Sté ordinateur Express c/ Sté ASI* ", le tribunal de commerce de Paris est allé au-delà de la mise en œuvre classique de ce type de condamnation en matière de droit d'auteur en réclamant la création d'un lien hypertexte avec un organisme de protection des auteurs (APP).

En matière répressive, seul un nombre limité de dispositions pénales prévoient que le juge puisse

prononcer à titre complémentaire la publication de la condamnation. En application de l'article 131-35 du code pénal, la diffusion de la décision peut notamment être exercée par un ou plusieurs services de communication audiovisuelle.

Il apparaît souhaitable d'étendre le champ d'application de ces dispositions, à la fois à de nouveaux supports mais aussi à de nouvelles infractions. Il pourrait ainsi être ajouté que si l'infraction a été commise sur un support de communication au public, le juge peut prononcer à titre complémentaire la diffusion de la décision sur ce même support ; par ailleurs, cette publicité devrait être possible pour d'autres infractions que celles aujourd'hui prévues et notamment la mise en péril de mineurs.

Possibilité de mettre fin à l'infraction

La vitesse de circulation et la fugacité des données qui caractérisent les réseaux rendent nécessaire de faire cesser rapidement l'infraction, de couper l'accès au site illégal ou d'interdire son hébergement.

L'exemple du parquet de Munich en 1995, imposant à la filiale allemande de la société Compuserve, de bloquer la consultation en Allemagne de 200 sites pédophiles et zoophiles, pose la question de la capacité juridique du juge de décider de telles mesures.

Aujourd'hui, seul le juge des référés agissant en matière civile peut prendre une telle décision en application de l'article 809 du nouveau code de procédure civile (mesures nécessaires pour prévenir un dommage imminent ou faire cesser un trouble manifestement illicite) ; cette procédure est bien adaptée au monde des réseaux et offre souplesse et célérité à l'action du juge ; d'ailleurs, la plupart des affaire jugées l'ont été en matière civile et selon la procédure du référé.

Cependant, l'action civile est subordonnée à celle d'un intérêt individuel lésé, d'une personne pouvant arguer d'un préjudice direct que lui cause l'infraction, ce qui n'est pas toujours le cas. Certaines infractions ne comportent, en effet, pas de victime et empêchent de ce fait le recours à la procédure de référé pour faire cesser l'infraction.

Deux voies sont dès lors envisageables : soit élargir les possibilités d'actions en référé et donner au parquet la possibilité de prononcer des mesures conservatoires permettant de couper l'accès au site ; cette solution serait contraire aux principes du droit processuel français et susciterait de vives controverses dans le cas de messages mettant en cause la liberté d'expression ; soit permettre au juge d'instruction d'ordonner une mesure de sûreté interdisant à titre provisoire l'accès ou l'hébergement d'un site litigieux.

Cette deuxième solution nécessite l'insertion d'une disposition spécifique dans le code de procédure pénale dès lors que les pouvoirs que le juge d'instruction tient de l'article 81 du code de procédure pénale de procéder à tout acte utile à la manifestation de la vérité et la faculté de requérir par commission rogatoire tout officier de police judiciaire de procéder aux actes d'information qu'il estime nécessaire par application de l'article 151 dudit code, n'emporte pas un tel pouvoir ; les dispositions relatives au contrôle judiciaire, de même, ne l'autoriseraient pas à couper l'accès ou l'hébergement à un site.

Il faut noter qu'un tel dispositif a déjà été mis en place de façon ponctuelle pour certaines infractions : en matière de publicité mensongère (article L 121-3 du code de la consommation) où le juge peut interdire la diffusion du contenu , en matière de proxénétisme (art. 706-36 du code de procédure pénale) où le juge peut prononcer la fermeture, à titre provisoire et pour trois mois renouvelables, du lieu de prostitution.

Une telle hypothèse nécessite cependant qu'un juge d'instruction soit saisi et qu'une instruction

soit ouverte, alors même que la seule décision du juge pourra être limitée à cette décision d'interdiction d'accès ou d'hébergement ; il peut dès lors être également prévu de confier ces nouveaux pouvoirs au président du tribunal de grande instance, s'inspirant de ceux qu'il détient déjà en matière de perquisitions liées aux stupéfiants ou au travail clandestin.

De tels pouvoirs devraient être étendus aux juge du fond qui prononceraient donc, à titre de peines accessoires, l'interdiction d'hébergement ou d'accès.

La violation de l'interdiction prononcée par le juge serait sanctionnée pénalement ; bien que ne liant que la personne contre qui elle est prononcée, une telle décision pourrait conduire à poursuivre, sur le fondement de la complicité, les fournisseurs d'accès et d'hébergement qui la méconnaîtraient.

Il serait en outre envisageable que, dans le cas d'une interdiction d'accès en France d'un site hébergé à l'étranger, le juge puisse demander à cet hébergeur, partie à l'instance, d'interdire que des utilisateurs français se connectent sur le site (à partir notamment de l'identification territoriale du nommage " .fr "). Ceci faciliterait grandement l'exequatur des jugements mais nécessite une convention internationale.

Il reste que l'efficacité de ces mesures est probablement, dans un espace mondial, plus symbolique que réelle : les possibilités de contournement existent et un éditeur de contenus illicites peut toujours se faire héberger dans un pays plus " tolérant ".

Une option écartée : remettre en cause l'architecture de la loi de 1881

Les difficultés liées notamment à la courte prescription de l'action publique prévue pour les infractions de presse par la loi du 29 juillet 1881 ont amené certains auteurs à suggérer l'établissement d'une distinction entre les infractions de presse d'ordre privé, telles que la diffamation et l'injure, qui continueraient de relever des régimes de prescription de courte durée, et les infractions dites d'" ordre public ", comme le révisionnisme ou l'incitation à la haine raciale, qui bénéficieraient du régime procédural de droit commun. En effet, si toutes les infractions portent atteinte à l'ordre public, il apparaît souhaitable de tenir compte de leur gravité.

Le projet de loi relatif à la lutte contre le racisme établi en 1996 prévoyait d'ailleurs de faire sortir le délit d'injure et de diffamation raciale de la loi de 1881 pour le soumettre au droit commun et notamment, au régime de prescription de droit commun de trois ans prévu en matière de délits.

Une telle approche qui risque de remettre en cause l'équilibre de la loi de 1881 par un biais un peu secondaire ne doit pas être retenue. La vraie interrogation est celle de l'applicabilité de ce texte au monde des réseaux alors même qu'il a été conçu pour un environnement différent.

De plus, les infractions pénales les plus graves touchant à la liberté de communication et ayant en particulier trait à la protection des mineurs renvoient au système de responsabilité éditoriale mais ne relèvent pas du régime de procédure spécifique de la loi de 1881.

Adapter la procédure à la fugacité des réseaux

La prescription

L'article 65 de la loi de 1881 prévoit une prescription abrégée de trois mois pour les délits de presse. Les infractions de presse sont ainsi considérées par la jurisprudence comme des infractions instantanées, le délai de prescription commençant à courir à compter du premier fait ou acte de publication, quelle que soit la périodicité de la publication ou sa durée de mise en

circulation.

L'application de ce court délai aux infractions de presse commises sur Internet, telles que la diffamation, n'est pas sans soulever certaines difficultés. Il s'avère en effet particulièrement délicat d'apporter la preuve de la date de première mise à disposition du public, et de déterminer ainsi à compter de quel moment la prescription commence à courir alors même que le document continue à être diffusé en ligne.

Appliquant la jurisprudence classique, le TGI de Paris, par une ordonnance en référé du 30 avril 1997 (Esig et Roger Berthault / Groupe Express), a constaté la prescription de l'action en diffamation contre une information diffusée sur Internet, dès lors que celle-ci avait pour point de départ " non le jour où les faits ont été constatés mais le jour du premier acte de publication ".

Si cette position devait être généralisée, la condamnation d'individus coupables de faits litigieux sur Internet et les réseaux, pouvant facilement invoquer la courte prescription, serait réellement difficile.

Dès lors, que faire ? La première parade pourrait être une évolution de la jurisprudence qui admettrait que chaque nouvelle modification du site fait à nouveau courir le délai de prescription comme dans le cas d'éditions successives d'un livre (Crim. 8 janvier 1991) ; cependant, ceci ne fait que rallonger le délai sans régler les questions de preuve.

La deuxième solution est de faire des infractions commises sur Internet des infractions " continues " qui durent tant que le message illégal est accessible. Cette solution a l'inconvénient de traiter de façon différente un même message illégal selon le support de circulation. Elle peut être mise en œuvre soit par une évolution de la jurisprudence qui admettrait que l'infraction est continue et se perpétue pendant toute la période où le message est lisible par l'utilisateur, soit en créant un régime spécifique de prescription pour les réseaux précisant que lorsqu'une infraction est commise sur ceux-ci, le délai prévu à l'article 65 de la loi de 1881 ne s'applique pas.

Les modalités de constatation des infractions

Le principe de liberté de la preuve (article 427 du code de procédure pénale) autorise le juge pénal à se fonder sur tous éléments de preuve (procès, verbal, témoignage...). Le juge décide d'après son intime conviction.

En revanche, la recherche et l'administration des preuves doivent obéir à un régime légal. En application des articles 14 et 15 du code de procédure pénale, la police judiciaire est chargée de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs tant qu'une information n'est pas ouverte.

Certaines preuves disposent ainsi d'une valeur probante plus importante que les simples témoignages. Les procès-verbaux ont à cet égard une valeur particulière parce qu'ils ne peuvent être effectués que par des officiers de police judiciaire, par des agents assermentés ou spécialement habilités par des dispositions spécifiques.

Il convient de citer à titre d'exemple que les agents agréés par le ministre de la Culture sont habilités à constater les infractions de contrefaçon, leurs constats ayant été la source de la plupart des actions engagées à ce jour en matière de propriété intellectuelle (voir *supra* troisième partie).

De façon plus générale, certains agents (douanes, répression des fraudes...), disposent de pouvoirs de police judiciaire, leur action étant limitée et entourée de conditions rigoureuses.

Face à la dispersion et à la multiplication des infractions concernant les réseaux, certains suggèrent d'investir d'autres personnes d'une mission de police judiciaire. Cette proposition ne

mérite pas d'être retenue : comment en effet justifier d'investir des personnels d'une compétence plus large pour les réseaux que celle qui leur a été reconnue pour le monde réel ? Comment s'assurer de l'homogénéité des constats si ceux-ci se multipliaient à travers des autorités trop diverses ? Il paraît plus opportun de développer les moyens de la police et de la gendarmerie afin d'élargir leurs moyens d'investigation.

Compétence et spécialisation des tribunaux

Trois critères permettent de fixer la compétence d'un tribunal :

– le lieu de commission de l'infraction ;

– le lieu du domicile d'une des personnes soupçonnées d'avoir participé à l'infraction ;

– le lieu d'arrestation d'une de ces personnes.

Au regard de la nature des infractions susceptibles d'être commises sur Internet, on peut considérer que les infractions seront commises sur l'ensemble du territoire français et que plusieurs juridictions sont en conséquence susceptibles d'être compétentes. L'engagement d'actions publiques par différents parquets est donc possible.

Certains en concluent qu'il faut réserver le traitement de ce type de contentieux à une juridiction particulière (TGI de Paris).

Une telle option, retenue pour les infractions terroristes concentrées sur Paris, ne semble pas opportune du fait de la dispersion potentielle des infractions liées à l'Internet, et il paraît plus sage de laisser jouer les règles de compétence de droit commun, d'autant qu'une souplesse est d'ores et déjà possible : en effet, au stade de l'enquête, les parquets peuvent se transmettre la procédure ; par ailleurs, la procédure dite de " règlement de juges " prévue à l'article 657 du code de procédure pénale prévoit que lorsque deux juges d'instruction se trouvent simultanément saisis de la même infraction, le ministère public peut requérir l'un des juges de se dessaisir au profit de l'autre.

En pratique, aujourd'hui, la plupart des affaires pourra ressortir de la compétence du parquet de Paris. En conséquence, des instructions pourraient être fixées par voie de circulaire incitant les parquets à se dessaisir au profit de la juridiction parisienne si l'infraction est commise à Paris.

En outre, face à la spécificité technique du réseau et à la méconnaissance qu'en ont beaucoup de magistrats, il a été suggéré de créer un corps de magistrats spécialisés dans le traitement ou le jugement des dossiers d'information judiciaire pour juger des crimes et délits commis sur Internet.

Or, comme on l'a dit plus haut, les faits perpétrés sur les réseaux ne sont pas d'une spécificité telle qu'elle justifierait un juge spécifique (juge de l'Internet) ; de plus, toute spécialisation conduirait à une assimilation avec une juridiction d'exception et risquerait d'être mal interprétée.

Si une compétence spécialisée doit être écartée, il paraît en revanche souhaitable de favoriser une meilleure formation de l'ensemble des magistrats, civilistes ou pénalistes, grâce à *l'élaboration de circulaires et à la mise en place d'une politique de formation continue* permettant aux juges d'appréhender les caractéristiques techniques et fonctionnelles du réseau.

Une circulaire pourrait en particulier avoir pour objet de définir les principales caractéristiques d'Internet et des réseaux à travers une description pratique de ceux-ci, de leur fonctionnement, de l'organisation des relations entre les différents acteurs et de la nature du contenu informationnel qui y circule. Ce texte pourrait en outre rappeler le dispositif législatif existant, les dispositions

pénales et la procédure applicable.

Créer une cellule interministérielle pour la criminalité de haute technologie

L'effort des diverses administrations concernant la criminalité liée aux nouvelles technologies est déjà important.

Le ministère de l'Intérieur a ainsi crée, en octobre 1994, deux unités spécialisées : le Service d'enquêtes sur les fraudes aux technologies de l'information (SEFTI) et la Brigade centrale de répression de la criminalité informatique (BCRCI). Le SEFTI, rattaché à la direction de la Police judiciaire de la préfecture de police de Paris, est constitué de vingt fonctionnaires ; la BCRCI, rattachée à la direction centrale de la Police judiciaire, a une compétence nationale et est composée de dix officiers de police. Ces deux services sont chargés de procéder à des enquêtes lorsque les systèmes de traitements automatisés d'informations font l'objet de malveillances ou sont utilisés pour commettre d'autres infractions.

Par ailleurs, la direction de la surveillance du territoire (DST) dispose d'une unité spécialisée pour diligenter les enquêtes et mène également une action de sensibilisation auprès des entreprises en matière de sécurité informatique.

Enfin, depuis septembre 1997, la direction générale de la Police nationale a mis en place une cellule de veille sur Internet qui peut être consultée par tous les services chargés de procéder à des investigations.

La Gendarmerie nationale, pour sa part, n'a pas souhaité constituer de services d'enquête spécialisés ; elle a cependant mis en place une unité à l'Institut de recherche criminelle de la gendarmerie (IRCGN) plus particulièrement chargée d'effectuer des missions d'expertise ou d'assistance.

Il faut ajouter que pour les infractions de droit commun commises sur le réseau, chaque service enquêteur spécialisé dans les différents domaines (proxénétisme, pédophilie, délit de presse...) conserve ses compétences et a formé parmi ses fonctionnaires des officiers de police capables de mener des investigations sur le réseau. La Douane en offre un bon exemple.

Toutes ces initiatives sont positives. Cependant, elles demeurent dispersées et peuvent être insuffisantes au regard des efforts et enjeux nouveaux que constituent l'Internet et les réseaux.

En effet, les possibilités nouvelles que les techniques offrent aux utilisateurs malveillants justifient que les services soient dotés de moyens comparables, notamment en matière de cryptologie ; de même, la dispersion des preuves et la complexité des poursuites nécessitent une action concertée et une collaboration accrue des enquêteurs.

Il semble dès lors nécessaire de renforcer les efforts déjà initiés et surtout la coordination entre les différents services.

À ce titre, la création d'un organisme de liaison à vocation interministérielle, associant l'ensemble des services concernés parait souhaitable : cette cellule favoriserait les échanges d'information et faciliterait les enquêtes, définirait des orientations générales en matière de criminalité de haute technologie, réfléchirait et établirait des outils techniques communs, établirait des statistiques précises sur les délits commis sur le réseau... elle constituerait également, par un pôle d'experts de haut niveau, un centre de ressources, notamment en matière de cryptologie (voir *supra* deuxième partie) auquel les différents services pourraient faire appel.

Aller au-delà de ces missions et regrouper certaines compétences comme celles des services

d'enquêtes spécialisées (mentionnées plus haut) de la direction centrale de la Police judiciaire et de la Gendarmerie nationale semble être souhaitable dans un souci d'efficacité et d'économies budgétaires ; une telle mesure qui rompt avec la tradition d'indépendance des différents services devra cependant être soutenue par une volonté politique forte. Seule une collaboration entre l'ensemble des enquêteurs, fondée sur la confiance et la transparence, donnera à cette action répressive sa véritable efficacité dans un environnement aussi éclaté et fugace que celui de la société en réseau.

Renforcer la coopération internationale

La dimension criminogène de l'Internet dépassant les frontières géographiques de l'État, celui-ci ne dispose pas nécessairement des moyens pour réprimer seul la délinquance cybernétique. Ainsi qu'ont pu le constater les membres du G8 dans leur déclaration commune lors du sommet de Washington en décembre 1997, " il est aujourd'hui impossible pour un pays, compte tenu de la nature des réseaux modernes de communications d'agir seul pour répondre à ce problème nouveau de la criminalité liée aux technologies de pointe ". Pour combattre un tel fléau transfrontalier, il devient impératif de considérer les voies d'une coopération internationale, car il est incontestable qu'une partie de la délinquance informatique a migré sur Internet.

À l'heure actuelle, il existe déjà de nombreux mécanismes d'entraide répressive internationale, laquelle peut être définie comme l'ensemble des moyens par lesquels un État prête le concours de sa force publique ou de ses institutions judiciaires à l'instruction, au jugement ou à la répression d'une infraction menée par un autre État. Toutefois, la plupart des instruments d'ordre multilatéral ont été mis en place dans un cadre géographique limité, circonscrit à l'Europe.

Ainsi, dans le cadre du Conseil de l'Europe, peuvent notamment être citées la convention d'extradition du 13 décembre 1957, la convention d'entraide judiciaire en matière pénale du 20 avril 1959, la convention européenne pour la répression du terrorisme du 27 janvier 1977, la convention pour le transfèrement des personnes condamnées du 21 mars 1983.

Au sein de l'Union européenne, ont été adoptées la convention du 25 mai 1987 relative à l'application du principe *non bis in idem*, la convention du 13 novembre 1991 sur l'exécution des condamnations pénales étrangères, l'accord du 25 mai 1987 concernant l'application de la convention du Conseil de l'Europe sur le transfèrement des personnes condamnées, l'accord du 27 mai 1989 relatif à la simplification et à la modernisation des modes de transmission des procédures d'extradition, l'accord du 6 novembre 1990 relatif à la transmission des procédures répressives. De plus, la convention d'application des accords de Schengen signée en 1990 contient de nombreuses dispositions en matière de coopération judiciaire et policière.

Par ailleurs, la France a signé des conventions bilatérales, et négocié de simples déclarations de réciprocité avec certains États, hors d'Europe.

L'ensemble de ces instruments de coopération paraît a priori *applicable à un contexte informatique*, dans la mesure où ces conventions ne font en général pas de différence en fonction du type de criminalité ou des modalités techniques de commission des infractions. Toutefois, les mesures d'exécution requises pour la mise en œuvre de la mission sollicitée peuvent soulever des difficultés dès lors qu'il s'agit de les appliquer dans le cyberespace. À titre d'illustration, on peut citer les difficultés éprouvées pour déterminer si la convention d'entraide judiciaire du Conseil de l'Europe de 1959 est ou non applicable à la perquisition de réseaux informatiques et à l'interception des communications. En effet, si la recommandation n° R (85) 10 sur les commissions rogatoires pour la surveillance des télécommunications a voulu lever certaines incertitudes, le comité d'experts chargé de la rédaction de cette recommandation a néanmoins indiqué dans son rapport explicatif (p. 101) qu'elle ne s'appliquait pas aux interceptions

effectuées dans le cadre ou en provenance d'un système ou d'un réseau informatique.

De plus, à les supposer applicables à Internet, ces mécanismes de coopération inter-étatiques risquent de se heurter à deux limites classiques :

– l'inexistence de convention d'entraide répressive avec certains pays, ce qui peut contribuer à la création de " paradis numériques " ;

– les difficultés liées à l'extradition dans les cas où il n'y a pas réciprocité de l'incrimination, où le caractère de gravité de l'infraction fait défaut, où l'infraction poursuivie peut apparaître comme de nature politique.

De surcroît, viennent s'ajouter à ces problèmes traditionnels des difficultés spécifiques à la criminalité dans le cyberespace, que l'on a pour l'essentiel déjà rencontrées dans le cadre national et qui, transposées dans un cadre supranational, ne font qu'exacerber le problème. Il s'agit notamment du suivi des communications électroniques par les services enquêteurs ; de la constitution des preuves de délits informatiques, en raison des très grandes différences d'un pays à l'autre quant aux conditions d'admissibilité des preuves ; de l'exécution de certaines mesures telles les perquisitions transfrontalières, ou l'interruption de la diffusion de messages à contenu illégal ; de la coordination des poursuites. Ces questions ne sont pas entièrement nouvelles : par la voie du satellite et des antennes paraboliques, des messages du monde entier parviennent à des téléviseurs situés sur un territoire. De même le développement de systèmes de communication GSM par satellite va-t-il compliquer les interceptions ; celles-ci doivent-elles être effectuées avec l'accord de tous les pays dans lequel le faisceau passe ? Dans la majorité de ces hypothèses, il conviendrait de repenser le cadre de l'entraide judiciaire, afin de créer une forme *sui generis* de coopération.

Il appartient donc aux États concernés de s'adapter pour permettre l'identification et la condamnation des délinquants, notamment en matière de criminalité informatique transfrontière. Des réflexions en ce sens, intéressantes et parfois constructives, ont déjà été menées au sein des États ou dans des instances internationales, qui mériteraient d'être actualisées ou approfondies afin de servir de base à une entraide judiciaire plus performante.

Dès juin 1989, le Conseil de l'Europe avait mis l'accent sur l'internationalisation des délits de haute technologie, avec l'adoption d'un rapport sur la criminalité en relation avec l'informatique. En septembre de la même année, le Comité des ministres adoptait une recommandation demandant aux États membres de tenir compte des principes directeurs préconisés par le Conseil de l'Europe. En septembre 1995, le Comité des ministres du Conseil de l'Europe adoptait la recommandation R 95 13 relative aux problèmes de procédure pénale liés à la technologie de l'information. Certaines des propositions y figurant mériteraient sans doute d'être intégrées dans un instrument contraignant. D'ailleurs, le Conseil de l'Europe a créé en 1997 un comité (PCCY) chargé d'élaborer, d'ici l'an 2000, une convention concernant la criminalité dans le cyberespace.

De même, le récent sommet des États membres du G8, qui s'est tenu à Washington en décembre 1997, a permis l'adoption de dix principes et d'un plan d'action qui devraient inspirer des initiatives internationales en la matière. Les principes adoptés prévoient en effet l'adaptation des législations répressives nationales, le renforcement des capacités techniques, l'amélioration de l'entraide judiciaire mutuelle, ainsi que l'engagement de ressources pour la formation et l'équipement des personnels d'enquête et la création d'un point de contact au niveau national chargé de recevoir les demandes d'enquêtes venues de l'étranger. Le ministère de l'Intérieur a été choisi pour assurer ce point de contact.

Enfin, au plan communautaire, une étude appelée COMCRIME du professeur Sieber, publiée au

début de l'année 1998, présente une analyse approfondie de la situation du droit pénal matériel et procédural des pays de l'Union européenne et ouvre des pistes pour faciliter la coopération judiciaire. Ces résultats nourriront les travaux sur le plan d'action contre la criminalité organisée, approuvé au Conseil européen d'Amsterdam.

À ce stade, que peut-on conclure ? La coopération judiciaire internationale est indispensable pour assurer une action efficace contre des sites ou des comportements litigieux dans l'espace mondial des réseaux ; les progrès sont fort lents et les réticences des États qui craignent une perte de souveraineté importante ; même entre pays démocratiques comparables comme ceux du Conseil de l'Europe, les différences de sensibilité restent fortes et donc la définition des infractions communes délicates ; dès lors, seule la détermination politique des États à mener une action contre les " paradis virtuels " et la délinquance de haute technologie peut les conduire à accepter l'abandon d'une partie de leur souveraineté afin de garantir l'efficacité de l'action répressive internationale.

Diverses pistes sont envisageables.

La coopération en matière d'enquête

La coopération peut prendre des canaux différents selon qu'il s'agira d'enquêtes officieuses ou de demandes officielles, par le truchement de commissions rogatoires.

? *L'enquête officieuse*

Il s'agit ici d'investigations menées par des enquêteurs dans le cadre d'une enquête préliminaire, ne nécessitant pas d'acte de procédure formel, mais plutôt la collecte d'informations sur des objets ou sur une personne, par exemple son identité exacte, sa filiation, sa dernière adresse. Le renforcement de la coopération internationale, à ce stade, apparaît comme une nécessité absolue pour lutter contre la criminalité sur les réseaux.

INTERPOL, dont le siège est à LYON, est l'organisme le plus souvent saisi de ce type de demandes. Cette instance intergouvernementale, assimilable à une organisation internationale, est chargée de la coopération policière internationale et a, à ce titre, pour objet de mettre en relation tous les services de police des États affiliés, soit environ 180 membres. Aux termes de l'article 2 de son statut, l'OICP a pour mission d'assurer et de développer l'assistance réciproque de toutes les autorités de police criminelle, dans le cadre des lois en vigueur dans les divers pays et dans le respect des principes de la Déclaration universelle des droits de l'homme, ainsi que d'établir et de développer toutes les institutions capables de contribuer efficacement à la prévention et à la répression des infractions de droit commun.

Il est évident qu'INTERPOL constitue un instrument privilégié pour l'échange entre enquêteurs d'informations concernant la criminalité dans le cyberespace, et un vecteur essentiel pour la collecte de renseignements dans le cadre d'enquêtes pénales ; son rôle devrait être renforcé dans les années qui viennent.

EUROPOL est également un lieu d'échange possible au niveau européen et sa compétence devrait sans doute s'étendre à la criminalité informatique.

? *L'échange de commissions rogatoires*

La France est liée à de nombreux États par diverses conventions internationales régissant les commissions rogatoires. Ces conventions, bi ou multilatérales, contiennent généralement des réserves ou des déclarations des États parties, qui ont pour but de définir les conditions ou modalités d'exécution des commissions rogatoires, compte tenu de spécificités nationales.

Le plus souvent, elles prévoient une clause d'exclusion dans les domaines politique, fiscal ou militaire, ainsi que dans les cas où l'État requis estime que l'exécution des actes sollicités serait de nature à porter atteinte à la souveraineté, à l'ordre public ou à ses intérêts essentiels. Ces formules permettent ainsi aux État de disposer d'une certaine marge d'appréciation pour exécuter ou non les missions qui leur sont confiées, sans risquer de voir leur responsabilité internationale engagée du fait de carence. En revanche, en l'absence de conventions, les commissions rogatoires ne peuvent être exécutées que si l'État requis y consent, et sous les formes et conditions prévues par le droit interne de cet État.

En France, les commissions rogatoires sont normalement transmises par voie diplomatique et adressées au ministère de la justice dans les formes prévues pour les demandes d'extradition, sauf clause différente. Ainsi, en ce qui concerne la Convention européenne d'entraide judiciaire, la transmission s'opère directement entre ministères de la Justice et, en cas d'urgence, les commissions rogatoires peuvent être adressées directement par l'autorité requérante à la partie requise, la transmission s'opérant éventuellement par l'intermédiaire d'INTERPOL. Par ailleurs, c'est l'autorité centrale, à savoir le ministère de la Justice, qui est seule habilitée à apprécier si la mission doit ou non être exécutée, au regard des exigences de notre droit interne. L'autorité judiciaire territorialement compétente n'est elle jamais à même de refuser d'apporter son concours. En tout état de cause, seul un magistrat instructeur peut exécuter directement, ou subdéléguer à des officiers de police judiciaire, une commission rogatoire provenant de l'étranger.

Cette procédure est lourde et apparaît particulièrement inadaptée à Internet, dont la rapidité et la fugacité des échanges constituent deux caractéristiques essentielles. Dans la mesure où la célérité est l'une des clés primordiales pour lutter efficacement contre la criminalité sur les réseaux, la réforme des mécanismes traditionnels de l'entraide constitue une nécessité.

À ce titre, il a été envisagé de confier au Ministère public, voire aux officiers de police judiciaire, le soin d'exécuter des commissions rogatoires étrangères sans contrôle préalable d'un juge. Une telle solution paraît toutefois contestable, car il semble indispensable que l'autorité judiciaire, en l'espèce un juge du siège, demeure la seule habilitée à exécuter une commission rogatoire étrangère, car son intervention constitue une garantie fondamentale pour les libertés individuelles, de valeur constitutionnelle.

De plus, l'accélération des procédures d'exécution des commissions rogatoires internationales implique une démarche globale, nécessitant une action conjointe des États intéressés et non une démarche unilatérale de la France. En ce sens, une solution uniquement nationale ne serait qu'insatisfaisante ou illusoire. Il importerait donc que, de manière concertée, les États acceptent de simplifier les règles en la matière, par exemple en renonçant à certaines clauses ou réserves qui ont pour effet de restreindre la nature ou la portée des mesures qui peuvent être effectuées dans l'État requis. En tout état de cause, la suppression éventuelle des obstacles actuellement posés à une rapide exécution dans le pays requis de l'ensemble des investigations sollicitées par le pays requérant nécessitera de longues négociations et ne saurait en conséquence être réalisée à bref délai, même si le plan d'action adopté par les États membres du G8 en décembre 1998 invite à engager une réflexion sur ce point.

Dans l'attente d'une plus ample réforme des mécanismes internationaux qui régissent l'exécution des commissions rogatoires, il serait possible de faciliter, dans le cadre de la Convention du Conseil de l'Europe, la transmission directe des commissions rogatoires de juge à juge – y compris lorsqu'il s'agit de retourner à la partie mandante les pièces de procédure une fois la mission exécutée – et de préconiser la communication systématique des pièces par télécopie en cas d'urgence . Par ailleurs, il serait aussi loisible de prévoir, dans certaines conventions bilatérales où la France est partie, l'insertion de clauses permettant une transmission des actes

judiciaires de juge à juge en cas d'urgence. De telles mesures permettraient vraisemblablement d'améliorer sensiblement la coopération judiciaire, au moins dans l'espace européen.

La coordination des poursuites dans un cadre international

La structure largement décentralisée de l'Internet n'interdit nullement d'imaginer des situations relativement complexes, dans lesquelles coexisteraient soit une pluralité de victimes résidant dans plusieurs pays, soit une pluralité d'auteurs demeurant dans différents pays, soit la combinaison de ces deux hypothèses.

Le principe no 2 adopté à Washington en décembre 1997 par les États membres du G 8 appelle à une coordination internationale. Pour faciliter la tâche des services chargés d'effectuer des enquêtes pénales dans ce type de situations, il conviendrait d'envisager que le point de contact institué dans ce cadre soit élargi à l'ensemble des pays du monde ; que par ailleurs, soit défini un point de contact international spécialisé pour la criminalité commise sur les réseaux, qui constitue un lieu permanent d'échanges d'informations ou de renseignements judiciaires, voire dans certaines hypothèses un mécanisme permettant une centralisation des enquêtes lorsqu'une même affaire présente des ramifications dans plusieurs pays. En ce sens, un renforcement des attributions d'INTERPOL ne pourrait que contribuer de manière significative à une rationalisation de la lutte contre la criminalité dans le cyberespace.

La coopération en matière d'exécution des décisions

Deux hypothèses sont à envisager :

– **l'exécution à l'étranger de décisions d'une juridiction française** : il convient à titre liminaire de rappeler que le nouveau code pénal a constitué une avancée certaine puisque, depuis 1994, l'exigence d'une double incrimination, c'est-à-dire la nécessité que le fait dommageable soit considéré comme une infraction pénalement réprimée dans l'État où il a été commis et en France, a été supprimée comme condition de compétence des juridictions françaises pour réprimer des infractions commises à l'étranger. Dès lors, les victimes françaises de ce type d'infractions peuvent en principe accéder plus facilement à un juge, puisqu'une juridiction française est normalement habilitée à juger et à réprimer ce type d'infractions. Toutefois, la difficulté réside dans le fait que le coupable des faits délictueux se trouve pour sa part à l'étranger, soit parce qu'il y réside habituellement, soit parce qu'il s'y est réfugié. La facilité qu'offre le nouveau code pénal de faire sanctionner en France un auteur étranger de faits délictueux commis depuis l'étranger risquera de demeurer théorique, si les autorités de cet État, requises pour exécuter la condamnation, n'assurent pas l'exécution des décisions de justice française. Est-ce à dire que la sanction prononcée par le juge pénal français sera inexécutée ? La réponse à cette question n'est pas nécessairement positive. En effet, il importe tout d'abord de rappeler que la condamnation pénale prononcée conservera sa vocation à s'appliquer dès lors que le condamné pénétrera sur le sol français et pourra ainsi être mise à exécution. En outre, la condamnation pénale relative aux intérêts civils pourra trouver à s'appliquer par une action de nature civile, engagée par la victime, en appliquant les règles définies par l'article 5 de la convention de Bruxelles du 27 septembre 1968 ;

– **l'exécution en France de décisions d'une juridiction étrangère** : en application du principe selon lequel l'autorité des décisions de justice s'attache aux seuls jugements rendus par les juridictions françaises, les décisions étrangères n'ont pas, de plein droit, vocation à recevoir exécution en France (Versailles 10 octobre 1983 D. 1984 IR p 87). En pratique, celles-ci ne seront exécutées que s'il existe une convention internationale régissant ce point, liant la France à l'État de la juridiction dont l'exécution de la décision est sollicitée. De plus, de telles conventions, lorsqu'elles existent, concernent généralement les peines d'emprisonnement et

fournissent des solutions en matière d'extradition de ressortissants étrangers ou de modalités d'exécution en France d'une peine prononcée à l'étranger contre un français. En tout état de cause, à défaut de convention réglementant l'extradition, la loi du 10 mars 1927 constitue, aux termes de son article 1er, un fondement juridique suffisant pour permettre aux autorités judiciaires françaises de se prononcer sur toute demande d'extradition émanant de l'étranger.

Conclusion

Il apparaît que le renforcement de l'identification des acteurs et de la capacité d'action du juge et de la police au plan national et international peut améliorer l'efficacité de la lutte contre les contenus et pratiques illégaux. Certains ont souhaité aller au-delà et inscrire l'activité des fournisseurs d'accès dans un " cahier des charges " contraignant, un statut, en en faisant une sorte de profession réglementée du fait de leur rôle privilégié. Ce cahier des charges aurait fixé des obligations de secret et de moralité, des habilitations pour les commissions rogatoires...

Cette solution, contraire à la logique de fonctionnement de l'Internet et préjudiciable au plan économique, ne doit pas être retenue ; en revanche, il est souhaitable de fixer des obligations spécifiques aux fournisseurs de services en ligne pour les services réellement nouveaux qu'ils offrent à l'utilisateur (voir *infra* cinquième partie).

Susciter et renforcer l'autorégulation des acteurs

L'autorégulation est un terme qui a suscité à la fois engouements et polémiques : engouement des libéraux désireux d'obtenir un retrait de l'intervention étatique ; polémiques face à une influence comportementale anglo-saxonne ne correspondant pas à nos mentalités et traditions. Il convient de clarifier ce débat.

Le monde des réseaux se prête mal à la réglementation étatique classique : son caractère mondial rend illusoire toute approche strictement nationale ; l'hétérogénéité des acteurs fait qu'il est difficile d'énoncer *a priori* des règles prenant en compte l'ensemble des situations de fait. La volatilité des contenus et la décentralisation du réseau rend tout contrôle un peu illusoire. Si l'objectif est de lutter contre les contenus ou pratiques illicites sur l'Internet, d'assurer cette " mise en droit " sans laquelle cet espace restera marginal comme lieu de sociabilité, il faut donc imaginer d'autres solutions, d'autres moyens.

L'autorégulation est une réponse.

Elle ne peut remplacer la loi : celle-ci, manifestation de la volonté générale, fixe des principes généraux, légitimes et obligatoires pour tous.

Certains la présentent comme située dans les " interstices " de la loi. Il semble préférable de ne pas laisser sous-entendre une défaillance de celle-ci, mais plutôt de *définir l'autorégulation comme un moyen d'appliquer les principes de la loi dans un environnement nouveau non prévu par celle-ci*.

L'autorégulation serait donc la responsabilisation des acteurs, une forme d'autodiscipline pour appliquer les principes des textes de droit aux réseaux, pour participer activement à la mise en place d'un État de droit au sein de celui-ci.

Cette approche ne s'oppose pas à celle de la réglementation et il ne s'agit pas de choisir l'une ou l'autre. En réalité, elles se combinent et se nourrissent l'une par l'autre.

L'autorégulation des acteurs a fait l'objet de nombreuses propositions, initiatives et expérimentations au plan national comme international ; divers organismes ou mécanismes ont

vu le jour et sont ainsi reconnus comme utiles dans la lutte contre les contenus illicites, l'information des utilisateurs, la formation des parents et des enfants, les dispositifs techniques de filtrage, les lignes d'urgence, les codes de déontologie et les contrats... Chacune de ces solutions a ses avantages et ses limites.

La France, très pionnière en 1996 dans son souci de développer la coopération internationale sur Internet en matière de déontologie des contenus, n'a pas véritablement abouti à des solutions concrètes dans ce domaine.

La création d'un organisme de corégulation de l'Internet et des réseaux est un moyen de se doter d'un système efficace de prévention et de lutte contre les " déviations " des réseaux. Elle offre de surcroît l'opportunité à la France de participer de façon active à la réflexion et à la mise en place de solutions innovantes, susceptibles d'être reprises par nos partenaires étrangers.

Des initiatives internationales convergentes

L'échec du Communication Decency Act a sonné le glas des approches fondées sur une simple transposition des schémas classiques de réglementation de la diffusion. Comme l'a énoncé elle-même la Cour suprême US dans sa décision de juin 1996, l'Internet s'apparente à une " conversation mondiale sans fin " et il est vain de vouloir limiter les contenus illicites, en interdisant leur diffusion.

Diverses expérimentations ont dès lors été lancées. Il ne peut être question de les analyser toutes mais seulement de tirer quelques enseignements de certaines d'entre elles.

En septembre 1996, les fournisseurs d'accès britanniques, en liaison avec les ministères de l'Intérieur et de l'Industrie, signent un engagement de " nettoyage du réseau " et créent la fondation Safety-Net dont la mission est de gérer une " hot-ligne " (ligne d'appel d'urgence), travailler sur la labelisation des sites et faire des recommandations pour améliorer la sécurité sur le réseau et la confiance des utilisateurs.

Aux Pays-Bas, de même, est créée en janvier 1996, par les fournisseurs d'accès, une fondation gérant une ligne d'urgence pour la pornographie enfantine ; une deuxième ligne est aujourd'hui ouverte pour les messages racistes.

Le bilan de ces deux initiatives, dans leur partie " ligne d'urgence " du moins, est controversé : ce mécanisme, ligne ouverte à la délation publique, est en soi un procédé contestable qui ne peut être accepté que pour des sujets très spécifiques : pédophilie, appel à la haine raciale... En outre, il importe de savoir qui gère cette ligne et selon quels critères. À ce titre, bien qu'apparemment efficace, le dispositif britannique de traitement des messages illicites a suscité beaucoup de critiques au motif qu'il donne à la ligne d'urgence des prérogatives très larges tant sur la qualification du contenu des sites que sur les possibilités de couper l'accès à ces derniers. Une association de fournisseurs d'accès a-t-elle cette légitimité ? N'y a-t-il pas un risque de censure ou de substitution au juge ?

De plus, les premières statistiques indiquent que la majeure partie des contenus illégaux détectés provient des États-Unis, ce qui rendrait nécessaire une coopération internationale entre lignes d'urgence.

Ces questions sont réelles et elles soulignent la nécessité d'avancer pas à pas, de comparer les expériences entre pays et de répondre à une question centrale : comment assurer la démocratisation du filtrage ?

D'autre initiatives ont suivi : la France en septembre 1996 saisissait l'OCDE, proposant à

l’adoption des autres pays membres une charte relative à la déontologie des contenus.

Cette proposition, assez mal reçue par nos partenaires du fait de sa connotation " étatiste ", a néanmoins été reprise par l’OCDE en mars 1997 et a permis d’impulser le travail international sur ces questions : trois réunions ont été organisées en juillet et octobre 1997 et en mars 1998 entre les États membres ; bien que les discussions aient été difficiles du fait notamment des réticences américaines et qu’elles n’aient pas, à ce stade, conduit à l’adoption de mesures concrètes, elles ont mis en évidence quelques points de consensus : l’importance de la formation et de l’éducation des acteurs à un environnement en réseau, la nécessité d’un partenariat entre les gouvernements, les utilisateurs et les industriels dans la lutte contre les contenus illégaux, la complémentarité entre une approche de " soft law ", comme les codes de conduites, et de " hard law " réglementaire ; elles ont également fait progresser la prise de conscience de l’interdépendance de tous les pays sur ces questions et l’intérêt, à ce titre, de la coopération internationale.

Aux États-Unis, prudents face à toute coopération internationale risquant de devenir contraignante, ont eux aussi travaillé activement sur l’autorégulation et incité les acteurs privés à mettre en place des mécanismes d’autodiscipline.

Un fournisseur d’accès comme AOL a ainsi mis au point des " conditions générales " contractuelles définissant sa déontologie, les procédures à suivre en cas de contenus illégaux ou préjudiciables et les modes de coopération avec les autorités de police.

Outre celui relatif aux logiciels de contrôle parental dont les premières statistiques montrent qu’ils sont peu utilisés, le débat le plus virulent a concerné la classification des sites, c’est-à-dire l’étiquetage de ceux-ci permettant un filtrage ultérieur par l’utilisateur. Une norme internationale et ouverte – la norme PICS – a été mise au point par le consortium W3C et elle permet de fixer des critères variés. Par exemple, la société RSAC (issue du monde des jeux vidéo) a procédé à la classification d’environ 50 000 sites selon les quatre critères de violence, sexe, langage et nudité. Le gouvernement américain a apporté son soutien à une telle démarche qui rend l’utilisateur responsable des contenus qu’il souhaite recevoir.

Mais les difficultés demeurent : sur quels critères se fait l’étiquetage ? Les choix américains correspondent-ils à la sensibilité européenne ? L’étiquetage doit-il être opéré par les éditeurs de contenus eux-mêmes ou par un tiers ? Est-il obligatoire ? Quelles en sont les conséquences sur l’accessibilité des sites au grand public ?

Voilà quelque unes des questions abordées dans un pamphlet de mai 1997 publié par American Civil Liberties Union (UCLA) et intitulé " Fahrenheit 451 : Is cyberspace burning ? " Cette association dénonce le risque de censure que la labelisation pourrait instituer dès lors qu’elle serait contrôlée par quelques opérateurs, contrôlant également les moteurs de recherche et cantonnant finalement certains contenus dans les " terra incognita " de l’espace virtuel. Ce scénario n’est pas seulement une adaptation du roman de Ray Bradbury ; il convient d’être vigilant sur le pluralisme et le mode de fonctionnement des agences de classification ainsi que sur les critères d’étiquetage. L’enjeu est bien, non de restreindre la liberté d’expression en identifiant des contenus " politiquement correct " progressivement obligatoires, mais d’éclairer le libre choix des utilisateurs par un filtrage démocratique.

L’Europe ne s’est pas voulue étrangère à ces préoccupations et a souhaité participer au débat mondial.

Dans le cadre de la réflexion sur l’extension de la directive " Télévision sans frontières " aux nouveaux services, la Commission réalise que s’il n’y a pas d’obstacles véritables au

développement de ceux-ci, il importe d'assurer, dans ce nouvel espace, un " haut niveau de protection de l'intérêt général ".

En octobre 1996, ont été adoptés le *Livre vert* sur la protection des mineurs et la dignité humaine ainsi qu'une communication relative aux contenus illégaux et préjudiciables sur l'Internet. La démarche de ces deux documents est celle de l'autorégulation des acteurs, la classification des sites et les dispositifs de filtrage par l'utilisateur. À la suite des consultations des États membres et des diverses parties intéressées, une proposition de recommandation du Conseil sur la protection des mineurs et la dignité humaine est adoptée le 18 novembre 1997.

Cette recommandation définit notamment des lignes directrices pour la mise en œuvre, au niveau national, d'un cadre d'autorégulation au sein desquelles figurent en priorité la représentation des parties concernées : " l'objectif est d'assurer que le développement, la mise en œuvre et l'évaluation d'un cadre d'autorégulation au niveau national s'appuient sur la participation pleine et entière des parties concernées, notamment les pouvoirs publics, les utilisateurs, consommateurs et les entreprises... " Seule une mobilisation de l'ensemble des parties garantit ainsi, selon la Commission, l'efficacité d'une telle démarche d'autorégulation. Par ailleurs, la recommandation fait référence aux codes de conduites, lignes d'urgence, logiciels de contrôle parental... et recommande que les opérateurs coopèrent avec la police dans la lutte contre les contenus portant atteinte à la dignité humaine.

Le 26 novembre suivant, le Conseil adopte un plan d'action communautaire pluriannuel visant à promouvoir une utilisation sûre de l'Internet ; c'est le volet opérationnel et financier de la Recommandation avec une orientation, cependant, un peu différente. Ce plan confirme la nécessité de mettre en place des lignes d'urgences dans chacun des pays, de développer des méthodes communes de classification et de filtrage mais ne se prononce pas sur les organismes d'autorégulation.

Prenant acte des travaux de l'OCDE, la Commission a également pris l'initiative, en juillet 1997 à Bonn, d'organiser une conférence internationale sur la société de l'information. Cet événement, largement médiatisé et illustrant la volonté politique des institutions communautaires sur ces questions, a donné lieu à l'adoption d'une déclaration commune consacrant la place déterminante du secteur privé et de l'autorégulation.

Il apparaît au rappel non exhaustif de toutes ces initiatives, qu'un véritable laboratoire mondial est en train de se mettre en place pour tenter de limiter les déviations d'un monde en réseau. Ce laboratoire a d'ores et déjà choisi des paradigmes plutôt convergents : le recours aux dispositifs techniques de filtrage, l'information et la formation des utilisateurs, la classification des contenus, la coopération des acteurs avec la police, la coopération internationale.

Des initiatives françaises peu conclusives

La réflexion française sur les autoroutes de l'information commence en 1994 par le rapport de M. Thery et celui du Commissariat au Plan ; il faut attendre cependant 1996 pour adjoindre à cette approche prioritairement technique une orientation plus politique liée à des enjeux de libertés publiques et d'ordre public. Il ne s'agit alors plus des autoroutes mais de la société de l'information qu'il convient d'organiser.

Un groupe de travail interministériel est mis en place, à l'initiative de F. Fillon et de Ph. Douste-Blazy afin d'étudier le cadre juridique de l'Internet et des réseaux ouverts et de faire des propositions permettant " dans le strict respect de la liberté de communication d'assurer un niveau satisfaisant de garantie de l'ordre public ".

Le rapport de ce groupe, présidé par Mme Falque-Pierrotin, est rendu en juin 1996 et conclut

notamment à la nécessité de recourir au contrôle *a posteriori*, d'appliquer le droit existant et de développer l'autorégulation des acteurs. Il recommande la création d'un comité des services en ligne, organisme " de veille, d'analyse et de médiation ", émettant des avis de nature déontologique sur les contenus litigieux, recevant les plaintes des utilisateurs et conseillant le gouvernement. Ce comité, distinct du Conseil supérieur de la télématique (CST) et du Conseil supérieur de l'audiovisuel (CSA), doit cependant articuler son action avec celle des deux organismes précités.

Par ailleurs, suite à la mise en cause de la responsabilités pénale de plusieurs fournisseurs d'accès dans des affaires d'appel à la haine raciale, le Gouvernement introduit lors de l'examen du projet de loi sur la réglementation des télécommunications trois amendements visant à organiser l'encadrement déontologique des réseaux.

Il ne reste de cette initiative que le nouvel article 43-1 de la loi du 30 septembre 1986 imposant à toute personne dont l'activité est d'offrir un service de connexion " de proposer à ses clients un moyen technique leur permettant de restreindre l'accès à certains services et de les sélectionner ". En revanche, les articles créant un Comité supérieur de la télématique auprès du CSA et précisant le mécanisme d'encadrement déontologique ont été annulés par le Conseil Constitutionnel par une décision en date du 23 juillet 1996.

À la suite de cet échec, François Fillon prend le parti de se retourner vers les professionnels et il confie, en octobre 1996, à Antoine Beaussant, président du GESTE, le soin d'élaborer un code de bonne conduite. Parallèlement, la France prend l'initiative de lancer, au sein de l'OCDE, une action de coopération internationale autour de la déontologie des contenus d'Internet et des services en ligne (voir *supra*).

À l'issue d'un travail important d'auditions, Antoine Beaussant rend son rapport en mars 1997 et propose une charte de l'Internet. Ce texte ambitieux affiche un objectif clair : " Pour faciliter le développement harmonieux de l'Internet, il faut préciser, dans le cadre des lois et traités, les règles et usages des acteurs et en faciliter la mise en œuvre par un outil simple et pragmatique d'autorégulation, le Conseil de l'Internet. "

L'approche, considérée comme trop autoritaire, ne suscite pas l'adhésion des autres professionnels ni des associations d'utilisateurs et un consensus ne peut s'établir. François Fillon décide alors de soumettre ces conclusions à un débat public sur le réseau à compter de mars 1997.

Les travaux se poursuivent, par ailleurs, avec un plus petit nombre de participants sous l'égide du professeur Michel Vivant. En juillet 1997, un texte est à nouveau publié, intitulé " le Manifeste ", document court et consensuel, définissant les quelques principes fondateurs de l'autorégulation en France et recommandant la mise en place un organisme d'autorégulation souple, consultatif et pluraliste.

Enfin, certains professionnels, AFA ou GESTE ont mené leurs propres réflexions : les premiers ont rédigé un code bonne conduite qui reste timide mais consacre cette préoccupation déontologique ; les seconds ont confirmé leur proposition de création d'un organisme à travers un texte intitulé " L'autorégulation a-t-elle un avenir en France ? ", mais sans réelle concertation avec les autres acteurs.

Outre ces travaux des acteurs privés, les rapports officiels maintiennent leur intérêt pour le monde des réseaux.

En novembre 1996, une mission est confiée au député Patrice Martin-Lalande qui, dans la 123e proposition de son rapport rendu en 1997, mentionne la nécessité de promouvoir l'autodiscipline

des acteurs et d'associer l'État à la constitution d'un organisme d'autorégulation.

De même, le rapport des sénateurs Turk, Jouyand et Herisson de septembre 1997 recommande, outre l'ouverture d'une ligne d'urgence et d'un Observatoire, la création d'une Agence de régulation de l'Internet, structure de droit privé, pluraliste, chargée de missions d'information, de conseil, de concertation et de coopération internationale avec les acteurs de l'Internet.

À ce stade de l'analyse, que peut-on conclure ?

? *L'expérience française relative à ces techniques nouvelles d'autorégulation est limitée*

La réflexion sur la classification des sites Internet n'a pas réellement commencé ; les services minitel n'ont jamais fait l'objet de cet étiquetage en dépit de la tentative avortée du Point bleu ; les seuls exemples de classification des contenus sont ceux de la signalétique TV ou des jeux vidéo ; pour ceux-ci, cependant, les ambitions sont modestes puisqu'il s'agit seulement d'une déclaration unilatérale du producteur.

Les logiciels de filtrage sont, comme dans les autre pays, peu connus et peu utilisés. Rares sont en outre les acteurs qui appliquent le nouvel article 43-1 de la loi de 1986.

Aucun programme d'information, issu du secteur public ou privé, sur les risques spécifiques que constitue l'espace réseau et sur les conditions d'un accès et d'une navigation sûrs n'a été élaboré ; au moment où l'on s'apprête à lancer un vaste programme de raccordement des écoles et des lycées, ce constat est particulièrement préoccupant.

Il n'existe pas de lignes d'urgence permettant de recevoir des plaintes, ni auprès de la police, ni auprès d'acteurs privés (sauf les services clients à vocation commerciale).

Enfin, le code de déontologie de l'AFA récemment publié, bien que constituant une avancée substantielle, reste modeste, sans être lié à une procédure de traitement des plaintes. Il conviendrait sur l'ensemble de ces points de mobiliser les acteurs publics et privés.

Deux schémas d'organismes d'autorégulation peuvent être écartés

? *Organisme de droit privé créé à l'initiative des seuls professionnels et sous le contrôle des fournisseurs d'accès*

Cette formule a longtemps été privilégiée par l'AFA au nom de sa relation privilégiée avec le consommateur final ; selon l'AFA, seuls les fournisseurs d'accès peuvent définir les usages dès lors qu'ils ont le quasi-monopole de l'accès à l'usager. L'AFA, cependant, est prête à associer à sa démarche, sous une forme consultative, les consommateurs, utilisateurs Internet ou associations familiales qui le souhaitent, mais en conservant la maîtrise des recommandations.

Ce système a le mérite de la simplicité du fait du nombre réduit des parties prenantes à la décision et de l'homogénéité de leurs préoccupations. Il ne correspond cependant pas au schéma de la recommandation européenne sur la protection des mineurs et la dignité humaine qui privilégie une approche plus pluraliste, associant l'ensemble des parties. Il n'a pas pour l'instant suscité l'accord des associations concernées.

Cette approche, en réalité, est celle d'une organisation professionnelle qui serait légitime à définir l'usage et les pratiques de ses membres mais sans que ses recommandations aient une portée générale.

? *Organisme de droit privé regroupant l'ensemble des acteurs de l'Internet*

Cette orientation était celle au départ de la mission d'Antoine Beaussant qui souhaitait associer tous les acteurs (fournisseurs d'accès, éditeurs de contenus, utilisateurs) afin de garantir la légitimité des avis rendus. Le modèle sous-jacent était celui du Bureau de vérification de la publicité (BVP), association de droit privée assurant une autodiscipline des acteurs de la publicité.

Il faut remarquer que le BVP est un organisme déjà ancien (1935) dans un secteur où les acteurs sont puissants et en nombre limité et sur un marché beaucoup plus mûr que celui de l'Internet aujourd'hui ; en outre, les consommateurs n'y sont associés que sous forme consultative, le BVP restant un organisme de professionnels (annonceurs, agences, supports publicitaires) ; enfin, l'histoire a montré qu'il était très difficile d'obtenir un consensus entre des acteurs de l'Internet aux préoccupations si différentes et aucun accord sur la composition de l'organisme n'a pu être trouvé au sein de la mission Beaussant ni au cours des travaux qui ont suivi.

La création d'un organisme de corégulation de l'Internet et des réseaux

Un consensus semble se dégager au plan national et international sur les points suivants :

– l'Internet et les réseaux étant un monde en pleine évolution et d'une grande complexité, il est nécessaire de créer un lieu de rencontre et de discussion entre les différents acteurs afin de réfléchir aux sujets d'intérêt commun, harmoniser les pratiques... en un mot, fixer les règles de la " civilité virtuelle " et créer un centre de compétences et d'expertise du réseau. Une telle enceinte n'existe pas, et les auditions réalisées par le Conseil d'État, qui ont confirmées de façon claire ce besoin, ne sauraient en tenir lieu de façon permanente ;

– la seule initiative privée n'a pas permis de créer en France une structure légitime pour lutter contre les contenus illicites ou préjudiciables dans un marché encore peu développé comme le marché français ;

– les usages et pratique ne peuvent être mis au point par les seuls fournisseurs d'accès qui n'ont qu'un angle d'analyse partiel ;

– l'organisme ne saurait être une instance émettant des avis contraignants de type Charte, car il imposerait une approche normative, étrangère aux attentes des acteurs et inadaptée au fonctionnement du réseau ;

– cet organisme ne saurait mettre en place un mécanisme de censure privée ou publique se substituant à l'action du juge ;

– l'organisme doit être souple de fonctionnement et évolutif dans ses missions afin de s'adapter à la réalité changeante des réseaux.

Dès lors, que faire ? L'objectif serait de mettre en place une structure expérimentale, pour une durée de deux ou trois ans, à l'issue de laquelle des modifications de l'organisation et des missions de l'organisme pourraient être envisagées.

Cette structure fonctionnerait selon une logique de droit privé et non de puissance publique en accord avec la philosophie générale de l'Internet et les attentes des acteurs.

La composition serait pluraliste, associant l'ensemble des acteurs de l'Internet, publics et privés, dans trois collèges distincts : éditeurs de contenus, prestataires techniques (accès, hébergement) et utilisateurs.

Sa compétence serait relative à la déontologie des contenus, des usages et comportements, et non

au traitement de questions spécifiques et techniques, comme celle de la propriété intellectuelle ou commerciale. Ces questions pourraient néammoins faire l'objet de recommandations générales.

Les missions de cette structure, inspirées de celles du Manifeste de juillet 1997, pourraient être les suivantes :

– élaboration de recommandations déontologiques d'ordre général sur les contenus, usages et comportements, accessibles en ligne. Ce travail ferait l'objet d'un rapport annuel ;

– gestion d'une ligne d'appel d'urgence sur les contenus de nature à porter atteinte à la dignité humaine ou à la protection des mineurs ; ces matières suscitent beaucoup d'inquiétudes aujourd'hui et font écho aux recommandations de la Commission européenne, ce qui est de nature à faciliter un soutien communautaire. La ligne d'appel serait ouverte à tous, sous réserve d'une identification claire de l'appelant afin de filtrer les messages abusifs. Dans le cas d'un appel " recevable ", l'éditeur de contenu ou le fournisseur d'accès ou d'hébergement en seraient informés afin de mettre fin à l'infraction ; ce n'est que face à leur inaction ou à leur récidive que le gestionnaire de la ligne saisirait les services de police compétents. Un contact direct avec le Parquet pourrait être prévu pour des infractions concernant des non-membres de l'organisme. Cette logique préventive, voulant instituer un climat prophylactique empêchant la réitération de l'infraction, se situe en amont de l'intervention judiciaire mais ne s'y substitue pas ;

– avis spécifique d'ordre déontologique sur le contenu de sites ou de services. Ces avis seraient communiqués aux intéressés et aux fournisseurs d'accès mais n'auraient pas de valeur contraignante auprès des acteurs qui seraient libres de les suivre ou pas ; cependant ces avis seraient de nature à éclairer les responsabilités en cas de procédure judiciaire et notamment de préciser la connaissance et les diligences exigibles en cas de contenu illicite (voir l'analyse sur la responsabilité). Il conviendra, au cas par cas, de rendre ces avis publics ;

– mission d'observation et de veille des technologies et usages de l'Internet, en liaison avec les organismes existants (observatoire des usages, INRIA,...) ;

– conseil au gouvernement sur les questions relatives à l'Internet et aux réseaux en France. L'organisme pourra être spécialement mandaté par le gouvernement sur des sujets ponctuels ;

– coopération internationale avec les organismes comparables et dans les enceintes internationales (OCDE, CEE, Conseil de l'Europe...) ;

– action de communication et d'information sur Internet et les réseaux ;

– encadrement de l'autorégulation des acteurs : sans aller jusqu'à un agrément des codes de conduite, l'organisme pourrait proposer un label de conformité à ses recommandations déontologiques que les professionnels s'engageraient volontairement à respecter. Il n'y aurait vérification de l'organisme qu'en cas de plaintes (cf procédure CNIL). L'organisme pourrait également recommander des contrats types et réfléchir aux dispositifs de classification des sites ;

– services rendus aux acteurs : médiation, arbitrage.

L'organisme va *de facto* constituer un centre d'expertise qui pourrait être sollicité par les acteurs ; ceci est possible dans le cas d'une expertise judiciaire. En revanche, compte tenu des risques de confusion par rapport à une mission d'intérêt général, il semble utile d'évaluer une telle mission avant de l'inscrire expressément dans les statuts de l'organisme, en analysant notamment les expériences américaines et canadiennes (Cybertribunal et Virtual Magistrate). En tout état de cause, la procédure d'avis, en elle-même, peut déjà faciliter le règlement amiable du conflit entre les parties.

La compétence de l'organisme devrait s'étendre aux services en ligne minitel/Audiotel.

Les modalités de régulation du minitel sont celles du décret d'avril 1993 ; ce décret est aujourd'hui inadapté dès lors qu'il reposait sur le monopole de France Télécom. Le mode actuel de réglementation, au sein duquel s'exerce la compétence du CST et du CTA, se situe dans un contexte spécifique liant les acteurs par voie contractuelle. L'ouverture à la concurrence des télécommunications conduit à s'interroger sur l'évolution du mode de régulation des services de télématique anonyme, écrite et vocale. La logique du système repose en effet sur le monopole de l'exploitant public auquel fait expressément référence le décret de 1993. On voit mal les nouveaux opérateurs reprendre de façon obligatoire les clauses des contrats types de France Télécom et des fournisseurs de services. Les problèmes rencontrés étant comparables et l'évolution des techniques permettant un accès simultané à Internet et aux services en ligne de type minitel et Télétel, la compétence de l'organisme nouvellement créé devrait s'étendre à ces derniers. Un tel rattachement illustrerait au surplus et de façon claire, la volonté des pouvoirs publics de voir les services télématiques migrer vers Internet. Le décret d'avril 1993 sera dès lors abrogé.

Quelle structure juridique pour ce nouvel organisme ?

Certains restent favorables à la mise en place d'une structure publique pour réguler les contenus illégaux sur les réseaux : l'AFPI affirme ainsi qu'un éventuel " Conseil de l'Internet " doit être nommé par l'État et pourvu de compétences réglementaires. La structure publique présente selon eux de nombreux avantages : simplicité de la nomination par arrêté, possibilité d'avoir des pouvoirs d'investigation, voire de contrainte, légitimité.

Les structures publiques qui ont été envisagées pour assurer le rôle de " régulateur des réseaux " sont soit une autorité indépendante, soit une commission administrative rattachée à un ministre (Justice, Culture, Premier ministre, voire un double rattachement) ou à une autorité administrative indépendante.

Il semble difficile de proposer une nouvelle autorité administrative indépendante, compétente pour les services Internet : la logique d'une telle institution est, en effet, en général de constituer un garant de l'application d'une réglementation, indépendant de l'État, lui-même acteur. Telle n'est pas la situation pour l'Internet qui ne fait pas l'objet d'une réglementation spécifique pour laquelle l'État risquerait d'être juge et partie ; à l'inverse, la logique de la corégulation est d'associer en amont l'ensemble des acteurs, publics et privés, à l'élaboration et à l'application de règles permettant le respect de la réglementation. Enfin, le constat selon lequel il n'y a pas un droit de l'Internet, comme on a pu mettre en place un droit de l'audiovisuel, mais des contenus soumis à des réglementations sectorielles spécifiques, rend peu adaptée la création d'une autorité publique unique compétente pour l'encontre des contenus, véhiculés sur le réseau, d'autant que les réseaux eux-mêmes devraient faire l'objet d'un traitement séparé et neutre (voir *infra* cinquième partie).

La création d'une commission administrative ne semble, elle aussi, guère adaptée au monde de l'Internet et des réseaux : elle risque d'apparaître au plan international comme l'illustration classique du centralisme administratif français ; elle serait la plus éloignée de l'autorégulation, voie qui semble s'imposer sur les réseaux. En outre, une proposition qui prévoyait le rattachement d'un comité de la télématique au CSA a été annulée par le Conseil constitutionnel par la décision du 23 juillet 1996 sus-mentionnée ; les professionnels sont enfin très réticents à cet égard. Il reste que le CSA semble aujourd'hui moins désireux d'une telle innovation, son articulation nécessaire avec la nouvelle structure pouvant se traduire simplement par la désignation d'un de ses membres au sein de celle-ci.

La solution la plus appropriée semble donc celle d'une structure privée à condition qu'elle puisse se " teinter " d'un caractère public lui permettant d'asseoir sa légitimité et de faciliter sa constitution.

Il pourrait s'agir d'une association " d'intérêt général ", ce qui l'autoriserait à employer du personnel privé et public mis à disposition et à recevoir, outre des subventions publiques (État, Communauté européenne...) des cotisations privées des acteurs.

L'assemblée générale serait ouverte à toutes les personnes morales, y compris les entreprises individuelles, ayant payé leurs cotisations, sans limiter l'adhésion aux seules associations. Chaque personne s'inscrirait dans un " collège ".

Le Conseil d'administration serait composé de représentants des trois collèges, élus par leurs pairs (3 par collège), ainsi que de membres nommés par l'État (3). Au total 12 membres auxquels l'on ajouterait trois personnalités qualifiées nommées par l'État dont le président ; en outre, participeraient aux travaux en tant qu'" observateurs " mais sans droit de vote, trois représentants du CSA, de la CNIL et de l'ART.

L'adhésion à l'association doit-elle être libre ou obligatoire ?

L'adhésion obligatoire garantit la représentativité mais nous éloigne d'une structure privée ; elle pourrait en outre apparaître contraire à l'article 15 de la Convention européenne de sauvegarde des droits de l'homme. Il convient de maintenir une participation libre et d'imaginer un mécanisme incitant à l'adhésion : peut-être, la possibilité pour l'organisme de proposer au ministre l'extension de ses recommandations à de non-membres au-delà d'une certaine période. Cette disposition ne crée pas un mécanisme contraignant, les recommandations restant des avis ; leur portée ne doit pas pour autant être négligée : elles permettent d'exercer une réelle pression sur les acteurs.

Compte tenu des dérogations au régime général des associations et afin de conforter le caractère d'intérêt général de la structure, celle-ci ne peut être créée que par la loi, les statuts pouvant être adoptés par décret. Une telle procédure a déjà été retenue pour la création du Conseil national des marchés financiers.

Enfin, l'organisme devra être doté des moyens financiers ou humains de nature à lui permettre d'exercer ses missions. Il semble possible d'estimer son budget global à 20 MF. À titre de comparaison, le budget annuel du Bureau de vérification de la publicité (BVP) est de 20 MF avec 22 collaborateurs, celui du Conseil national des arts culinaires de 12 MF et de l'Association française sur le nommage (AFNIC), nouvellement créée, de 10 MF avec une dizaine de collaborateurs.

Ce financement doit être assuré à la fois par des subventions publiques, nationales et communautaires, et par des cotisations des acteurs ; celles-ci pourront varier selon la part de marché de l'intéressé et conditionner les droits de vote. Dans tous les cas, il conviendra d'assurer un financement stable et suffisant à l'organisme.

Cinquième partie

Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel

et des télécommunications

Le droit de la communication est marqué par la distinction entre le régime des services et réseaux de télécommunications, d'une part, et le régime des services et réseaux audiovisuels, d'autre part. Cette situation s'explique par le fait que chaque réseau est longtemps demeuré principalement dédié à un service : le spectre hertzien à la radiodiffusion (télévision, radio, ...) et le réseau téléphonique filaire de France Télécom à la téléphonie locale ou le minitel, par exemple. En outre, lorsqu'un service est susceptible de transiter par des réseaux variés, son régime varie souvent en fonction des réseaux empruntés. Ainsi, le régime des services de télévision obéit à des règles différentes selon que la diffusion emprunte le satellite, le câble ou le réseau hertzien .

Internet s'inscrit avec difficulté dans ce cadre traditionnel qui repose sur la distinction des services et des réseaux et fait largement dépendre le régime des services des supports empruntés. **Internet présente en fait la particularité de ne pouvoir être qualifié, au sens strict, ni de réseau ni de service**. Si l'on fait parfois appel à la notion de réseau pour qualifier Internet, ce n'est que par référence aux modalités de transport de l'information et non pour désigner un type particulier de support. En pratique les données accessibles via l'Internet transitent par tous types de supports (réseau téléphonique, câble, satellite, etc.). Internet ne constitue pas non plus un service en lui-même mais permet l'accès à une grande variété de services. Certains services sont spécifiques et constituent véritablement des nouveaux services : messagerie (e-mail), forums de discussion. D'autres services offerts, pour certains à titre encore largement expérimental, sont plus classiques : vente par correspondance, accès à des bases de données, presse en ligne, radio, images animées, téléphonie, etc.

Ainsi, Internet ne constitue ni un nouveau service, ni un nouveau réseau mais une modalité nouvelle d'accéder à des services qui emprunteront toutes sortes de supports pour parvenir jusqu'au terminal de l'utilisateur.

L'impossibilité de ranger l'Internet dans les catégories existantes (réseau ou service) peut conduire à le présenter comme l'archétype d'un phénomène nouveau, la convergence entre les mondes jusqu'alors séparés des réseaux informatiques, de l'audiovisuel et des télécommunications. Internet est en effet au cœur d'une mutation qui conduit à distendre le lien traditionnel entre les services et les supports. Avec Internet, accessible par tous les réseaux et offrant l'accès à des contenus transnationaux d'une grande variété, **la réglementation des services ne peut plus dépendre des supports empruntés**. C'est l'objet même de ces services et des contenus qu'ils véhiculent qui importe. La convergence pourrait donc conduire à la révision des schémas réglementaires traditionnels marqués par une approche sectorielle en partie dépassée par l'évolution des technologies. C'est la proposition d'un stimulant *Livre vert sur la convergence des secteurs des télécommunications, des médias et des technologies de l'information et les implications sur la réglementation* présenté en décembre 1997, à l'initiative de M. Martin Bangeman, commissaire européen en charge des télécommunications (DG XIII). Ce *Livre vert* a donné lieu à une très large consultation. Les rapporteurs de cette étude ont nourri de leurs premières conclusions la réponse du gouvernement français à ce document. Il apparaît que si l'analyse du *Livre vert* doit être nuancée, la convergence rend bien nécessaire une adaptation de la réglementation de la communication et des services en ligne .

Le phénomène de convergence ne doit pas remettre en cause la distinction entre communication au public et correspondance privée

L'analyse du Livre vert de la Commission européenne sur le phénomène de convergence

Le *Livre vert* estime très avancée la convergence des secteurs des télécommunications, des médias et des technologies de l'information

Le *Livre vert* distingue trois niveaux de convergence : d'abord la convergence des réseaux et celle des terminaux ; ensuite la convergence des industries ; enfin celle des services offerts. En pratique, le phénomène de convergence traduirait pour l'essentiel la capacité des différentes plates-formes (supports) à transporter des services similaires et dans une moindre mesure la fusion progressive des équipements grand public comme le téléphone, la télévision et les ordinateurs personnels. La convergence des réseaux et des services serait bien avancée : des opérateurs de télécommunications offrent des services audiovisuels sur leurs réseaux, et inversement des opérateurs audiovisuel (notamment les câblo-opérateurs) offrent des services de télécommunication, incluant la téléphonie vocale.

Cette convergence est rendue possible par le recours à une technologie jusqu'alors dédiée à l'informatique : le numérique. Cette technologie devient le langage commun d'univers jusqu'alors séparés. Elle permet de transformer données, son et images dans un langage universel exprimé en séries de 1 et de 0. Le grand avantage de cette technologie est de permettre la manipulation et la compression des données , limitant ainsi les contraintes résultant de la pénurie de ressources liée à l'utilisation traditionnelle des modes de transmission analogiques. Internet est décrit comme au cœur de ce processus. Il permet l'accès à des services audiovisuels comme de télécommunications. Il est accessible par des terminaux informatiques (PC multimédia), audiovisuel (télévision), et de télécommunication fixes ou mobiles (téléphones aptes à recevoir des données multimédia).

Des adaptations de la réglementation seraient rendues nécessaires par le phénomène de convergence

Tout l'enjeu du *Livre vert* est de susciter un débat sur les adaptations de la réglementation rendues nécessaires par le phénomène de convergence en général et par l'émergence de l'Internet en particulier. Partant du constat que la convergence aura un impact économique et social globalement positif, il est proposé de lever les barrières existantes ou potentielles susceptibles de la freiner. Les réglementations sectorielles actuelles, élaborées dans un contexte de pénurie de ressources disponibles, constituent l'une des principales difficultés identifiées .

L'un des défis résulterait de la difficulté à opérer désormais une **distinction entre les communications publiques et privées**. Aussi, selon le *Livre vert* (p. 23), la convergence pourrait conduire à déplacer la limite actuelle entre ce qui relève de la réglementation des communications publiques et privées. Il était auparavant assez facile de ranger les différents services dans des catégories bien déterminées. Il n'en va plus de même avec l'émergence de nouveaux services marqués par une certaine ubiquité. Internet est le principal révélateur de ces difficultés. Ainsi, " un utilisateur d'Internet peut indifféremment parler ou écouter, entremêlant les communications publiques (dont le contenu est – tout au moins dans le cas de la radiodiffusion – traditionnellement réglementé) et les communications privées (traditionnellement non réglementées). Ce décalage constant entre l'édition et les modes de communication privée, chacun étant réglementé par des principes très différents, constitue l'un des principaux défis de la réglementation de l'Internet. " (p.7)

Pour surmonter ces difficultés, trois options sont proposées par le *Livre vert* :

– *option 1* : adapter les réglementations actuelles pour prendre en compte les caractéristiques

spécifiques des nouveaux services ;

– *option 2* : créer une catégorie nouvelle de " nouveaux services " peu réglementée, coexistant avec les deux grandes catégories traditionnelles (audiovisuel et télécommunications) ;

– *option 3* : élaborer un nouveau cadre réglementaire commun aux différents secteurs de la communication.

La réalité du phénomène de convergence et son impact sur la réglementation appellent un constat nuancé

Toute analyse réglementaire prospective suppose de procéder à une évaluation préalable de la réalité du phénomène de convergence. Il ressort des différentes auditions que, si la réalité du phénomène de convergence est bien tangible, elle est néanmoins variable selon les niveaux d'analyse et sans doute surestimée par le *Livre vert* pour ce qui concerne les marchés et les industries. De même, l'incapacité de la réglementation à faire face à l'apparition de services interactifs d'une nature mixte ne doit pas être exagérée, au moins pour ce qui concerne la distinction actuelle entre communications publiques et privées qui demeure pertinente.

Le phénomène de convergence concerne essentiellement les réseaux mais progresse sur les services sous l'influence de l'Internet

? *La convergence technologique est plus avancée pour les réseaux que pour les terminaux*

La convergence des réseaux est manifestement la plus avancée. Des services, jusqu'alors véhiculés par des réseaux dédiés, peuvent désormais être transmis sur de nouveaux supports, offrant une véritable alternative aux opérateurs. Cette évolution concerne tant l'offre d'accès aux services en ligne que la radiodiffusion ou la téléphonie. Chacun de ces types de services empruntait pour l'essentiel un réseau spécifique : le réseau filaire traditionnel de télécommunication pour le minitel et la téléphonie ; le spectre hertzien pour la télévision. Il n'en va plus de même aujourd'hui. Le spectre hertzien est aujourd'hui utilisé pour la téléphonie mobile et, dans un proche avenir, la mise en place d'une nouvelle norme de téléphonie mobile rendra possible la diffusion de données multimédia (" Universal Mobile Télécommunication System ", nouvelle norme de téléphonie). Le traditionnel réseau téléphonique filaire, dopé par le recours à de nouvelles techniques de transmission comme l'xDSL et l'ATM , constituera lui aussi une nouvelle infrastructure alternative susceptible de véhiculer des images animées et des données multimédia.

La substituabilité des réseaux est patente s'agissant de l'Internet qui peut tous les emprunter, voire les fédérer dès lors qu'ils sont tous aptes à la communication dans un même langage : le numérique couplé au protocole informatique TCP/IP. Si le réseau téléphonique demeure le vecteur privilégié des échanges en ligne, le câble, le satellite, voire le réseau électrique et le spectre hertzien terrestre constituent de réelles alternatives. Ainsi, à titre d'exemple, des messages peuvent être reçus par voie satellitaire (voie aller du serveur vers l'utilisateur) tandis que la voie de retour (de l'utilisateur vers le serveur) empruntera le traditionnel réseau téléphonique. Canal plus expérimente auprès de 200 abonnés cette possibilité, qui devrait permettre d'offrir un accès Internet à haut débit à ses abonnés, indispensable pour permettre la diffusion d'images animées de bonne qualité.

Pour autant, la convergence des technologies est loin d'être totale et il paraît abusif d'évoquer aujourd'hui la constitution d'un vaste réseau intégré. Les anciens réseaux subsistent, de nouveaux réseaux apparaissent, mais ils demeurent toujours principalement dédiés à certains services. Ainsi, il est plus probable que les services de télévision emprunteront demain des

technologies de diffusion numérique hertzienne, par satellite ou par câble, plutôt que le traditionnel réseau téléphonique dont il n'ont pas la maîtrise et, qui offre des largeurs de bande passante encore étroites au niveau de la boucle locale d'accès aux usagers. Surtout, l'intégration des différents réseaux supposerait des terminaux uniques ou véritablement substituables. Or, le téléviseur et l'ordinateur individuel demeurent affectés à des usages spécifiques. Si techniquement il est d'ores et déjà possible de recevoir des images animées sur un PC *via* l'Internet, et d'accéder à Internet à partir d'un poste de télévision (Web TV), il n'est pas impossible que les particuliers maintiennent, pour des raisons de commodité et de confort, une préférence pour un cumul de terminaux (téléphone, ordinateur, télévision), même lorsqu'ils sont accessibles par un réseau unique (le câble par exemple).

? *La convergence des services progresse sous l'influence de l'Internet*

L'Internet permet de plus en plus une offre alternative de services traditionnels. Des services de télévision ou de téléphonie ne doivent pas être considérés comme de nouveaux services au seul motif qu'ils sont accessibles via Internet. Il ne s'agit pas de nouveaux services, mais d'une nouvelle offre de services traditionnels. Dans un tel cas, il apparaît nécessaire de procéder à un examen de cette offre pour apprécier s'ils sont véritablement substituables aux anciennes modalités de mise à disposition du public afin de prévenir des distorsions de concurrence. Tel serait, par exemple, le cas si des services de téléphonie vocale ou de télévision étaient proposés *via* l'Internet par des opérateurs n'étant pas soumis aux contraintes réglementaires ou tarifaires qui s'imposent aux acteurs de ces deux secteurs.

Ce n'est pas véritablement le cas aujourd'hui pour les services de télévision sur Internet qui, du fait de la médiocre qualité de l'image et le faible intérêt des diffuseurs de télévision pour les services de " Webcast ", ne devraient pas se substituer à l'offre traditionnelle de télévision dans un proche avenir.

Il n'en va pas de même pour les services de téléphonie vocale qui apparaissent sur l'Internet et suscitent un véritable intérêt des consommateurs et des fournisseurs d'accès à Internet. Des utilisateurs d'Internet parviennent à établir des communications vocales avec leurs correspondants grâce à des logiciels installés sur leurs ordinateurs équipés de haut-parleurs. Surtout, une offre de tels services à l'initiative des fournisseurs d'accès, dite de seconde génération, se développe aux États-Unis au Japon , et fait son apparition en Europe. Aux États-Unis, les opérateurs de téléphone longue distance ont saisi la Federal Communication Commission d'une plainte, justifiée par le détournement de trafic dont ils seraient victimes, dès lors que la téléphonie sur Internet est facturée au tarif des communications locales et que ces services ne sont pas soumis aux obligations qui pèsent sur eux. La FCC examine cette question et pourrait proposer une adaptation de la réglementation pour prévenir les distorsions de concurrence.

La Commission européenne a préféré l'année dernière (communication du 7 mai 1997) écarter la qualification de téléphonie vocale sur Internet, en se fondant sur la définition juridique précise de la téléphonie vocale, donnée à l'article 1er de la directive no 90-388-CE du 28 juin 1990 relative à la concurrence dans les marchés des services de télécommunications. La Commission estimait alors que les communications vocales sur Internet ne peuvent être considérées comme un service de téléphonie vocale qu'à la condition de remplir plusieurs critères cumulatifs : les communications doivent faire l'objet d'une exploitation commerciale ; être fournies au public ; au départ et à destination des points de terminaison du réseau public commuté par le réseau téléphonique fixe ; et, assurer le transport direct et la commutation de la voix en temps réel. Pour la Commission, l'une des conditions au moins n'était pas satisfaite : celle liée à la commutation de la voix en temps réel. Toutefois il y a lieu de tenir compte de développements technologiques récents permettent aujourd'hui de raccourcir considérablement les délais nécessaires à la

transmission de la voix et de l'apparition d'une offre commerciale par les fournisseurs d'accès à Internet. Une approche plus pragmatique, qui s'attacherait à déceler le caractère substituable des services de téléphonie, sur Internet à l'offre traditionnelle conduirait sans doute à une conclusion différente. (Voir *infra* pour une analyse plus détaillée des implications réglementaires).

? *La convergence des industries demeure limitée*

La concentration horizontale entre les acteurs de la communication demeure relativement limitée. Certains groupes réunissent toutefois des filiales ou des participations importantes dans des entreprises de chacune des grandes branches de la communication. Vivendi (nouvelle appellation de la Générale des eaux) illustre cette démarche. Le groupe réunit en effet Canal + (audiovisuel), Havas (médias), Cégétel (télécommunications). Les synergies entre les différentes branches, se développent progressivement, notamment à travers Numéricable (ex-Compagnie générale de vidéocommunication) et l'offre d'accès à Internet (récents accords Canal +, AOL, Cégétel). La Lyonnaise des eaux offre aussi un bon exemple de convergence des services avec son offre numérique sur le câble qui permet à l'usager, par un abonnement unique, d'avoir accès à la télévision numérique, à Internet à haut débit et au téléphone.

En pratique, on ne constate pas encore de grands mouvements de fusions ou acquisitions qui donneraient naissance à des géants de l'informatique, de l'audiovisuel et des télécommunications. En règle générale, les acteurs du secteur de la communication préfèrent prendre des participations, nouer des accords avec d'autres acteurs exerçant des métiers proches et complémentaires. Tel est par exemple le cas pour France Télécom, fournisseur d'accès à Internet (Wanadoo) et actionnaire du bouquet satellite TPS, ou de Microsoft qui se rapproche d'opérateurs de télévision. En revanche, l'on assiste à un véritable mouvement de diversification des opérateurs, même s'ils privilégient toujours leur métier de base. C'est notamment le cas des gestionnaires d'infrastructures, qui cherchent à valoriser leurs réseaux au mieux et par conséquent à ne pas en limiter l'usage à leur destination initiale. Les câblo-opérateurs offrent des services de téléphonie vocale sur le câble, et des propriétaires de réseaux téléphoniques ou même électriques (expérience menée en Grande-Bretagne) se montrent intéressés par les contenus multimédia.

Cette convergence des industries est donc pour le moment la moins avancée. C'est peut-être aussi celle qui devrait avoir l'impact immédiat le plus modéré sur la réglementation. Les problèmes susceptibles de survenir relèvent pour l'essentiel du droit commun de la concurrence. Des exigences spécifiques (recherche du pluralisme de l'information pour l'audiovisuel qui justifie un dispositif limitant la concentration ; ouverture à la concurrence du secteur des télécommunications marqué par une situation monopolistique à l'origine, nécessitant des dispositions particulières et notamment un droit à l'interconnexion au réseau de l'exploitant initial) nécessitent toutefois le maintien d'un droit sectoriel de la concurrence.

La distinction traditionnelle entre communications publiques et privées ne doit pas être remise en cause par le développement des services en ligne de nature mixte

? *Le droit français est marqué par une importante distinction entre communication audiovisuelle et correspondance privée*

En droit français, cette distinction est fondamentale. Elle est prévue à l'article 2 de la loi du 3 septembre 1986 qui dispose dans son alinéa 2 : " On entend par communication audiovisuelle toute mise à disposition du public ou de catégorie de public, par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toutes nature qui n'ont pas le caractère d'une correspondance privée. " La notion de correspondance

privée n'a fait l'objet d'aucune définition législative. Une circulaire du 17 février 1988 a cependant précisé ces notions : " La communication audiovisuelle se définit par opposition à la correspondance privée. Il y a correspondance privée lorsque le message est exclusivement destiné à une (ou plusieurs) personnes, physique ou morale, déterminée et individualisée. À l'inverse, il y a communication audiovisuelle lorsque le message est destiné indifféremment au public en général ou à des catégories de public, c'est-à-dire un ensemble d'individus indifférenciés, sans que son contenu soit fonction de considérations fondées sur la personne. "

La qualification de communication audiovisuelle implique un contrôle du respect d'objectifs d'intérêt général (déontologie de l'information, protection des mineurs, identification de la publicité...), tandis que celle de correspondance privée implique au contraire le respect du secret des correspondances et l'obligation de s'abstenir de toute ingérence dans la transmission des messages .

Contrairement à une interprétation répandue, la distinction ne repose pas sur des critères techniques opposant les services de télécommunications " point à point " (d'utilisateurs à utilisateurs) et les services audiovisuels " point – multipoints " (d'un diffuseur à de multiples utilisateurs), mais sur la nature de la communication. Dans un cas, le message est mis à la disposition du public, dans l'autre il est exclusivement destiné à une ou plusieurs personnes et revêt un caractère privé.

En conséquence, pour plus de clarté, **le concept de communication au public devrait se substituer à celui de communication audiovisuelle**. Ce dernier, à la différence de la notion de correspondance privée, tend à mélanger la destination du message (qui vise le public et non des personnes bien individualisées) et le service offert (services audiovisuels de radio ou de télévision). Dès lors que toute communication au public ne relève plus nécessairement d'une logique traditionnelle de diffusion par des services audiovisuels, il apparaît préférable d'adapter la terminologie et de rechercher l'exact pendant de la notion de correspondance privée qui, elle, ne laisse rien sous-entendre quant aux modalités de transmission et aux contenus de la communication.

La plupart des services en ligne présentent une nature mixte : ils ont pour partie le caractère d'une communication au public et pour partie le caractère d'une correspondance privée (par exemple, une transaction peut donner d'abord lieu à une offre commerciale de caractère publicitaire et être suivie d'une commande par courrier électronique). Faut-il pour autant chercher à ranger le service dans l'une seulement des deux catégories ?

? *Un service mixte, qui n'a pas exclusivement le caractère d'une correspondance privée, ne saurait être qualifié seulement de communication au public*

Il serait inopportun de déplacer la frontière entre communications publiques et privées. Ranger un service de nature mixte dans l'une seulement des deux catégories ne permet pas de veiller à la préservation de l'ensemble des garanties qui doivent entourer la mise en œuvre du service. Prenons l'exemple d'un service de vidéo à la demande . Un tel service revêt manifestement un caractère de communication au public dans la mesure où le service est mis à la disposition du public. Mais la consommation de ce service donne lieu à une commande et à un paiement qui présentent le caractère d'une correspondance privée. Aussi, ne faire de ce service que l'accessoire d'un service audiovisuel et qualifier exclusivement ce service de communication audiovisuelle serait réducteur. À l'inverse, extraire totalement ce service de la sphère de l'audiovisuel ne paraît pas justifié. Dès lors que ce service donne lieu une communication au public, il importe de veiller au respect d'objectifs d'intérêt général (voir, *infra*, une liste possible d'objectifs constituant un socle minimal) et notamment, dans le cas de la vidéo à la demande, au

respect de la propriété littéraire et artistique.

En réalité, un même service peut relever à la fois de la législation audiovisuelle et du code des postes et télécommunications. Cette analyse vient récemment d'être confortée par la cour d'appel de Paris, par deux arrêts du 28 avril 1998 relatifs à un litige opposant des câblo-opérateurs à France Télécom, arbitré par l'Autorité de réglementation des télécommunications . L'ART, saisie sur le fondement de l'article L. 36-8 du code des postes et télécommunications , s'était estimée compétente pour trancher un litige relatif à la fourniture de service d'accès à Internet sur des réseaux câblés. France Télécom estimait l'ART incompétente pour trancher un litige concernant l'offre d'accès à Internet qui relevait selon l'opérateur public de la législation sur l'audiovisuel. Mais la cour d'appel de Paris, comme l'ART, a estimé que les réseaux câblés permettaient aussi d'offrir des services de télécommunications dès lors que la technique rendait possible l'utilisation de ces réseaux dans deux sens (" le sens descendant, qui transporte des signaux depuis la tête du réseau jusqu'à l'abonné ; le sens remontant, qui transporte des signaux depuis l'abonné jusqu'à la tête du réseau et au-delà comme dans le cas d'Internet, réseau mondial d'ordinateurs connectés entre eux "...) et que le service d'accès à l'Internet pouvait être qualifié de service de télécommunications au sens de la directive sur la libéralisation des télécommunications .

Ainsi, plutôt que de chercher à déplacer les frontières des deux catégories existantes pour rattacher artificiellement des services mixtes à l'une d'elle, **il paraît plus opportun de chercher une application combinée des législations sur l'audiovisuel et sur les télécommunications lorsque cela est nécessaire**.

Si une remise en cause de cette distinction fondamentale doit être écartée, il n'en demeure pas moins nécessaire de procéder à des adaptations de la réglementation de la communication en général et de l'Internet en particulier.

Des adaptations de la réglementation sont rendues nécessaires par la convergence technologique et le développement des services en ligne

Le phénomène de convergence et le développement rapide de l'offre de services en ligne conduit, on l'a vu, à distendre le lien traditionnel unissant le plus souvent des services et des réseaux qui leur sont dédiés.

Si la tentation de créer une nouvelle catégorie juridique pour " les nouveaux services " semble devoir être écartée, le phénomène de convergence rend souhaitables, à moyen terme, certaines adaptations de la réglementation de la communication. Sans prétendre à l'exhaustivité, quelques pistes peuvent être suggérées. À court terme, le cadre juridique pourrait faire l'objet d'une adaptation ponctuelle, permettant d'encadrer le développement de l'offre de nouveaux services en ligne.

Adapter à moyen terme la réglementation de la communication

Renoncer à la tentation de créer une catégorie juridique de " nouveaux services "

À certains égards, la tentation de créer une vaste catégorie de nouveaux services, peu réglementés, coexistant avec les deux grandes catégories traditionnelles (audiovisuel et télécommunications), est en germe dans la législation et les réflexions communautaires. À côté des services de radiodiffusion " point-multipoints traditionnels ", il faudrait tenir compte de

l'émergence de nouveaux services fournis de " point-à-point " et sur appel individuel (par exemple, la vidéo à la demande).

Ces nouveaux services sont définis pour la première fois par la directive no 83-189, modifiée en 1997, sur la transparence réglementaire dans le marché intérieur pour les services de la société de l'information, par opposition aux services traditionnels de radiodiffusion sonores et télévisuels qui relèvent eux de la directive télévision sans frontière, dans les termes suivants : " Tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance par voie électronique et à la demande individuelle d'un destinataire de service. " Cette directive met en place une simple procédure d'information de la Commission sur les réglementions des États membres. Elle revêt toutefois une grande importance dans la mesure où elle isole une nouvelle catégorie de services, dans la perspective éventuelle de définir par la suite un régime juridique qui lui serait applicable. La définition retenue est très large. Elle englobe en fait des services interactifs qui relèvent de l'audiovisuel à l'exception, semble-t-il, des services de radiodiffusion cryptés. En pratique sont visés notamment : la vidéo à la demande, le commerce électronique, les services d'information multimédia, la publicité électronique, les téléservices professionnels.

La création d'un régime juridique spécifique (allégé) pour ces nouveaux services (option 2 du *Livre vert* présentée plus haut), de prime abord séduisante, présenterait plusieurs inconvénients :

– tout d'abord, créer un régime juridique spécifique pour des nouveaux services, entre la catégorie des services qui relèvent de la communication au public et les services de correspondance privée, conduirait à remettre en cause la distinction entre communication au public et correspondance privée et à priver les destinataires de ces services des garanties attachées à cette distinction (voir *supra*) ;

– elle suppose ensuite qu'il soit possible de déterminer avec précision les frontières de cette catégorie si l'on souhaite à terme lui appliquer une réglementation spécifique allégée (option 2 du *Livre vert*). Or, la partition entre ces nouveaux services, les services audiovisuels classiques, les nouveaux services audiovisuels (cryptés) et les services de télécommunication au sens strict, semble bien difficile à opérer ;

– elle va à l'encontre de l'objectif de neutralité dans le traitement de services comparables (voir *infra*) ;

– enfin, une réglementation unique paraît difficile à envisager pour des services aussi divers que la presse en ligne, la vidéo à la demande, la vente par correspondance ou la télémédecine.

Aussi, il semble préférable de s'orienter vers une approche privilégiant la neutralité dans le traitement des réseaux et des services.

Tendre à terme vers plus de neutralité dans la réglementation des réseaux et des services

? *Le régime des réseaux*

La réglementation actuelle demeure très marquée par une distinction entre le régime des services audiovisuels (qui relèvent pour l'essentiel de la loi du 30 septembre 1986 et du contrôle du CSA) et celui des services télécommunications (régis par le code des postes et télécommunications et relevant de la compétence du ministre chargé des Télécommunications et de l'Autorité de régulation des télécommunications). Cette distinction emporte des effets sur le régime des réseaux. Un même réseau obéira dans certain cas à un régime différent selon qu'il véhicule des services audiovisuels ou de télécommunications. Ainsi, le régime des supports demeure très

largement dépendant de la nature des contenus véhiculés.

Une telle **disparité de traitement se justifie pour la gestion du spectre hertzien qui devrait rester une ressource rare**. Certaines bandes passantes sont réservées aux services audiovisuels, alors que, d'un point de vue strictement économique il serait plus rentable de les allouer à un usage de télécommunications civiles intensif. La rareté du spectre rend indispensable le maintien d'un contingent de ressources hertziennes pour l'audiovisuel , afin d'assurer le respect d'objectifs d'intérêt général (notamment le pluralisme et l'accès à l'information).

En revanche, dans d'autres cas, l'allégement de la contrainte de rareté des ressources et le caractère substituable des réseaux rend contestable la disparité du régime des réseaux. **Des réseaux substituables devraient obéir à des régimes comparables** (pour l'exploitation du câble et du satellite, par exemple, qui doivent relever tous deux d'un régime déclaratif). De même, le régime des réseaux ne devrait plus être conditionné par le service transporté. Il en va en particulier aujourd'hui ainsi pour le câble obéissant à un régime nettement plus contraignant lorsqu'il est dédié à des services audiovisuels. Or, seul le régime des services véhiculés sur le câble doit demeurer variable (il n'est donc question d'aligner que le régime des infrastructures). Une uniformisation du régime des supports permettrait aussi d'alléger les contraintes pesant sur les opérateurs multiservices, et donc de favoriser la mise à disposition du public d'accès à des services en ligne dans des conditions attractives (accès à Internet à haut débit en particulier).

? *Le régime des services*

Il importe de veiller à la neutralité dans le traitement de services comparables ou alternatifs. Le degré de protection des usagers doit être identique, de même que le degré de contrainte pesant sur les opérateurs. Aussi, un service ne devrait bénéficier d'un traitement ni plus souple ni plus sévère qu'un service existant comparable, au seul motif qu'il est offert selon de nouvelles modalités.

Un service tout d'abord, ne doit pas obéir à un régime plus sévère qu'un autre, au seul motif qu'il est offert par un opérateur dont le métier principal est différent. Les services en ligne relèvent aujourd'hui d'un simple régime déclaratif, dont on a vu qu'il n'était pas adapté (voir *supra* quatrième partie, sur l'obligation de déclaration des services relevant de l'article 43 de la loi du 30 septembre 1986). Dans le cas par exemple d'une offre multiservices (télévision + services en lignes interactifs) proposée à l'abonné d'un bouquet numérique, il n'apparaît pas justifié d'imposer à l'opérateur des contraintes supplémentaires au seul motif que le service en ligne est offert en complément d'un autre service " principal " plus réglementé. Le même service (par exemple le téléchargement de jeux vidéo ou des services financiers en ligne) obéirait dans un cas à un régime de liberté s'il est proposé par un opérateur dont c'est l'activité principale, et dans un autre à un régime de conventionnement contraignant, s'il est l'accessoire d'un service qui relève aujourd'hui d'un tel régime. Une telle approche ne paraît pas plus fondée que celle consistant à vouloir attraire en totalité dans la sphère de l'audiovisuel des services de nature mixte. Elle ne serait justifiée que s'il est avéré que le service dit " accessoire " nécessitait un traitement comparable au service principal (notamment si le service en ligne empruntait lui aussi le spectre hertzien, dans le cas, par exemple, d'une offre numérique hertzienne terrestre).

À l'inverse, il n'apparaît pas plus justifié de soumettre à un régime allégé des services comparables à d'autres. Par souci de neutralité, il importe de ne pas chercher à réglementer spécifiquement des services au motif qu'ils sont offerts selon de nouvelles modalités (et notamment *via* Internet), et de veiller au contraire à ce que les exigences imposées à des services soient comparables s'ils sont substituables. Ainsi, le respect de la " chronologie des médias " s'impose à la vente de vidéocassettes en magasins et devrait donc aussi s'appliquer aux services interactifs de vidéo à la demande qui sont en pratique substituables .

Dans certains cas, le caractère transfrontière du réseau et la difficulté à localiser un serveur rendra toutefois difficile à l'avenir la mise en œuvre de ce principe d'égalité de traitement, si le régime des services " traditionnels " demeure en l'état. Si aujourd'hui la qualité de l'image et le débit (chargement par paquets) rendent peu attractifs le téléchargement des films en ligne, une évolution rapide est attendue. Rendue possible par la mise en place de réseaux à haut débit et par le développement de nouvelles normes d'images haute définition (les normes MPEG 4), elle devrait avoir un impact sur l'industrie des programmes. Aux États-Unis, certains acteurs de l'audiovisuel et notamment les grandes majors de Hollywood, se montrent la fois intéressées par les nouvelles perspectives qui s'offrent à eux pour valoriser leurs catalogues de programmes, mais aussi très préoccupés par les risques de contrefaçon (ce point est traité dans la troisième partie) et de perturbation des circuits d'exploitation traditionnels. Les risques sont certainement plus importants encore, dans un pays comme la France, qui doit en partie la vitalité de sa production audiovisuelle et cinématographique aux obligations pesant sur les diffuseurs établis sur son territoire, notamment par le biais de quotas de diffusion d'œuvres originales européennes et françaises. Aujourd'hui, des chaînes de télévision établies à l'étranger, et notamment en Grande Bretagne, sont reçues en France par satellite échappant à certaines obligations imposées en France aux diffuseurs pour contribuer au soutien de l'industrie des programmes et la culture européenne . L'éventualité que des diffuseurs ne soient tentés de délocaliser à l'avenir tout ou partie de leur activité à l'étranger ne peut être exclue, s'il devient possible de recevoir par différents canaux en France, et notamment *via* l'Internet, des programmes en provenance du monde entier, échappant à toute forme de contrainte réglementaire. Cette éventualité incite à **réfléchir dès aujourd'hui aux éventuelles adaptations des mécanismes existants de soutien aux industries de programmes européennes** que rendrait nécessaire un tel phénomène.

Adapter la réglementation de l'audiovisuel et des télécommunications en faisant prévaloir une distinction entre les réseaux et les contenus

Dès lors que les réseaux ne sont plus dédiés à des services particuliers et permettent tous de véhiculer tous types d'informations (voix, données, images fixes ou animées), la distinction traditionnelle entre, d'un côté, la régulation des services et des réseaux audiovisuels et, de l'autre, la régulation des services et des réseaux de télécommunications perd de sa pertinence. Une distinction nouvelle apparaît entre deux types de réglementations qui appellent des modes de régulation distincts :

– la réglementation technique et économique des réseaux qui doit être transversale dès lors qu'ils permettent la transmission de tous types d'informations ;

– la réglementation des contenus mis à la disposition du public, qui doit être variable selon les secteurs, à l'exception d'un socle minimal commun à tous les services (voir *infra*).

La régulation des contenus et services empruntant les réseaux de télécommunications, et en particulier celle des contenus audiovisuels mis à la disposition du public, doit demeurer sectorielle. Il apparaît inopportun dans ce cas, de confier à une seule autorité le soin de contrôler tous les contenus mis la disposition du public. Des services tels les forums de discussion, l'accueil de sites Web, la vente à distance, l'accès à des bases de données, la télémédecine, la téléformation, comportent une composante communication au public mais ne nécessitent pas le même traitement que la radio ou la télévision, qui demeurent des média de masse spécifiques. Ainsi, de même que le CSA ne régule pas aujourd'hui la presse ou la télématique, il paraît peu adapté de confier demain à une seule autorité le soin de contrôler les contenus audiovisuels, la publicité sur tous les supports, la presse et l'ensemble des contenus mis en ligne. Il va en revanche de soi que des services de radio ou de télévision sur Internet devront rester de la compétence de l'autorité chargée de contrôler les programmes audiovisuels. Dans le cas de l'Internet, qui ne relève pas d'une traditionnelle logique de diffusion, il semble préférable de

s'orienter vers la combinaison d'une corégulation avec les professionnels, sous le contrôle du juge, pour encadrer les services propres au réseau (voir *supra* quatrième partie, et *infra* sur l'encadrement de ces nouveaux services), et de la régulation habituelle des services traditionnels concernés .

En revanche, une même autorité pourrait assurer la régulation technique des réseaux de télécommunication, dès lors que ces réseaux véhiculent tous types de services. De même, si dans un proche avenir les acteurs de l'audiovisuel et des télécommunications, qui exerçaient à l'origine des métiers différents, offrent des services similaires et donc concurrents, le recours à des régulations économiques sectorielles séparées apparaîtra moins pertinent.

Au total, il semble donc **préférable d'écarter l'option 2 du *Livre vert* (création d'une catégorie juridique de nouveaux services) et de lui préférer l'option 1 (adaptation des législations existantes) s'agissant des services ou contenus, et l'option 3 (une législation transversale) pour ce qui concerne la réglementations technique et économique des réseaux de télécommunication**, sous réserve de maintenir un traitement spécifique pour les réseaux utilisant des ressources hertziennes.

Ces réflexions prospectives d'ordre général sur la réglementation de la communication formulées en guise de réponse au *Livre vert* de la Commission européenne sont largement conformes aux orientations privilégiées par le Gouvernement dans la réponse officielle de la France à ce document en avril 1998. Au-delà de celles-ci, le cadre juridique pourrait faire l'objet d'une adaptation plus ponctuelle à court terme, permettant d'encadrer le développement très spécifique de l'offre de nouveaux services en ligne.

Définir un cadre juridique pour les services en ligne

Définir un cadre juridique pour les prestataires de services en ligne n'est pas aisé. On a vu que sont offerts sur les réseaux des services de toutes natures : de communication au public comme de correspondance privée, gratuits (une fois l'accès au réseau payé) ou payants, " traditionnels " ou nouveaux. Ce dernier point est essentiel et il semble important de se préserver de deux tentations. La première serait de considérer tous les services interactifs comme nouveaux, la seconde serait de rejeter l'idée que des services vraiment nouveaux ne soient soumis à des obligations minimales. Les prestataires de services en ligne doivent respecter des principes généraux, la législation applicable aux services " traditionnels " qu'ils délivrent et des obligations spécifiques au titre de l'offre de services véritablement nouveaux.

Plusieurs niveaux de législation applicables aux services en ligne peuvent ainsi être distingués :

– les grands principes applicables à toute communication (ceux de la communication au public ou ceux de la correspondance privée) ;

– la législation sectorielle applicable au service qui est offert (vente à distance, publicité, télémédecine, téléphonie, télévision, etc.) ;

– le régime des opérateurs de service en ligne (code des postes et télécommunications pour les modalités d'utilisation et d'accès aux réseaux ; encadrement spécifique des services d'accès et d'hébergement).

Pour l'essentiel, le cadre juridique des services en ligne existe. Il s'agit de différentes législations sectorielles qui nécessitent parfois quelques adaptations (code de la consommation, code de la propriété intellectuelle, etc.). Au-delà du cadre existant, il apparaît souhaitable de procéder, d'une part, à la définition des grands principes applicables à toute communication au public et, d'autre part, de procéder à la définition d'exigences minimales spécifiques qui s'imposent aux

fournisseurs de services en ligne.

Les services en ligne relèvent de la législation applicable aux services " traditionnels "

Ces services sont soumis aux dispositions du code des postes et télécommunications en tant qu'ils sont des services de télécommunications.

Les services en ligne relèvent de la législation applicable aux services traditionnels.

Il n'apparaît pas souhaitable de créer une nouvelle législation pour les services accessibles *via* l'Internet (voir, *supra*, les réserves sur la création d'une catégorie de nouveaux services). Le régime de ces services doit autant qu'il est possible demeurer indépendant des nouvelles modalités d'y accéder. Il doit en revanche varier en fonction des contenus véhiculés : un service commercial devra respecter les règles de la vente à distance, une activité éditoriale doit être soumise au respect des règles qui la régissent (déontologie, responsabilité éditoriale, déclaration du directeur de la publication), un service de téléphonie respectera les obligations prévues par le code des postes et télécommunications, un service de télévision (si ce n'est pas la simple reprise d'un service déjà autorisé ou déclaré) respectera les obligations du régime le plus souple prévu par la loi (régime déclaratif et respect de certaines exigences, notamment en matière publicitaire).

Le présent rapport procède à l'examen de l'application à l'Internet d'un certain nombre de ces législations, en particulier pour ce qui concerne le commerce électronique (voir, *supra*, la deuxième partie et en particulier les développements relatifs à l'application des législations sur la publicité et sur la vente à distance). Dans certains cas, la prestation de services " traditionnels " en ligne peut rendre nécessaire des adaptations de la législation. C'est, semble-t-il, le cas pour la téléphonie vocale.

? *L'offre de service de téléphonie par des fournisseurs d'accès pourrait rendre nécessaire une adaptation du code des postes et télécommunications*

Au regard des définitions des articles L. 32-1° et L. 32-6° du code des postes et télécommunications , les services offerts par les fournisseurs d'accès à l'Internet sur les réseaux de télécommunications relèvent du régime des services de télécommunications (même si le service est de nature mixte, avec une composante service audiovisuel : voir *supra*). La fourniture de services en ligne suppose l'accès à un réseau dont les modalités sont prévues par la loi de réglementation des télécommunications. En vertu de l'article de l'article L. 34-2 : " La fourniture au public des services de télécommunications autre que le service téléphonique est libre. " Les services sont soumis à autorisation pour l'utilisation de certaines fréquences hertziennes et à un régime de déclaration auprès de l'ART lorsque le service est fourni sur des réseaux câblés. La qualification de service de télécommunications entraîne aussi l'application de dispositions qui garantissent un accès aux réseaux de télécommunications ouverts au public .

Dès lors que les services Internet empruntent des réseaux de télécommunications, l'ensemble des textes relatifs à ces derniers sont applicables, qu'il s'agisse des conditions d'établissement des réseaux (L. 33 à L. 33-4 du code des postes et télécommunications) ou des modalités de fonctionnement de ces réseaux. En particulier, si les opérateurs de réseaux dédiés à l'Internet sont soumis aux dispositions de l'article L. 33-1, les dispositions relatives à l'interconnexion seront applicables (décision de l'ART n° 97-88 du 9 avril 1997 approuvant l'offre technique et tarifaire d'interconnexion de France Télécom).

Certaines adaptations de cette législation pourraient s'avérer nécessaires, dès lors que le service de téléphonie sur Internet sera pour l'utilisateur comparable à celui dont il dispose sur les

réseaux commutés classiques. Il sera nécessaire de faire application de la législation sur la téléphonie pour permettre le **maintien d'un cadre légal assurant une concurrence loyale entre tous les fournisseurs de services de télécommunications et prenant en compte l'intérêt des utilisateurs**. Il en va notamment de l'équilibre du financement du service universel (auquel contribuent les opérateurs qui n'assument pas l'ensemble des obligations du service universel des télécommunications). Cette évolution sera rendue nécessaire si se développe en France une offre de services de téléphonie de seconde génération sur Internet, qui permette de joindre n'importe quel numéro de téléphone du réseau public commuté à partir d'un ordinateur individuel, voire d'un combiné téléphonique, la communication étant acheminée *via* l'Internet par le fournisseur d'accès à Internet. À la différence de la téléphonie de première génération, il ne s'agit donc plus de l'installation par les utilisateurs eux-mêmes de logiciels transformant, à l'insu du fournisseur d'accès et dans des conditions encore assez médiocres, la voix en données et réciproquement, mais, par les fournisseurs d'accès, d'une offre de téléphonie de qualité.

En principe, une telle offre de téléphonie devrait relever – sans qu'il soit absolument nécessaire d'adapter la définition de la téléphonie vocale donnée par l'article 1er de la directive 90/338 précitée –, de l'article L. 34-1 du code des postes et télécommunications qui prévoit un régime d'autorisation, l'obligation de contribuer au financement du service universel et, en contrepartie le droit à l'interconnexion au réseau des opérateurs (régime de l'article L. 33-1 ; en pratique, il s'agit de l'interconnection au réseau de France Télécom). Toutefois, la définition d'un service de téléphonie au public obéissant actuellement à des critères très stricts (voir *supra*), il paraît difficile en l'état de faire application de la législation aux fournisseurs d'accès. Le morcellement des acteurs sur Internet accentue les difficultés. On a vu qu'une offre est qualifiée de service téléphonique si elle répond à un certain nombre de critères (l'exploitation commerciale de l'acheminement et de la transmission de la voix en temps réel en provenance et à destination de réseaux publics commutés). Si différents acteurs assurent l'un la commutation, l'autre la transmission, un troisième l'accès par le réseau public commuté – ce qui correspond à la façon dont Internet fonctionne aujourd'hui pour la transmission de données –, il devient aisé de détourner la réglementation.

Ces difficultés préoccupent l'Autorité de réglementation des télécommunications qui estime que, si elles existaient dans le cadre de la fourniture de service téléphonique classiques, elles sont exacerbées sur Internet, compte tenu de la multiplicité des acteurs concernés. Une adaptation de la législation nationale semble donc nécessaire. Elle pourrait, le cas échéant, tendre à rendre plus attractif le statut de fournisseur de service de télécommunication n'exploitant pas de réseau, en substituant un régime déclaratif au régime d'autorisation, suivant en cela la solution retenue par plupart des autres pays européens, qui n'ont pas instauré de régime d'autorisation individuelle dans ce cas, le droit communautaire laissant aux États membre le choix pour ces opérateurs n'exploitant pas de réseau entre régime déclaratif et régime de licence. Il importerait en revanche de veiller en contrepartie au respect d'exigences essentielles (qualité et accès au service) et à la contribution financière des fournisseurs d'accès offrant un service de téléphonie vocale au service universel des télécommunications.

Définir un socle minimal d'obligations applicables aux services en ligne

? *Toute communication en ligne doit respecter des principes essentiels*

Toute communication au public doit respecter un socle minimal de principes d'intérêt général, qu'il serait souhaitable de fixer par voie législative. Certains de ces principes font l'objet de législations spécifiques, mais la vertu pédagogique d'un rappel général ne doit pas être négligée compte tenu de leur importance : la protection des mineurs ; le respect de la dignité humaine, de la vie privée et des données personnelles ; le respect de la propriété intellectuelle. Un autre principe plus spécifique pourrait utilement être fixé : l'identification de la publicité comme telle.

Par ailleurs, toute communication de nature privée est soumise aux principes de neutralité et de confidentialité du message transmis (voir *supra* sur ce point la première partie de ce rapport).

? *Créer un régime d'obligations minimales pour encadrer l'offre de services en ligne*

Au-delà du droit commun des télécommunications qui a vocation à s'appliquer, selon des modalités peu contraignantes, si les services offerts ne relèvent pas de la téléphonie vocale, l'activité des fournisseurs d'accès et d'hébergement devrait être soumise au respect d'un certain nombre d'exigences minimales. Ces exigences trouvent leur justification dans le développement de services véritablement nouveaux qui nécessitent un minimum d'encadrement. L'offre d'accès à Internet est un nouveau service. Cet accès à Internet permet ensuite de jouir de nombreux services interactifs, dont certains sont déjà " traditionnels " (accès à des bases de données, commerce électronique, téléphonie,...), d'autres véritablement sans équivalent, qui connaissent un franc succès : messagerie électronique, accès à des sites Web et à des forums de discussion.

Il est dès lors légitime d'imposer **par voie législative** le respect d'exigences spécifiques à l'offre de ces services, qui ne sont pas réglementés par ailleurs. Les activités de services en ligne doivent s'exercer librement mais il importe de veiller à ce que l'offre d'accès et l'hébergement respecte quelques exigences. Les principes suivants pourraient être retenus pour permettre notamment l'accomplissement dans de bonnes conditions des missions de la police et de la justice (voir pour plus de détails la quatrième partie de ce rapport) :

– les intermédiaires doivent être à même de fournir, en tant que de besoin, l'identité de leurs abonnés, sans pour autant être obligés de vérifier celle-ci ;

– l'hébergeur doit vérifier qu'un responsable de site a été désigné (chaque site devant porter la mention de son responsable) et être à même de fournir, en tant que de besoin, ses coordonnées ;

– les fournisseurs d'accès doivent conserver les données de connexion pendant une durée d'un an ;

– les intermédiaires sont soumis à un régime de responsabilité de droit commun, sauf en cas d'activité éditoriale (régime de responsabilité en cascade) ;

– un organisme de corégulation doit être créé ;

– le juge pénal peut ordonner de faire cesser la mise à disposition du public un message susceptible d'être constitutif d'une infraction pénale.

Conclusion

Le phénomène de convergence est encore embryonnaire. Ses conséquences restent à évaluer et les pistes dégagées dans ce rapport doivent être approfondies. Ce phénomène conduira sans nul doute à une restructuration du droit de la communication autour de concepts plus généraux et plus neutres à l'égard des technologies utilisées. L'évolution du droit communautaire dans ce domaine devra donc être suivie attentivement, en veillant à ce que les considérations d'intérêt général priment sur des logiques qui s'avèreraient exclusivement techniques ou économiques.

Annexes

Annexe 1

Résumé des propositions

Recommandations générales

• Ne pas créer un droit spécifique à Internet.

• Combiner la réglementation étatique avec l'autorégulation des acteurs.

• Développer la coopération entre États pour faire respecter le droit sur les réseaux numériques.

• Définir des orientations stratégiques communes assurant la cohérence des positions françaises dans les diverses négociations internationales concernant Internet et les réseaux numériques. Prévoir un dispositif interministériel de coordination sur ce sujet.

• Mettre en place un dispositif de veille et d'observation juridiques des réseaux numériques.

1re partie
Protéger les données personnelles et la vie privée

• Élargir le rôle de la CNIL au suivi des divers procédés d'autorégulation : labellisation des codes de conduite et de déontologie, des contrats types, information sur les dispositifs techniques, formation des utilisateurs et renforcement du *contrôle a posteriori*.

• Rechercher un équilibre entre anonymat et " traçabilité " des personnes en cas d'enquête.

• Élaborer un accord international fixant des principes déontologiques communs pour la collecte et l'utilisation des données personnelles (information de l'utilisateur sur les finalités de la collecte, droit d'opposition et de rectification, etc.).

• Lancer une étude sur la notion de personne virtuelle.

2e partie
Favoriser les échanges par une confiance accrue des acteurs

1 – Transactions électroniques et protection du consommateur

• **Lever certaines ambiguïtés relatives au régime de la publicité sur Internet :**

– veiller, lors de la transposition de la directive 97/55 sur la publicité trompeuse, à ce que les services en ligne soient couverts par le champ d'application de la législation sur le publicité trompeuse et sur la publicité comparative. Ne pas inclure les réseaux numériques dans la liste des supports sur lesquels la publicité comparative est prohibée ;

– étendre à toute communication au public l'obligation d'identification d'une publicité comme telle ;

– déterminer plus clairement l'applicabilité aux services en ligne des législations spécifiques sur la publicité ;

– encourager les initiatives des professionnels de la publicité, notamment au niveau européen, visant à adapter les pratiques publicitaires aux réseaux numériques : labels ; protection contre le " spamming " par la mise en place de listes Robinson " stop publicité ".

• **Clarifier la qualification juridique d'une transaction sur Internet :**

– une transaction relève du droit de la vente à distance. Lorsque le droit de rétractation ne s'applique pas, il faut inciter à le prévoir par voie contractuelle, et imposer que les consommateurs en soient dûment informés ;

– retenir la qualification de démarchage à titre exceptionnel (en cas de " spamming ").

• **S'assurer que les consommateurs ont bien été informés** préalablement à la prise de commande **et ont manifesté clairement leur consentement** (confirmation par courrier électronique ou " cliquage " en deux étapes).

• **Informer les consommateurs concernés dans leur langue.** Clarifier le champ d'application de la loi du 4 août 1994 relative à l'emploi de la langue française en tenant compte, pour ce qui concerne les services en ligne, de la destination des messages.

• **Assurer l'identification des professionnels sur l'Internet :**

– prévoir la possibilité, en cas d'enquête judiciaire, d'obtenir des bureaux d'enregistrement des noms de domaines les informations nécessaires à l'identification du titulaire du nom de domaine ;

– inciter les gestionnaires des registres nationaux du commerce à les mettre en ligne ;

– imposer aux sites commerciaux de faire apparaître de manière claire sur la page d'accueil, certaines mentions (nom, raison social, adresse postale de l'organisme responsable du site) ;

– encourager la mise en place de labels délivrés par des organismes professionnels ou des organisations de consommateurs. Prévoir dans les contrats types de commerce électronique des clauses d'identification de l'auteur de l'offre.

• **Encourager les professionnels à la mise en place d'instruments garantissant un respect effectif des droits du consommateur** (notamment des contrats types) et à jouer le rôle d'intermédiaire d'une transaction (relation contractuelle triangulaire entre l'acheteur, la galerie marchande et le magasin).

• **Déroger partiellement par traité aux règles de conflits de lois prévues par la convention de Rome du 19 juin 1980**, trop favorables au vendeur dans un contexte de transactions électroniques, par l'introduction d'un nouveau critère : la destination du message, déterminée par le jeu d'un faisceau d'indices. Si la transaction est précédée d'un message à destination du consommateur : c'est la loi du lieu de résidence du consommateur qui s'appliquera dans le silence du contrat, et si le contrat prévoit l'application de la loi du lieu de résidence du vendeur, le consommateur ne pourra être privé de la protection que lui assurent les lois impératives de son pays.

• **Définir dans une convention internationale un socle minimal de principes relatifs à la protection du consommateur** (informations essentielles à porter à la connaissance du consommateur), et si possible mettre en place à terme des règles de fond plus détaillées, s'inspirant de la directive européenne sur la vente à distance.

2 – La reconnaissance de la valeur juridique du document et de la signature électroniques

• **Reconnaître la valeur probatoire du message électronique authentifié par une signature fiable :**

– définir dans le code civil les fonctions d'une signature (identifier le signataire et manifester son consentement au contenu de l'acte auquel elle est attachée et aux obligations qui en découlent) et préciser les exigences (intégrité et imputabilité) qui permettent de considérer qu'une signature électronique remplit ces fonctions ;

– maintenir l'exigence des écrits sous seing privé pour les actes important (article 1341 du code civil), mais réévaluer le seuil de 5000 F exigé pour les actes civils par le décret no 80-533 du 15 juillet 1980 en compensant l'érosion monétaire et en retenant un montant compatible avec le passage à l'Euro (1000-1500 Euros, par ex.) ;

– prévoir qu'un document électronique tient lieu d'écrit sous seing privé sous certaines conditions : authentification par une signature électronique fiable et conservation durable du message sous le contrôle du signataire ;

– créer un régime de présomption légale réfragable, lié à la délivrance d'un certificat par un tiers de certification accrédité.

• **Favoriser la mise en place d'une offre de services de certification :**

– ne pas soumettre l'activité de certification à un régime de licence obligatoire, mais limiter le jeu de la présomption légale au cas où intervient un tiers de certification dûment accrédité ;

– subordonner l'accréditation (facultative) au respect d'exigences précises définies par l'État, dans le respect des orientations prévues par la directive communautaire sur la signature électronique en préparation ;

– faire délivrer les accréditations par des organismes privés offrant de fortes garanties (type COFRAC) et prévoir un système de contrôle *a posteriori*, pouvant conduire au retrait des accréditations ;

– instaurer un principe de reconnaissance mutuelle des certificateurs au plan international, en veillant au respect de la réciprocité et à l'adoption d'une approche technologiquement neutre.

3 – Les enjeux de la cryptologie

• **Assouplir les contraintes posées par la réglementation** pour l'agrément des " tiers de séquestre ", afin de permettre à un grand nombre d'organismes tels que les fournisseurs d'accès et à des administrateurs de réseau de jouer ce rôle.

• **Remplacer le régime d'autorisation préalable par une simple déclaration** pour la fourniture et l'importation de moyens de cryptologie comportant un dispositif de séquestre de clés, même pour les clés supérieures à 40 bits.

• **Constituer auprès du Premier ministre un pôle technique** doté de moyens matériels et informatiques nécessaires pour le décryptage des messages qui lui seraient transmis par les services de police ou de sécurité dans le cadre des interceptions de correspondance autorisées par la loi.

• **À plus long terme**, si la France restait le seul pays développé à pratiquer le système des " tiers de séquestre ", remplacer celui-ci par l'exigence de recouvrement de clés directement auprès de l'utilisateur.

4 – L'adaptation de la fiscalité au commerce électronique

• **Mener une étude approfondie sur l'adaptation de la fiscalité au commerce**

électronique, en concertation étroite avec les acteurs et les institutions concernées au plan national et international (Union européenne, OCDE, OMC).

• **Adapter dans la mesure du possible le régime et de la TVA :**

– pour les opérations qui donnent lieu à la livraison physique d'un bien commandé *via* Internet, renforcer les contrôles douaniers et développer de nouveaux systèmes de contrôle en liaison avec les transporteurs de fret express (conventions types au niveau communautaire). Etudier l'opportunité d'introduire une franchise sur l'importation de biens d'un faible montant ;

– qualifier le téléchargement de biens dématérialisés de prestations de service, et harmoniser les règles de territorialité prévues à l'article 9 de la sixième directive du 17 mai 1977. Prévoir que tous les services délivrés par des opérateurs établis hors de l'Union européenne seront taxés au lieu de consommation (ce qui suppose d'achever l'harmonisation des taux de TVA en Europe pour éviter des distorsions au sein de l'Union) mais qu'il leur revient seulement de désigner dans l'Union Européenne un représentant fiscal unique pour déclarer la TVA dans chacun des États membres, en appliquant les taux de TVA en vigueur dans cet État.

• **L'application du concept d'établissement stable (impôt sur les sociétés) aux serveurs Internet doit faire l'objet d'une interprétation claire et harmonisée dans le cadre de l'OCDE** (adaptation de la convention modèle), en veillant à éviter que la vente des biens immatériels échappe à toute taxation dans les pays où la marge est réalisée.

• **Évaluer les possibilités d'associer des tiers au recouvrement des taxes, ou au moins à l'effort d'identification des parties et transactions**. Etudier la possibilité de faire opérer une retenue fiscale par les intermédiaires financiers.

5 – Noms de domaine et droit des marques

• **Donner un " mandat international " au futur organisme de régulation du système des noms de domaine (DNS)** : ce mandat pourrait émaner d'une organisation internationale (UIT, OMPI) et réaffirmer certains principes : les noms de domaines sont une ressource publique limitée, qui doit être régulée par un organisme à caractère international, dans le respect du droit de la propriété industrielle.

• **Créer des nouveaux domaines génériques (gTLD)**, correspondant aux principaux secteurs de l'activité économique (" .alim ", " .fin ", etc.). Cette solution pourrait aussi s'appliquer dans le domaine français " .fr " (exemples : " .alim.fr ", " .fin.fr ", etc.)

• Résoudre les litiges entre les titulaires de noms de domaine et les titulaires des marques correspondantes par un **système de médiation et d'arbitrage en ligne**, et non par un contrôle *a priori* des justificatifs de marques du demandeur d'un nom de domaine.

• **Assouplir la " charte de nommage " du domaine français " .fr "**, en remplaçant le contrôle préalable des demandes de noms de domaine par un mécanisme d'arbitrage en ligne, soit pour l'ensemble du " .fr ", soit au moins pour un ou plusieurs sous-domaines " libres " (par exemple, " .lib.fr "). Supprimer le recours obligatoire à un prestataire technique inscrit auprès de l'AFNIC.

3e partie
Valoriser les contenus par la protection de la propriété intellectuelle

• **Faciliter l’acquisition par les employeurs des droits d’exploitation sur les œuvres des salariés**, non seulement pour les œuvres multimédia mais plus généralement pour toutes les œuvres créées dans le cadre du contrat de travail.

• À moyen terme, **lancer une réflexion plus générale sur la notion d’auteur**, notamment salarié.

• **Adapter, dans un cadre international, le régime des exceptions au droit d’auteur :**

– conserver le principe légal selon lequel la copie privée est présumée autorisée, mais permettre aux titulaires de droits de l’interdire par une mention expressse sur leur site. Les titulaires de droits qui ne s’opposeront pas à la copie privée pourront bénéficier du mécanisme légal de " rémunération pour copie privée " financée par une redevance étendue à tous les supports d’enregistrement ;

– introduire une exception en faveur de la " copie technique volatile ", faisant partie intégrante d’un procédé technique ayant pour unique finalité de permettre l’utilisation en ligne d’une œuvre, et dont l’existence doit être limitée à la durée de transmission. Envisager également une exception pour la " copie technique temporaire " faite sur les " caches " des fournisseurs d’accès, pendant la durée maximale autorisée pour chaque œuvre par le titulaire des droits, en contrepartie d’une " rémunération pour copie technique " financée par une redevance prélevée sur les abonnements des fournisseurs d’accès ;

– imposer aux responsables de sites de prévoir un dispositif technique limitant le bénéfice des exceptions aux utilisateur résidant dans le pays d’émission.

• **Définir la contrefaçon de marque sur les réseaux numériques :** poser le principe que le fait qu’un site présente un produit ou un service sous une marque qui, dans certains pays, appartient à d’autres titulaires que le responsable du site ne saurait constituer, à lui seul, une contrefaçon. Celle-ci n’est constituée que lorsqu’il y a publicité ou vente effective dans l’un des pays en cause.

• **Harmoniser les règles relatives aux conflits de lois et de juridictions en matière d’atteinte aux droits de propriété intellectuelle :** confirmer l’orientation de la jurisprudence tendant à retenir la loi ou le tribunal du (ou des) pays de réception pour la part de préjudice subi dans chacun d’entre eux. Mais donner au titulaire de droits lésé la faculté de saisir un tribunal (autre que celui du lieu d’émission), présentant le lien le plus étroit avec le préjudice, qui serait compétent pour réparer l’intégralité du préjudice subi au plan mondial, en faisant une application distributive des lois des différents pays de réception pour la part du préjudice subi dans chacun d’entre eux.

• **Renforcer la lutte contre la contrefaçon :**

– interdire et sanctionner la fabrication et la vente de tout matériel permettant, dans son usage normal, le contournement des mécanismes techniques de protection des œuvres contre les copies illicites ;

– renforcer la coopération des titulaires de droits : pour améliorer l’information du public et des responsables de sites sur les principes de la propriété intellectuelle, pour faciliter l’obtention des autorisations pour l’exploitation " en ligne " (sur un site) d’œuvres existantes et pour lutter contre la contrefaçon sur Internet ;

– limiter la responsabilité pour contrefaçon des fournisseurs d’accès et d’hébergement aux cas où ils ont connaissance du caractère contrefaisant d’un contenu et s’abstiennent de couper

préventivement l'accès au site ou à la page concerné ;

– accroître le nombre d'agents assermentés habilités à constater les contrefaçons en matière littéraire et artistique, en permettant également aux tribunaux de faire appel à eux au titre de " consultants judiciaires ". Créer une nouvelle catégorie d'agents assermentés, compétents pour constater les contrefaçons en matière de propriété industrielle ;

– donner la faculté au président du tribunal de grande instance d'ordonner, à titre conservatoire, à tout fournisseur d'accès ou d'hébergement la coupure de l'accès au contenu contrefaisant. Donner le même pouvoir au juge du fond ;

– simplifier et accélérer la procédure de l'*exequatur* permettant l'application dans le pays d'émission d'un jugement rendu dans le pays de réception, au moins pour ce qui concerne la partie du jugement prononçant l'injonction tendant à faire cesser l'émission du contenu contrefaisant vers le pays de réception (à charge pour le site d'adopter les dispositifs techniques nécessaires pour filtrer les demandes d'accès en provenance de ce pays).

4e partie
Lutter contre les contenus et comportements illicites

• **Clarifier les responsabilités :** la responsabilité éditoriale est limitée à l'activité d'édition de contenus. Pour les autres fonctions, responsabilité de droit commun.

• **Renforcer l'identification des acteurs :** suppression de la déclaration préalable de l'article 43 de la loi du 30 septembre 1986 ; obligation de fournir l'identité des abonnés aux autorités publiques dans les cas prévus par la loi ; obligation pour les fournisseurs d'accès de conserver les données de connexion pendant un an ; institution d'une sanction en cas de fausse déclaration d'identité ; obligation pour tout site de communication au public de mentionner l'identité du responsable du site.

• **Adapter la procédure judiciaire :** possibilité pour le juge d'interdire l'accès à un site ainsi que son hébergement technique, de prononcer des peines complémentaires comme l'interdiction d'avoir une page personnelle. Adaptation de la prescription de courte durée pour les infractions commises sur les réseaux. Possibilité d'ordonner la publication des jugements en ligne.

• **Créer un pôle interministériel** pour la criminalité de haute technologie : centre d'expertise commun à toutes les administrations et outil d'échanges et de discussion.

• **Renforcer et simplifier la coopération internationale en matière judiciaire :** possibilité de transmettre au sein du Conseil de l'Europe les commissions rogatoires directement de juge à juge. Poursuite des travaux communautaires dans la suite, notamment, du rapport du professeur Sieber et du plan d'action " G7/P8 ".

• **Développer l'autorégulation :** création d'un organisme privé de corégulation des réseaux, associant acteurs publics et privés. Expérimentation des divers procédés d'autorégulation.

5e partie
Adapter la réglementation de la communication à la convergence de l'informatique, de l'audiovisuel et des télécommunications

• **Ne pas remettre en cause la distinction entre communication au public et correspondance privée :**

– pour plus de clarté, substituer cependant le concept de " communication au public " à celui de " communication audiovisuelle " ;

– chercher une application combinée des législations sur l'audiovisuel et sur les télécommunications lorsque cela est nécessaire (dans le cas des services mixtes qui relèvent de ces deux régimes à la fois), plutôt que de déplacer la frontière entre les deux catégories existantes. Il n'est pas nécessaire de créer une catégorie juridique nouvelle de " nouveaux services ", coexistant avec les deux grandes catégories traditionnelles.

• Adapter à moyen terme la réglementation de la communication pour tenir compte des effets de la convergence technologique :

– tendre à terme vers plus de neutralité dans la réglementation des réseaux et des services. Face à l'allègement de la contrainte de rareté, tendre vers une uniformisation du régime des supports (sauf pour la gestion du spectre hertzien) pour favoriser notamment la mise à disposition du public le plus large d'un accès à des services en ligne dans de bonnes conditions (accès à Internet à haut débit) ;

– veiller à ce que des services équivalents ou substituables soient soumis à des contraintes réglementaires comparables, afin d'éviter toute distorsion de concurrence entre eux ;

– réfléchir à l'adaptation des dispositifs de soutien aux industries de programme, le cas échéant au niveau européen ;

– maintenir une réglementation et une régulation sectorielles des services mis à la disposition du public. S'orienter pour les services en ligne vers la combinaison d'une corégulation avec les professionnels et la régulation habituelle des services concernés. Tendre en revanche vers une régulation technique et économique des réseaux, qui soit uniforme et transversale.

• Définir un cadre juridique pour les services en ligne :

– appliquer les différentes législations sectorielles aux services en ligne en les adaptant le cas échéant ;

– adapter notamment le code des postes et télécommunications, dès lors que le service de téléphonie sur Internet sera pour l'utilisateur comparable à celui dont il dispose sur les réseaux commutés classiques. Une possibilité serait de rendre plus attractif le statut de fournisseur de service de télécommunication n'exploitant pas de réseau, en substituant un régime déclaratif au régime d'autorisation ;

– définir un socle minimal d'obligations applicables à toute communication en ligne : protection des mineurs ; respect de la dignité humaine, de la vie privée, des données personnelles et de la propriété intellectuelle ; identification d'une publicité comme telle ;

– créer un régime d'obligations minimales par voie législative, pour encadrer l'offre de services en ligne et permettre l'accomplissement dans de bonnes conditions des missions de la police et de la justice.

Annexe 2

Présentation d'Internet

L'Internet (Inter-Networks), parfois appelé " le réseau des réseaux ", est un ensemble de réseaux informatiques privés et publics qui sont interconnectés entre eux grâce à un protocole de

communication commun. Son principe a été imaginé par les milieux américains de la défense et de la recherche dans le contexte de la " guerre froide ", puis l'Internet s'est progressivement généralisé au domaine civil et commercial.

Historique

Le premier réseau de téléinformatique à grande échelle a été mis en place par le ministère américain de la défense en 1969 : il s'agit de l'ARPANET, dont le développement a été assuré par l'Advanced Research Project Agency. Ce réseau reposait sur le principe d'un maillage dépourvu de centre, ce qui devait permettre de préserver l'essentiel des données si une partie du réseau venait à être détruite dans un affrontement Est-Ouest.

Mais la connexion entre réseaux, c'est-à-dire " l'Internet " proprement dit, n'est devenue possible qu'avec la définition de normes communes, notamment le protocole de communication " TCP/IP " , qui est progressivement élaboré dans les années 1970. En 1979, le ministère américain de la défense crée l'Internet Configuration Board. Puis, en 1983, la partie militaire du réseau (MILNET) est isolée, ARPANET devenant civil, mais principalement destiné à la communication entre les établissements scientifiques. En 1990, ARPANET est intégré au réseau de la National Science Foundation qui en finance le développement jusqu'en 1995.

Deux évolutions techniques majeures permettent d'ouvrir l'Internet au grand public :

– la création, en 1992, du " world wide web (www) " développé par le CERN à Genève : il s'agit d'un système d'interface graphique, très ergonomique et très facile d'utilisation, qui permet de passer d'une page ou d'un site à un autre en " cliquant " sur un lien dit " hypertexte ". La navigation sur la " Toile " devient ainsi extrêmement aisée ;

– l'apparition, à partir de 1995, de grands réseaux privés interconnectés, qui prennent le relais du réseau de la National Science Foundation.

Les principaux acteurs de l'Internet

• **L'utilisateur ou " internaute "** consulte ou échange des informations à partir de son ordinateur, qui est connecté au serveur informatique de son " fournisseur d'accès à Internet " par une ligne téléphonique classique ou par un réseau câblé.

• Le **" fournisseur d'accès à Internet "** est un prestataire technique qui met son serveur, connecté en permanence au réseau Internet, à la disposition de ses abonnés pour leur permettre de circuler dans le réseau Internet, d'accéder aux sites et d'échanger du courrier électronique.

• Le contenu des sites du réseau Internet est élaboré par des **" éditeurs de contenus "**, qui peuvent être des entreprises de presses, des sociétés commerciales, des associations ou des individus présentant des " pages personnelles ".

• Le site est généralement hébergé sur le serveur informatique d'un prestataire technique, appelé **" fournisseur d'hébergement "** , qui permet l'accès au site depuis le réseau Internet.

• Le fonctionnement des réseaux, c'est-à-dire de l'infrastructure qui transporte l'information, est assuré par les **gestionnaires de réseaux de télécommunications**. Au plan international, l'Internet est constitué de réseaux supranationaux interconnectés privés (MCI, Sprint, AOL...). Ces grands réseaux sont eux-mêmes connectés à d'autres réseaux de moindre niveau, fournisseurs d'accès internationaux (Oléane) ou " régionaux " (RENATER en France), ainsi qu'à des réseaux " fermés " reliés à l'Internet (les Intranets, par exemple entre les différents établissements d'une entreprise).

Principes techniques

Le transport de l'information se fait, depuis la naissance de l'ARPANET en 1969, selon deux principes :

– le réseau n'est pas hiérarchisé, c'est-à-dire qu'il n'y a ni centre, ni point de passage obligé dans le cheminement de l'information ;

– les données sont regroupées et transportées par paquets (appelés " datagrammes "). Chaque paquet suit alors un cheminement différent à travers le réseau Internet, en utilisant les liaisons informatiques les moins chargées de manière à optimiser le temps de transmission.

Le transport de l'information est permis par l'usage du protocole de communication commun TCP/IP : il s'agit d'un langage numérique standardisé au niveau international, et utilisable sur tout réseau relié à l'Internet. L'identification de l'émetteur et du destinataire des données se fait par leur adresse au format IP (Internet Protocol). Il s'agit d'adresses numériques qui permettent de les localiser physiquement dans le réseau. L'attribution de ces adresses est organisée et centralisée par l'Internet Assigned Numbers Authority (IANA), qui se trouve aux États-Unis. Toutefois, les " internautes " ont la possibilité de désigner les sites qu'ils souhaitent consulter par un nom, appelé " nom de domaine " (par exemple, " sncf.fr "), plutôt que par l'adresse numérique, plus difficile à mémoriser (voir deuxième partie, chapitre 5, du rapport).

Quelques données sur la croissance d'Internet

La taille de l'Internet à un instant précis est difficile à évaluer, mais des ordres de grandeurs peuvent cependant être donnés. Le nombre d'utilisateurs de l'Internet peut être évalué entre 80 et 100 millions d'internautes en 1998 contre un million seulement en janvier 1990. Le trafic sur Internet s'accroît de 30 % par mois, 85 000 nouveaux noms de domaines étant enregistrés chaque mois .

L'Internet est resté longtemps développé essentiellement aux États-Unis. Ce déséquilibre tend néanmoins à s'amoindrir sensiblement : alors que les États-Unis représentaient plus des 2/3 des utilisateurs d'Internet en 1995, ils n'en représentaient plus que la moitié environ en avril 1997, soit 41 millions. À cette même date, le nombre d'utilisateurs d'Internet était était estimé à 11 millions au Japon, 4,7 millions en Allemagne, 2,5 millions au Royaume-Uni, 2 millions en Corée et 1,4 millions en France. Le nombre de sites rapporté au nombre d'habitant est également très variable. Il est particulièrement élevé aux États-Unis et dans les pays du Nord de l'Europe .

En ce qui concerne la France, on observe encore un certain retard en matière d'utilisation de l'Internet. En particulier, la France ne représente que 4 % du nombre de domaines en Europe, contre 36 % pour le Royaume-Uni et 21 % pour l'Allemagne . Toutefois, la croissance du nombre d'utilisateurs est de plus en plus forte : ce nombre est ainsi passé de 150 000 en 1995 à 1,4 millions en 1997. Il faut rappeler par ailleurs que le minitel équipe 25 % des foyers français, avec 15 millions d'utilisateurs. En outre, 10 000 sociétés ont déjà un serveur télématique et donc une expérience largement transposable à l'Internet.

Annexe 3

Glossaire

AFA – Association des fournisseurs d'accès à des services en ligne et à Internet

Cache –Stockage temporaire des pages les plus consultées, soit sur le serveur, soit dans la mémoire de l'ordinateur de l'utilisateur

Cookie – Petit fichier envoyé par un gestionnaire de site sur le disque dur de l'utilisateur permettant d'identifier celui-ci lors de sa connexion au site et de mémoriser celle-ci

Courrier électronique, ou mél (E-mail) – Service de messagerie électronique. (exemple d'adresse : martin.telecom.gouv.fr)

EDI – Échange de données informatisées entre les entreprises

FCC, Federal Communication Commission – Instance américaine de régulation des télécommunications et de l'audiovisuel

Firewall – Passerelle sécurisée entre le réseau local d'une entreprise et l'Internet, permettant de prévenir les éventuelles attaques de personnes extérieures à travers cet accès

FTP, File Transfer Protocol – Protocole spécifique de l'Internet pour le téléchargement des fichiers

GESTE – Groupement des éditeurs de services en ligne

HTML, Hypertext Markup Language – Langage définissant le format des informations mises sur le web, par exemple la place du texte et des images, la définition des liens hypertextes, la procédure de remplissage des formulaires...

HTTP, Hypertext Transfer Protocol – Protocole de communication client-serveur utilisé pour les échanges de données sur la toile

IAB, Internet Achitecture Board – Instance de supervision technique de l'Internet Society, qui oriente et utilise à des fins normatives les travaux effectués au sein de l'Internet Engineering Task Force. L'IETF (Internet Engineering Task Force) est subordonné à l'IAB, et fédère les groupes techniques qui développent les technologies et les protocoles de l'Internet. L'Internet Research Task Force prépare quant à lui les évolutions de long terme

IANA, Internet Assigned Number Authority – Organisme réglant et centralisant l'attribution des adresses numériques. Il a la possibilité de déléguer ses pouvoirs à des organismes locaux (RIPE NCC en Europe)

Intranet – Par opposition à l'Internet, l'Intranet désigne l'utilisation des technologies et des protocoles de l'Internet dans un milieu fermé, par exemple une entreprise qui souhaite constituer un réseau entre ses différents établissements

Internaute – Désigne un utilisateur de l'Internet

IP, adresse IP, Internet Protocol – Protocole de routage de l'Internet, qui assure l'acheminement des paquets de données (" datagrammes "). L'*adresse IP* attachée aux paquets désigne son destinataire et permet donc que le routage soit effectué

ISOC, Internet Society – Association internationale, ouverte à tous, se donnant pour mission le développement de l'Internet. Il existe un " chapitre français " de l'ISOC

Forum de discussion, Groupe de discussion, Newsgroup – Groupe d'utilisateurs d'Internet qui échangent par courrier électronique des informations (" news ") sur un même thème. Le forum peut avoir un modérateur, personne par laquelle transitent tous les messages postés au groupe et qui vérifie que le contenu du message est en rapport avec le thème du groupe. La plupart des forums de discussion n'ont pas de modérateur

Lien hypertexte – Principe qui permet, en sélectionnant un lien proposé sur une page web, de

passer instantanément à une autre page ou à un autre serveur. Ceci permet une navigation de proche en proche qui est à la base du succès du web

Liste de diffusion – Liste de participants à un groupe de discussion et de leurs adresses électroniques. Les messages envoyés à la liste sont ensuite expédiés par courrier électronique à chacun des participants qui se sont préalablement abonnés. La possibilité de s'abonner à la liste peut être ouverte à tous ou réduite à certaines catégories d'utilisateurs

Miroir – Réplication d'un site sur un autre

Moteur de recherche – Service proposé aux internautes leur permettant de trouver les sites correspondant aux mot clés qu'ils ont sélectionnés (sorte d'annuaire). Les plus connus sont Altavista, Lycos, Webcrawler, Netsearch de Netscape, et Yahoo. Ces services " indexent " les pages des différents sites, c'est-à-dire qu'ils leur associent des mots clés afin de permettre aux internautes de les localiser plus facilement

NIC, Network Information Center – Ces organismes, par délégation de l'IANA, gèrent une partie des adresses IP et les noms de domaines. Le NIC France gère les noms de domaine ayant le suffixe " .fr "

Nom de domaine – Nom attaché à un site correspondant à une adresse numérique IP (exemple : *telecom.gouv.fr*)

OMPI – Organisation mondiale de la propriété intellectuelle

PICS, Platform for Internet content selection – Système permettant la classification des contenus de l'Internet

Proxy – Serveur informatique assurant l'interface entre les abonnés du fournisseur d'accès ou l'Intranet, et le réseau Internet

Push/Pull – La technologie dite " push " consiste à fournir à l'utilisateur, directement dans sa boîte aux lettres électronique, l'information qui l'intéresse (selon les choix et les intérêts qu'il a exprimés ou en fonction de son profil comportemental). Elle s'oppose au principe dit " pull ", qui est la règle générale sur l'Internet, selon lequel c'est le consommateur qui va, de lui-même, chercher l'information sur les sites

RENATER, Réseau national de télécommunications pour la technologie, l'enseignement et la recherche – Reliant les universités et les centres de recherches français entre elles et à l'Internet à travers une infrastructure à haut débit

RIPPE NCC, Réseaux IP Européens Network Coordination Center – Associations des fournisseurs de réseaux Internet européens, attribuant notamment les adresses IP aux correspondants nationaux

Routeur – Machine informatique effectuant le routage des paquets de données à travers le réseau Internet, à l'aide de leur adresse IP

Spam/spamming – Technique de prospection de masse visant à adresser, grâce à un robot de gestion d'adresses électroniques, un même message à une liste de diffusion sans accord préalable des membres de celle-ci. Cette technique est utilisé notamment pour l'envoi de messages publicitaires (publipostage)

TCP/IP, Transmission Control Protocol over Internet Protocol – Désigne les protocoles communs de communication utilisés par l'Internet, permettant l'interconnexion généralisée entre

réseaux hétérogènes

Toile, World Wide Web, Web – Désigne l'ensemble des logiciels, protocoles, serveurs et contenus constituant le monde accessible à partir des logiciels de navigation Netscape, Internet Explorer, Mosaic... et qui permettent aux internautes d'accéder à des serveurs multimédia interactifs reliés entre eux par des liens hypertexte, en utilisant le protocole TCP/IP

UIT, Union internationale des télécommunications – Organisation spécialisée de l'ONU, située à Genève, chargée de promouvoir les services de télécommunication dans le monde

URL, Universal Ressource Locator – Syntaxe informatique du web indiquant la localisation d'une ressource ou d'une page Internet (par exemple : *www.telecom.gouv.fr/français*)

Usenet – Réseau des groupes de discussion

Annexe 4

Composition du groupe d'étude

Groupe plénier

Président

Jean-François THERY, président de la Section du rapport et des études du Conseil d'État

Rapporteur général

Isabelle FALQUE-PIERROTIN, maître des requêtes au Conseil d'État

Rapporteurs de l'étude

Olivier COURSON, maître des requêtes au Conseil d'État

Olivier JAPIOT, maître des requêtes au Conseil d'État

Membres du groupe

Guy AUBERT, conseiller d'État en service extraordinaire

Noël CHAHID NOURAI, conseiller d'État

Denis CROZE, Institut national de la propriété industrielle

Anne de la PRESLE, secrétariat général du gouvernement

Paul FLORENSON, ministère de la Culture

Bernard GONDRAN, ministère de l'Industrie

Emmanuel GUILLAUME, conseiller d'État, directeur juridique à France-Télécom

Laurent JACQUES, ministère de la Justice, direction des affaires civiles et du sceau

Daniel KAHN, avocat à la cour

Paul LAGARDE, professeur des universités, conseiller d'État en service extraordinaire

Bruno LASSERE, conseiller d'État

Bruno NEDELEC, ministère des Affaires étrangères, direction des affaires juridiques

Daniel PADOUIN, commissaire principal de police, directeur général du service d'enquête sur les fraudes aux technologies de l'information

Marcel PINET, conseiller d'État honoraire, membre de la Commission nationale de l'informatique et des libertés

Pierre SIRINELLI, professeur des universités, doyen de la faculté Jean-Monnet, Paris Sud

Sous-groupe 1 : protection de l'individu

Rapporteur du groupe

Isabelle FALQUE-PIERROTIN, maître des requêtes au Conseil d'État

Jacques CARRERE, ministère de la Justice

Sylvie CECCALDI, ministère de la Justice

Emmanuel GUILLAUME, conseiller d'État, directeur juridique à France-Télécom

Rémi HEITZ, ministère de la Justice

Jacques LOUVIER, service juridique et technique de l'information

Bruno NEDELEC, ministère des affaires étrangères, direction des affaires juridiques

Jean-Yves OLLIER, maître des requêtes, secrétaire général adjoint du Conseil d'État

Daniel PADOUIN, commissaire principal de police, direction générale du service d'enquête sur les fraudes aux technologies de l'information

Marcel PINET, conseiller d'État honoraire, membre de la Commission nationale de l'informatique et des libertés

Sous-groupe 2 : commerce électronique

Rapporteur du groupe

Olivier COURSON, maître des requêtes au Conseil d'État

Guy AUBERT, conseiller d'État en service extraordinaire

Noël CHAHID-NOURAI, conseiller d'État

Anne de la PRESLE, secrétariat général du gouvernement

Bernard GONDRAN, secrétariat d'État à l'Iindustrie

Jérôme HUET, professeur des universités

Laurent JACQUES, ministère de la Justice, direction des affaires civiles et du sceau

Daniel KAHN, avocat à la cour

Pascal LAGARDE, secrétariat d'État à l'Industrie

Francis LORENTZ, inspecteur général des finances, président EPFR

Sous-groupe 3 : propriété intellectuelle

Rapporteur du groupe

Olivier JAPIOT, maître des requêtes au Conseil d'État

Valérie-Laure BENABOU, maître de conférence de droit

Denis CROZE, Institut national de la propriété industrielle

Paul FLORENSON, ministère de la Culture

André LUCAS, professeur des universités

Hélène de MONTLUC, ministère de la Culture

Pascale de SAINTE-AGATHE, secrétariat d'État à l'Industrie

Pierre SIRINELLI, professeur des universités, doyen de la faculté Jean-Monnet, Paris Sud

Alain THRIERR, conseiller en propriété industrielle

Marie-Hélène TONNELLIER, avocat

Michel VIVANT, professeur des universités

N.B. Cette étude a également été réalisée avec le concours de Myriam PETIT, documentaliste, et de François-Xavier LANFRANCHI, stagiaire, étudiant à l'Institut d'études politiques de Paris.

Annexe 5

Liste des personnes auditionnées ou consultées

Institutions et administrations

Sénat

M. Alex TÜRK, sénateur

Autorité de régulation des télécommunications (ART)

M. Jean-Michel HUBERT, président

M. Dominique ROUX, membre du collège

M. Pierre-Alain JEANNENEY, directeur général

M. Frédéric DUAUX, chef du service international

Commission nationale de l'informatique et des libertés (CNIL)

Mme Louise CADOUX

Mme Marie GEORGES

Conseil supérieur de l'audiovisuel (CSA)

Mme Anne DURUPTY, directeur général

M. François HURARD, chef du service des programmes

Mme Laurence FRANCESCHINI, chef du service juridique

M. Sébastien CROIX, service juridique

Premier ministre

M. Francis BRUN-BUISSON, chef du service juridique et technique de l'information

M. le général DESVIGNE, chef du service central de sécurité des systèmes d'information

M. Hubert MARTY-VRAYANCE, service central de sécurité des systèmes d'information

Mme Charlotte-Marie PITRAT, commissaire du gouvernement près la CNIL

Ministère de la Justice

M. André ALBERT

M. Etienne APAIRE, juge d'instruction, tribunal de grande instance de Paris

M. François CORDIER, tribunal de grande instance de Paris, quatrième section

M. Jean-Jacques GOMEZ, premier vice-président, tribunal de grande instance de Paris

M. Dominique GUIRAND

M. Pierre-André LAGEZE

M. LECLERC, conseiller à la Cour de cassation

M. Jean-Wilfrid NOEL

Mme Florence SCHMIDT-PARISEY

Ministère de l'Intérieur

M. Denis BLANCHER, direction de la surveillance du territoire

M. Marcel VIGOUROUX, direction centrale de la Police judiciaire

Ministère des Affaires étrangères

M. Bertrand de CORDOUE, représentation permanente de la France auprès de l'Union européenne

Mme Aurélie LAPIDUS

M. Damien LORAS

M. Jean-Marie MAGNIEN

Mme Annie MARI

M. Laurent PAILLARD

M. Philippe POUZOULET, représentation permanente de la France auprès de l'Union européenne

M. Dominique ROGUEZ, conseiller commercial, ambassade de France en république fédérale d'Allemagne

Ministère de l'Économie

M. Jean JOURNET, service de la législation fiscale

M. Daniel KELLER, service de la législation fiscale

M. Olivier PERRAULT, délégué aux systèmes d'information

Direction générale de la concurrence, de la consommation et de la répression des fraudes

M. Pierre GABRIE

M. Francis AMAND

M. Joël DANGIO

M. ROCHARD

Direction générale des stratégies industrielles

M. Jean-Luc ARCHAMBAULT, directeur

M. Didier BUREAU

M. Vincent THERY

M. Lionel VODZILAWSKY

Direction des postes et télécommunications

M. Patrick de GUERRE, directeur

Mme Véronique BARRY

M. Jean-Pierre DARDAYROL, service des télécommunications

Mme Bettina MEDIONI, chef du service juridique

Ministère de la Défense

M. Bernard PREVOST, directeur général de la Gendarmerie nationale

M. FERRY, chef d'escadron, direction générale de la Gendarmerie nationale

M. RIVIERE, Institut de recherche criminelle de la Gendarmerie nationale

Centre national de la cinématographie

M. Marc TESSIER, directeur général

Mme Anne COCHARD, directeur-adjoint

Mme Paule LAPPINI, directeur adjoint (affaires européennes)

INRIA-AFNIC

M. Jean-Yves BABONNEAU

M. Christian CLAVELERA

M. Bruno KOECHELIN

Autres administrations

M. Philippe BELAVAL, directeur général de la Bibliothèque nationale de France

M. Jean-Jacques de BRESSON, président du Conseil supérieur de la télématique

M. Serge CHAMBAUD, Institut national de la propriété industrielle

Organismes internationaux

Commission européenne

D.G.III – M. Michel CATINAT – M. Dominique GONTHIER

D.G. X – M. PAULGER – Mme LABOURDETTE

D.G. XIII – M. Robert VERRUE, directeur général – M. Frans DE BRUINE, directeur – M. Richard DELMAS – M. Christopher WILKINSON

D.G. XV – M. John MOOG, directeur général – M. BORNEMAN – M. BOUHAN – M. Emmanuel CRABIT – Mme Carole CROELLA – Mme Margot FROELINGER – M. Jörg REINBOTHE – M. VAN DER VEER – Mme Birgit WEISE-MONTAG

D.G. XXI – M. Michel AUJEAN, directeur de la fiscalité indirecte

Conseil de l'Union européenne (Secrétariat général)

M. CRETIN – M. NEUMANN

CNUDCI – M. Renaud SORIEUL

OCDE – M. John DRYDEN, Mme Teresa PETERS

OMPI – M. Francis GURRY

UNESCO – M. Philippe QUEAU

Professeurs des universités

M. CATALA

M. Pierre-Yves GAUTHIER

Mme Jane GINSBURG, université de Columbia (États-Unis)

M. LE GALL

M. Xavier LINANT de BELLEFONDS

M. LEVENEUR

M. Didier TRUCHET

M. Pierre TRUDEL, laboratoire de droit public de Montréal (Canada).

Avocats

Me Michel BEJOT

Me Alain BENSOUSSAN

Me Jacques-G. BITOUN

Me CAPRIOLI

Me Olivier DEBOUZY

Me Pierre DEPREZ

Me Bernard EDELMAN

Me Vincent FAUCHOUX

Me Christiane FERAL-SCHUL

Me Maître GENON-CATALOT

Me Olivier ITEANU

Me Isabelle LEROUX

Me Jean MARTIN

Me Olivier de la MYRE MORY

Me Thierry PIETTE-COUDOL

Me Thaïma SAIMAN

Me Valérie SEDALLIAN

Me Gilles VERCKEN

Associations et organismes professionnels

Agence de protection des programmes

M. Daniel DUTHIL, président

Association des fournisseurs d'accès (AFA)

M. Christian SAPET, président de l'AFA et directeur général d'Infonie

M. Le TOQUIN

Association française des banques

M. Raymond BRONNER, conseiller juridique

AFNOR

M. Jean-Michel BORDE

Association française des bibliothécaires

Mme BELLAICHE

Association des professionnels de l'information et de la documentation

Mme Florence WILHELM, président

Association française pour le commerce et les échanges électroniques (AFCEE)

Mme Claudine SCHMUCK

Bureau de vérification de la publicité (BVP)

M. Lucien BOUIS, directeur

Mme Nathalie VARILLE, responsable du département Internet

Chambre des notaires

M. Bruno VINCENT

Chambre syndicale des producteurs exportateurs de films français

M. Pascal ROGARD, président

CNPF – COMIPI

M. Claude SAUTORY

Fédération nationale de la presse spécialisée

M. DETAILLEUR

GESTE

M. Antoine BEAUSSANT, président

GFII

M. CHAUMIER, président

GIE Carte bancaire

M. Michel ESPAGNON

GIE DYADE

M. Eric BANTEGNIE

IRIS

Mme Meryem MARZOUKI

ISOC (Internet Society)

M. Bruno OUDET, président du Chapitre français

M. Daniel KAPLAN, vice-président du Chapitre français

SACD

M. Olivier CARMET, président

Mme Nicole ZMIROU, directeur des affaires juridiques

SACEM

M. Jean-Loup TOURNIER, président

M. Thierry DESURMONT

Mme Catherine KERR-VIGNALE

SCAM

M. Laurent DUVILLIER

SELL

M. Hervé PASGRIMAUD

Syndicat national des éditeurs phonographiques

M. Hervé RONY

Syndicat des entreprises de vente par correspondance et à distance

M. Bernard SIOUFFI

Syndicat national de l'édition

M. Serge EYROLLES

Union des annonceurs

M. Alain GRANGE-CABANNE, directeur général

Union des fabricants

Mme Monique HENNERICK

W3 Consortium

M. Jean-François ABRAMATIC

Entreprises et opérateurs

AOL – M. Bertrand LE FISCHER

AT&T – M. KERKESLAGER, vice-président

Audiosoft – M. François-Xavier NUTTAL, président

Bouygues – M. Thierry MILEO, directeur stratégies et affaires extérieures – M. Nicolas

PROUTEAU

British Telecom – Mme BUISSON – M.VIVIER

BT France – M. VUILLAUME

Canal Plus – M. Marc-André FEFFER, vice-président – Mme N'GUYEN, service juridique

Cégétel – M. Jean-Pascal TRANIE – M. Maurice CAVARETTA – M. HAYWARD – Mme J. FROMERICH

Chaman – M. Denis FRIEDMAN

Columbia – Mme Valérie WIEDMER

Compagnie bancaire – M. Jean-Michel BILLAUT

Cryo – M. Philippe ULRICH

Les Echos – M. JANET, responsable de l'édition électronique

Edelweb – M. Paul-André PAYS, président

Euritis – M. Jean-François BOISSON

France Télécom Interactive – M. Yves PARFAIT

Gallimard – M. Pierre COHEN-TANUGI

Hachette-Filipacchi Grolier – M. Hervé DIGNE

Havas Edition Electronique – Mme Valérie DIAMANT-BERGER

IBM Europe – M. Arnaud BRUNET, service juridique – M. Gilles RAGUENEAU, direction des relations extérieures

Infogrames – M. Bruno BONNELL, président – M. LIORET

L'Oréal – M. José MONTEIRO – M. Georges-Edouard DIAS

Lyonnaise des eaux – M. Gérard MESTRALLET, président – M. Pierre BOURIEZ – M. Cyril DU PELOUX

Matranet – M. Fabrice BOURDEIX, directeur général adjoint

Microsoft France – M. Jean-Philippe COURTOIS, directeur général – M. Jean DEPASSE

Montparnasse Multimédia – M. CHASQUES, directeur général – Mme ANGLADE – M. Edouard MORHANGE

Netscape Communication corporation – M. Peter HARTER, Public Policy Counsel, Mrs Roberta KATZ, vice-président & general counsel

Radio France International – M. Christian CHARPY

Verisign – M. Michael S. BAUM

Experts et autres personnalités

Mme Michelle d'AURAY, ministère de l'Industrie, Canada

M. Eric BARBRY, juriste

M. Larry GERBRANDT, cabinet Paul Kagan Associates, États-Unis

M. Jack GRAY, International Writers Guilds Association

M. Pierre LEDUC, ministère de l'Industrie, Canada

Mme Frédérique OLIVIER, juriste

M. Brian WALTON, Writers Guild of America, États-Unis

M. Bertrand WARUSFEL, conseil en propriété industrielle

Personnes rencontrées lors de la mission d'étude aux États-Unis (Los Angeles/Washington) du 1er au 8 avril 1998

Congrès

House of Representatives

M. Mitch Glazier, Chief Counsel, Subcommittee on Courts and Intellectual Property, Judiciary Committee

Library of Congress

Shira Perlmutter, Register Associate for Policy and International Affairs, Copyright Office

Administrations fédérales

Federal Communications Commission

M. Mike Nelson, Director, Technology Policy

Federal Trade Commission

Commissioner Thompson

M. Liusa Rosenthal

M. Medine

Department of Commerce

Mrs Lynne Berseford, Office of Legislative and International Affairs, Patent & Trademark Office

Mrs Paula Bruening, Attorney Advisor, National Telecommunications & Information administration (NTIA)

M. James Andrew Lewis, Director, Office of Strategic Trade and Foreign Policy controls, Bureau of Export administration

Mrs Barbara Wellberry, Chair of the ITA, Special counsel for Electronic commerce

Department of Justice

Mrs Betty Chave, Senior Trial Attorney

M. Philip Reitinger, Trial Attorney

Associations

Artists Rights Foundation

M. Elliott Silverstein, President

American Intellectual Property Law Association (AIPLA)

M. Michael Kirk, Executive director

Direct Marketing Association

M. Cerasale, Senior Vice President

Information Technology Association of America

M. Jon Englund, Vice-President Software Division

Mrs Sheila O'Neill, Vice-President Global Affairs

International Intellectual Property Association

M. Steeve Metalitz

Motion Picture Asociation

M. Fritz Attaway, Senior Vice President Government Affairs

M. Axel aus der Mülhen, Copyright Attorney

The Center for Democracy & Technology

M. Daniel Weitzner, deputy Director

Entreprises

America on Line

M. Bill Burrington, Director Law & Global Public Policy

Mrs Julie Garcia, Senior Counsel

Amstrong Hish Jackoway Tyerman & Wertheimer

M. Barry Tyerman, Partner (avocat)

Microsoft Corporation

M. Mark Berejka, federal Regulatory Affairs Manager

M. Jack Krumholz, Director of Federal Government Affairs,

Sony Picture Entertainment

M. Jarid Jussim, Executive VP, Legal affairs

Ambassade de France aux États-Unis

M. Jean-François Boittin, ministre conseiller, chef des services de l'expansion économique

M. Guy Yelda, consul général à Los Angeles

M. Bruno Jactel, conseiller commercial

Mme Marie-Hélène Forget, conseiller juridique

M. Jean-Michel Costaseque, attaché télécommunications

Publications du Conseil d'État
chez le même éditeur

Collection " Études et documents du Conseil d'État "

Rapport public du Conseil d'État, 1993. Considérations générales :

Décentralisation et ordre juridique (EDCE, no 45), 1994

Rapport public du Conseil d'État, 1994. Considérations générales :

Service public, services publics : déclin ou renouveau (EDCE, no 46), 1995

Rapport public du Conseil d'État, 1995. Considérations générales :

La transparence et le secret (EDCE, no 47), 1996

Rapport public du Conseil d'État, 1996. Considérations générales :

Sur le principe d'égalité (EDCE, no 48), 1997

Rapport public du Conseil d'État, 1997. Considérations générales :

Sur le droit de la santé (EDCE, no 49), 1998

Collection " Les études du Conseil d'État "

L'aide juridique : pour un meilleur accès au droit et à la justice, 1991

Sports : pouvoir et discipline, 1991

L'urbanisme : pour un droit plus efficace, 1992

Régler autrement les conflits :

conciliation, transaction, arbitrage en matière administrative, 1993

Les pouvoirs de l'administration dans le domaine des sanctions, 1995

La responsabilité pénale des agents publics

en cas d'infractions non intentionnelles, 1996

Les groupements d’intérêt public, 1997

Rendre plus attractif le droit des fondations, 1997

Pour une meilleure transparence de l’administration, 1998

Collection " Document d’études "

Jurisprudence du Conseil d’État :

• années 1988 à 1996 (disponibles)

• année 1997 (Document d’études 6.10)

Collection " Notes et études documentaires "

Sciences de la vie – De l’éthique au droit, ND no 4855, nlle éd. 1988

Administration et nouvelles technologies de l’information

(une nécessaire adaptation du droit), ND no 4851, 1988

Le Conseil d’État, par J. Massot et J. Marimbert, ND no 4869, 1988

Les établissements publics : transformation et suppression, ND no 4876, 1989

Hors collection

La justice administrative en pratique, nlle édition, 1998