

Les difficultés d'application d'un droit en évolution

Qu'il agisse des contenus ou du « contenant », la nouvelle économie numérique s'avère donc grande utilisatrice de la propriété intellectuelle, qu'elle paraît avoir identifiée comme l'un des instruments les plus efficaces pour soutenir son développement. De cet engouement découle le nombre croissant de litiges qui font l'actualité juridique de l'Internet dans le monde entier. Mais loin d'être la preuve de difficultés insurmontables que rencontrerait la « régulation » du cyberspace, ces péripéties sont plutôt la manifestation de ce que le droit de la propriété intellectuelle est en train de faire sa propre révolution technologique et de s'adapter au nouveau contexte des réseaux et de la communication numérique. Il est naturel que l'application concrète de droits intellectuels dans un contexte aussi changeant rencontre certaines difficultés pratiques et suscite des conflits. Rien d'anormal ni de choquant, mais au contraire un contexte

favorable à l'évolution du droit, à l'émergence de nouveaux concepts et de nouvelles solutions.

Des difficultés propres aux réseaux numériques

L'utilisation des réseaux numériques pour transférer et diffuser l'information induit certaines contraintes techniques et de nouvelles pratiques. Dès lors, bien que la propriété intellectuelle s'applique sur l'Internet comme dans le monde réel, il en résulte certaines difficultés spécifiques d'application, essentiellement dues à la qualité numérique des reproductions qui peuvent être effectuées sur les réseaux et au caractère ouvert et mondial de ces derniers.

62

La copie de « qualité numérique »

Support de créations intellectuelles protégées, comme avant lui le papier ou la pellicule, l'Internet présente pourtant une particularité liée à sa nature numérique. Par principe un objet numérique peut être reproduit à l'identique par n'importe quel ordinateur, alors que la copie d'une création sur support analogique est nécessairement dégradée par rapport à l'original.

Cette différence de qualité entre la copie analogique traditionnelle et la copie numérique peut avoir de grandes conséquences s'agissant des règles juridiques applicables à l'usage des œuvres par leurs utilisateurs finaux. D'une certaine façon, la règle traditionnelle du droit d'auteur selon laquelle l'utilisateur peut procéder librement à des copies destinées à son « usage privé » découle de ce que ces copies sont restées longtemps bien différenciables de

l'original et souvent – du fait de leur moindre qualité – impropres à une commercialisation pouvant concurrencer cet original. En revanche, dès que le support devient numérique et que sa reproduction permet de constituer de nouveaux exemplaires strictement identiques à l'original, le risque de les voir concurrencer les droits du créateur augmente considérablement. C'est la raison pour laquelle notre droit de la propriété intellectuelle a – nous l'avons vu – d'ores et déjà refusé l'exception de copie privée s'agissant des logiciels.

Mais cette question a pris une acuité nouvelle avec le développement des réseaux numériques. Sur l'Internet, on cumule les avantages de la copie numérique, ceux de l'accès immédiat aux contenus numérisés et la possibilité de rediffuser soi-même les copies réalisées. Là où un simple utilisateur de logiciel ne pouvait devenir qu'un pirate de petite envergure, puisqu'il ne pouvait copier qu'un petit nombre de logiciels et généralement pas organiser une diffusion à grande échelle, l'internaute peut beaucoup plus facilement devenir un contrefacteur efficace, donc dangereux, puisqu'il peut facilement accéder à un grand nombre d'œuvres ou de logiciels, puis en diffuser les copies. Une parfaite illustration de cette démultiplication structurelle de la contrefaçon sur le Net vient de nous être donnée avec l'essor rapide de certains logiciels de rediffusion et de partage des fichiers musicaux au format MP3 ; le déjà fameux logiciel Napster, contre l'usage duquel plusieurs procès ont été menés en 2000 aux États-Unis, en est une bonne illustration. Tirant profit du succès sur le réseau de cette nouvelle norme de compression numérique – format cependant conçu pour offrir une qualité de reproduction inférieure à la qualité professionnelle

nécessaire pour la gravure des disques compact audio —, ce logiciel permet d'organiser une immense bourse d'échanges entre tous ses utilisateurs, chacun d'eux pouvant accéder via Internet aux fichiers MP3 détenus par les autres et en faire à son tour une copie. La mise en place de cet immense *juke-box* mondial a évidemment soulevé la fronde de tous les éditeurs de disques (et de nombreux musiciens) qui ont vu dans le développement de cette pratique le risque d'une organisation collective de la contrefaçon, donc un risque économique majeur pour la rémunération des auteurs et de leurs éditeurs.

La délocalisation des infractions

64

Le caractère international de l'Internet crée une seconde difficulté dans l'application des règles de propriété intellectuelle. Elle tient à la délocalisation des agissements se produisant sur les réseaux, malgré l'impression de proximité extrême que crée l'environnement « virtuel » : l'internaute qui consulte l'information, le serveur sur laquelle elle est stockée et celui qui possède des droits sur elle peuvent se trouver situés à des milliers de kilomètres les uns des autres. C'est pourquoi certains penseurs du « cyberspace » voudraient le considérer comme une nouvelle réalité indépendante du monde physique et juridiquement autonome¹. Sans aller jusque-là, il faut simplement reconnaître que le droit peut rencontrer certaines difficultés d'application pratique sur l'Internet. Car il ne suffit pas d'avoir la preuve qu'un document numérique a été reproduit ou réutilisé sans autorisation pour pouvoir tirer toutes les conséquences de cette contrefaçon. Encore faut-il que l'auteur de l'infraction soit identifiable personnellement, que l'on rassemble des preuves

de sa culpabilité, qu'une juridiction s'estime compétente pour le condamner et qu'enfin la victime puisse ensuite faire exécuter la sanction prise contre le contrefacteur, là où il se trouve.

Or il est évident qu'actuellement la réunion de l'ensemble de ces conditions est souvent difficile à réaliser, ce qui limite l'effectivité des règles de propriété intellectuelle, et plus largement de toutes les règles de droit, sur l'Internet. S'agissant des exigences d'identification et de preuve, la difficulté principale vient du caractère extrêmement ouvert de ce type de réseau numérique. Sur un réseau fermé du type réseau privé ou Intranet, l'identification des intervenants et la preuve de ce qu'ils y font sont généralement assurées par des moyens de contrôle d'accès et d'authentification. Sur l'Internet, et particulièrement sur le Web, règne au contraire aujourd'hui un large anonymat. Certes, nous avons déjà indiqué que chaque fournisseur d'informations pouvait recourir à des moyens spécifiques pour sécuriser l'accès à ses ressources ou pour obtenir la preuve de tel ou tel agissement sur le réseau. Mais la logique ouverte et non contraignante qui a fait jusqu'ici le succès du Net freine l'aspiration des fournisseurs à imposer des contraintes à l'usage de leurs services.

Quant à la question des juridictions compétentes pour trancher un litige et faire appliquer la décision prise, elle rejoint la question plus vaste des disparités juridiques entre États. Les règles applicables et les juridictions compétentes varient d'un territoire à l'autre, et le pouvoir de sanctionner et d'obliger au respect de la chose jugée demeure un attribut souverain des États. Il en va ainsi de la propriété intellectuelle. Les droits sont généralement territoriaux et leur application relève des juges de chaque

État, ce qui peut déboucher dans certains cas sur des conflits de loi ou de juridiction.

Ces disparités sont heureusement limitées par des traités internationaux (comme les conventions de Berne et de Genève en matière de droit d'auteur, ou la convention d'Union de Paris pour la propriété industrielle) ou par les efforts d'harmonisation communautaire en Europe, mais elles demeurent importantes. L'usage de l'Internet ne fait que souligner cet état de fait : à partir du moment où les parties à un litige peuvent être installées dans des États différents, le choix de la juridiction compétente pour agir et la détermination du droit applicable peuvent être difficiles. Mais l'Internet n'est pas sans faciliter les choses. En effet, en matière de contrefaçon en particulier, il est toujours possible, du fait des traités internationaux, d'agir devant le tribunal du lieu du dommage, là où la contrefaçon s'est produite. Or, l'accès à l'Internet étant mondial, on peut considérer que la contrefaçon est effective en tout point du globe, puisque la copie contrefaisante peut être consultée partout. Dès lors, la victime supposée de la contrefaçon peut généralement agir devant le tribunal de son choix et les tribunaux se considèrent facilement compétents, même s'ils n'apprécient pas toujours de la même manière l'importance du préjudice subi, donc celle de la réparation financière à accorder.

66

L'exemple des litiges relatifs aux noms de domaine

Un exemple très significatif des difficultés de propriété intellectuelle qu'engendre l'usage de l'Internet est relatif

à l'attribution des « noms de domaine * ». Ces noms qui sont employés pour identifier phonétiquement et visuellement des sites et des adresses sur le Net se retrouvent souvent en conflit avec des droits de propriété intellectuelle, notamment avec les marques.

L'organisation du nommage sur l'Internet

Dans la mesure où l'Internet n'est pas un réseau unique mais seulement une interconnexion de réseaux distincts utilisant le même standard, la question de l'identification des machines et des utilisateurs a toujours été délicate et cruciale. S'assurer que chaque ordinateur connecté à l'un des réseaux de l'Internet pouvait correspondre avec tous les autres a requis, dès l'origine, d'imposer une logique d'identification commune, quel que soit le réseau IP* considéré. Ce fut durant vingt ans le rôle d'une minuscule entité, l'*Internet Assigned Numbers Authority* (IANA), limitée à un universitaire, John Postel, l'un des fondateurs de l'Internet, et à quelques secrétaires, entité hébergée par l'Université de Caroline du Sud et ayant passé un accord technique avec l'administration fédérale américaine. S'appuyant sur trois organismes régionaux (l'APNIC pour l'Asie et l'Océanie, le RIPE NCC pour les continents européens et africains et l'ARIN pour le continent américain et l'ensemble des zones non couvertes), l'IANA a veillé à ce que chaque nouveau serveur reçoive une adresse technique unique, sous la forme d'un ensemble de chiffres, proche des numéros téléphoniques, dénommée « adresse IP* ».

67

Mais dès les débuts de l'utilisation publique de l'Internet s'imposa également la nécessité de donner aux serveurs et aux services qu'ils hébergent une dénomination facile à

utiliser. C'est pourquoi on donna aux « domaines », c'est-à-dire aux ressources d'information accessibles sur le Net, un nom composé d'une chaîne de caractères alphanumériques. Afin de distinguer les différentes catégories de ressources, chaque nom fut complété par un suffixe, dénommé en anglais *top level domain**, soit TLD.

Jusqu'à présent ces suffixes ont toujours été de deux sortes : soit national (par exemple « .fr » pour les domaines français, « .uk » pour les britanniques...), soit un des quelques suffixes génériques créés en 1983 aux États-Unis : « .com » pour les entreprises commerciales, « .edu » pour les activités d'enseignement, « .org » pour les organismes non gouvernementaux, « .mil » pour les armées américaines, « .gov » pour les administrations fédérales américaines, « .net » pour les activités liés au Net et « .int » pour les organisations internationales.

68 La réservation et l'octroi des noms de domaine dans ces différentes catégories furent confiés pour les TLD nationaux à des organismes ou associations locales (par exemple, l'Association française pour le nommage Internet, AFNIC, pour les domaines « .fr ») et pour les sept premiers TLD génériques (gTLD) à une société privée américaine, Networks Solutions Inc. Ces différents organismes appliquèrent un principe commun qui avait l'apparence de la simplicité : « premier arrivé, premier servi ».

Tout cela n'empêcha pas l'apparition de graves difficultés lorsque, à partir de 1995, les entreprises commerciales commencèrent à créer massivement sites et services sur le Net. Cela provoqua d'abord un accroissement des enregistrements de noms – avec comme corollaire les premiers litiges autour de certains noms devenus indisponibles – mais conféra surtout une nouvelle valeur

au nom de domaine : ce nom désignant un site devenait un nouveau moyen d'identification et de promotion internationale pour l'entreprise concernée, en d'autres termes, un nouvel avatar de ses propres marques. Dès lors le conflit avec les règles traditionnelles de la propriété industrielle était inévitable.

La lutte contre les *cyber-squatters*

Lorsque les internautes commencèrent à constater que les entreprises commerciales allaient mettre un point d'honneur à ouvrir des sites Web sous des noms de domaine identiques à leur raison sociale ou à l'une ou l'autre de leurs marques vedettes, certains comprirent qu'il pouvait y avoir là une source de revenus facile. Plus rapides que certaines entreprises qui n'avaient pas encore perçu l'importance de la réservation des noms de site, des internautes demandèrent l'enregistrement à leur profit de noms de domaine reproduisant de grandes marques internationales, puis contactèrent les titulaires de ces marques en leur proposant de leur transférer le droit d'usage du nom de domaine moyennant finances. On appela rapidement ces parasites d'un nouveau genre les *cyber-squatters*, et si bon nombre d'entre eux réussirent à négocier de discrètes et rémunératrices transactions avec leurs victimes, certaines entreprises ainsi rackettées entreprirent des actions administratives ou judiciaires pour se faire réattribuer les noms de domaine qui correspondaient à leurs marques. Dans certains cas la bataille fut rude et tous les procédés furent convoqués : certains *cyber-squatters* n'hésitèrent pas sur les moyens pour infléchir la détermination de leurs cibles, et firent en sorte que le

nom de domaine détourné renvoie vers le site d'une entreprise directement concurrente !

La réaction vive de grands titulaires de marques internationales fut généralement payante et, dans la plupart des États, les juridictions leur donnèrent facilement raison en considérant que l'utilisation sans autorisation par un tiers d'un signe déposé comme marque pour désigner un site Internet devait être considérée comme une contrefaçon, dès lors qu'il était possible d'accéder à ce site pirate ou parasite depuis l'un des territoires sur lesquels la marque était protégée. Une telle décision fut parfois facilitée quand la marque contrefaite pouvait être considérée comme « notoire » au sens des traités internationaux sur la propriété industrielle, c'est-à-dire comme suffisamment connue par le public pour faire l'objet d'une protection accrue, même en dehors des domaines commerciaux dans lesquels elle est usuellement utilisée.

70

De leur côté, certains organismes d'enregistrement prenant conscience de la situation adoptèrent des règles administratives préventives en vue de limiter les risques d'abus. C'est ainsi que l'AFNIC française décida de réserver la possibilité d'enregistrement des noms de domaine « .fr » aux entreprises qui pouvait justifier d'une raison sociale identique au nom qu'elles demandaient : en d'autres termes la société Flammarion pouvait obtenir un « flammarion.fr », mais non un « dominos.fr », puisque Dominos n'est qu'une marque de cet éditeur et non sa raison sociale. Ce filtrage sévère qui visait à empêcher l'appropriation frauduleuse de la raison sociale d'une entreprise française dans le sous-domaine « .fr » fut souvent critiqué comme ayant freiné l'expansion du nombre de site en « .fr » et incité un grand nombre de sites français à s'enregistrer en

« .com ». Mais ce souci de l'AFNIC et de quelques autres bureaux d'enregistrement nationaux visait bien à prévoir une parade au *cyber-squatting*, préoccupation qui commençait également à se faire jour au niveau des domaines génériques (gTLD) gérés aux États-Unis par NSI.

Après de longues négociations menées sous l'égide de l'Organisation mondiale de la propriété intellectuelle (OMPI) à Genève, il fut décidé de mettre en place une procédure administrative de règlement des litiges destinée à lutter contre les « enregistrements abusifs effectués de mauvaise foi » et de décentraliser les activités d'enregistrement des gTLD en les confiant à différentes entités locales sous le contrôle d'une nouvelle organisation pluraliste, l'*Internet Corporation for Assigned Names and Numbers* (ICANN). Celle-ci fut créée en octobre 1998 pour reprendre les missions de l'IANA et son premier travail consistait à mettre en place les nouvelles procédures de règlement de litige et à créer de nouveaux gTLD sectoriels (disponibles en 2001), pour désengorger le « .com » et réduire les risques de conflit.

71

Les conflits entre noms de domaine et marques

Si la lutte contre le *cyber-squatting* a marqué les esprits, elle ne représente pas le seul aspect de la confrontation entre droit des marques et noms de domaine. En effet, même en l'absence d'« enregistrement de mauvaise foi », l'organisation du nommage sur le Net peut susciter des conflits délicats. On peut même dire que les litiges les plus insolubles sont ceux qui opposent deux titulaires de bonne foi.

Plusieurs cas de figure peuvent se produire. Le moins difficile à appréhender est celui où un internaute de bonne

foi ayant créé un site sous un nom de domaine de son choix se voit opposer une marque identique (ou encore très proche phonétiquement ou intellectuellement). Dans cette situation, les décisions de jurisprudence donnent le plus souvent raison au titulaire de la marque car celui-ci possède un véritable droit de propriété qu'il peut opposer aux tiers, alors que l'enregistrement du nom de domaine concurrent n'est qu'une formalité technique destinée à permettre d'identifier un site sur l'Internet et ne crée aucun autre effet de droit. Mais cette supériorité juridique de la marque sur les droits découlant de l'enregistrement d'un nom de domaine Internet n'est pas totale.

72

Première difficulté, quand la marque et le site contestés sont utilisés dans deux domaines économiques différents : de quel droit le titulaire d'une marque couvrant les services de publicité (ce fut le cas dans l'affaire Alice, jugée en France en 1998-1999) pouvait-il, par exemple, s'opposer à son usage comme nom de domaine désignant un site spécialisé dans les logiciels ? Conformément au droit des marques, il ne peut pas y avoir de contrefaçon si le domaine d'utilisation du signe contesté n'est pas identique ou au minimum similaire à celui que couvre la marque : c'est pourquoi, dans l'affaire Alice précitée, l'agence de publicité requérante fut finalement déboutée de son action à l'encontre de la société informatique qui avait enregistré « alice.fr ». D'un autre côté, on comprend que le titulaire de la marque veuille obtenir le transfert du nom de domaine, car les internautes accèdent à un autre site que le sien lorsqu'ils tapent sa marque sur leur clavier, ce qui peut représenter un réel préjudice économique. La raison en est que sur l'Internet le nommage ne respecte aucun des deux principes qui limitent traditionnellement

les effets des marques : la territorialité (chaque marque est protégée dans une zone déterminée) et la spécialité (chaque marque n'est protégée que pour une ou plusieurs catégories de produits ou de services spécifiées lors de son dépôt). Ce qui dans le monde physique permet la cohabitation paisible entre différentes marques ne fonctionne plus sur le Net, où tous les sites sont accessibles du monde entier et où le premier site qui utilise un nom le monopolise techniquement sans distinction de territoire ou de secteur d'activité.

Deuxième difficulté, plus importante encore, lorsque la marque s'opposant au nom de domaine a été déposée postérieurement à l'enregistrement de celui-ci. Un premier exemple a été jugé en France en 1999 par le tribunal de grande instance du Mans (affaire Microcaz c. Oceanet). Dans cette affaire assez complexe un concours de circonstances a permis au titulaire du nom de domaine « .fr » de faire valoir une apparente antériorité dans l'usage du titre de son site sur le titulaire de la marque française qui l'attaquait, et de convaincre le juge. En conséquence, ce dernier a annulé la marque supposée postérieure, au motif que l'usage antérieur du nom de domaine pouvait constituer l'équivalent d'un nom commercial ou d'une enseigne, que le droit des marques reconnaît comme antériorité opposable à l'enregistrement d'une marque. Même si cette décision surprenante ne fait pas jurisprudence, elle montre que la marque aura de moins en moins le dernier mot à l'encontre de noms de domaine pouvant justifier d'une présence réelle et ancienne sur le Net.

Le cas de figure presque insoluble reste celui qui se produit entre deux titulaires de marques identiques, couvrant simplement des territoires ou des produits différents. Les

deux antagonistes étant alors l'un et l'autre de bonne foi et pouvant faire valoir un titre de propriété industrielle de même valeur, on comprend qu'il n'est pas facile pour les juges ou les arbitres de trancher, et aucune solution simple ne peut être réellement efficace. Faut-il reconnaître le droit au nom de domaine au titulaire de la marque la plus ancienne? Donner raison à celui dont la marque a été enregistrée pour les produits ou services les plus proches des activités de communication par des réseaux électroniques? Peut-on éviter – lorsqu'il s'agit de marques couvrant des territoires différents – que chaque juridiction nationale compétente rende un jugement favorable au titulaire dont la marque a effet sur son sol, entraînant ainsi un conflit juridique insurmontable? Le dernier rapport du Conseil d'État sur le droit de l'Internet n'hésite pas à reconnaître qu'une telle situation représente actuellement

74

« une grande source d'insécurité juridique ».

On voit donc bien qu'au-delà de la nécessaire protection des marques contre les enregistrements frauduleux effectués par les *cyber-squatters*, l'harmonisation entre droit des marques et nommage sur l'Internet va être complexe à réaliser et nécessitera sans doute la mise en œuvre de mécanismes techniques et juridiques innovants. Mais c'est ainsi que l'Internet et les nouveaux services vont obliger le droit de la propriété intellectuelle à se moderniser et à inventer des solutions, prouvant par là sa vitalité.

Les solutions qui s'élaborent

Qu'il s'agisse des risques de contrefaçon des contenus numériques en ligne ou des conflits entre noms de domaine

et marques, on voit bien que l'Internet ne méconnaît pas la propriété intellectuelle, mais que ses caractéristiques technologiques et économiques créent des situations nouvelles, auxquelles les règles traditionnelles peuvent avoir des difficultés à s'appliquer. On peut s'en inquiéter et l'on doit sûrement s'en préoccuper, mais de telles difficultés font de l'Internet un véritable « laboratoire » juridique préfigurant le droit du commerce et de la propriété dans l'économie numérique mondialisée de demain. Il est d'ores et déjà possible d'apprécier la vitalité de cette remise en cause des catégories classiques du droit de la propriété intellectuelle en étudiant les nouvelles pistes sur lesquelles travaillent juristes et praticiens du commerce électronique. Il y a sans doute là des solutions émergentes qui pourraient bien servir ultérieurement de modèles à d'autres aspects de la « gouvernance » de l'Internet.

75

Les nouvelles formes de règlement des litiges

Dans le domaine sensible des conflits entre marques et noms de domaine, la création de l'ICANN a notamment permis de mettre en place une procédure innovante de règlement précontentieux des litiges. Son principe est l'acceptation par avance du recours à l'un des organismes d'arbitrage accrédités par l'ICANN, au sein duquel un *panel* d'arbitres indépendants prend en charge l'instruction du dossier et transmet à l'autorité d'enregistrement (le *registrar* ou « registraire » dans le vocabulaire en usage) dans un délai de quelques semaines, une décision (de maintien du nom de domaine ou de son transfert) à laquelle le registraire doit se conformer.

Bien évidemment une telle procédure, qui repose sur la seule acceptation contractuelle des déposants de noms de

domaine, n'empêche aucune des deux parties en conflit de saisir un juge pour obtenir une décision judiciaire en sa faveur. Mais toute la logique du dispositif repose sur l'intérêt que peut représenter pour les deux parties de recourir à un mécanisme rapide et dont la décision est susceptible de produire ses effets au niveau mondial, plutôt que de suivre des procédures judiciaires longues, coûteuses et dont les effets seraient généralement limités aux territoires nationaux de chacune des juridictions. Le pari de l'ICANN et des organisations qui ont soutenu la mise en place de sa politique de règlement des litiges (au premier rang desquelles l'OMPI, dont le centre d'arbitrage a d'ailleurs été accrédité par l'ICANN) est le suivant : les internautes et les entreprises intéressées par l'usage du Net préféreront la commodité de la procédure en ligne et c'est ainsi qu'émergeront les prémices d'une future juridiction virtuelle de l'Internet, qui permettra de dépasser les conflits de lois nationales et les querelles territoriales.

Cette logique n'est pas limitée à la seule question de la résolution des litiges relatifs aux noms de domaine. Dès 1996 une initiative universitaire américaine créait le site *The Virtual Magistrate*, qui proposait ses services d'arbitrage pour régler les différents litiges pouvant survenir entre fournisseurs de services et internautes. Cet exemple fut notamment suivi par l'expérience du *Cybertribunal* de l'Université de Montréal en 1998-1999, dont certains responsables sont aujourd'hui parmi les membres actifs d'un autre centre de médiation et d'arbitrage en ligne accrédité par l'ICANN.

C'est dire que les difficultés d'application du droit que l'Internet crée dans certains cas – en l'occurrence, la gestion des noms de domaine, mais aussi les petits conten-

tieux entre abonnés et producteur d'un service en ligne – peuvent se révéler finalement propices à une créativité technique et juridique et à l'expérimentation de nouvelles formes de pratique du droit sur les réseaux.

La redéfinition du régime de la copie numérique

S'agissant des risques de contrefaçon induits par la diffusion numérique des contenus, l'une des questions actuellement en cours d'évolution concerne la notion de « copie à usage privé », qui constitue traditionnellement une exception au droit d'auteur. Appliquée à la diffusion de contenus sur l'Internet, cette notion peut rencontrer certaines difficultés liées aux singularités techniques des réseaux numériques.

Les modes de transmission de données sur le Net paraissent ne pas pouvoir se contenter de l'exception pour copie privée (voir p. 30) et nécessiter qu'on élargisse le champ des exceptions au droit d'auteur en leur faveur. Il s'agit essentiellement des copies qui se produisent à différents niveaux des réseaux lors de l'accès d'un internaute à un contenu en ligne.

La simple visualisation d'un contenu sur le poste de travail de l'internaute nécessite déjà qu'une copie – au moins provisoire – de ce contenu ait été effectuée : d'abord dans la mémoire vive de son ordinateur, puis, généralement, sur une partie de son disque dur dédiée à la sauvegarde transitoire des données reçues, que l'on appelle « cache ». Mais la pratique des intermédiaires de réseau (fournisseurs d'accès, hébergeurs...) conduit aussi ces derniers à pratiquer, dans le but d'accélérer les accès et le chargement des données, une copie de toutes les données consultées par leurs utilisateurs sur des serveurs

intermédiaires dénommés « serveurs *proxy** ». Or peut-on considérer que ces copies techniques, réalisées de manière transparente et invisible lors de chaque connexion, entrent toutes dans la catégorie des copies à usage privé de l'internaute et échappent donc au risque d'être taxées de contrefaçon ?

On pourrait sans doute l'admettre des copies temporaires effectuées par l'ordinateur de l'internaute — pourtant, lorsque ce dernier circule sur le Net pour des raisons professionnelles, sa navigation ne s'inscrit plus dans un contexte d'usage privé — mais pas des copies sur les serveurs *proxy*, puisqu'il s'agit bien de copies réalisées dans le cadre d'une activité de services professionnelle. Autrement dit, une stricte application des lois sur la propriété intellectuelle pourrait faire considérer comme contrefaisantes des reproductions effectuées automatiquement pour des raisons techniques. Comme il y aurait là une source d'incohérences et de conflits juridiques, il a donc été jugé préférable de faire évoluer les termes mêmes de nos lois pour considérer explicitement ces différentes formes de copies techniques comme de nouvelles exceptions au droit de l'auteur. C'est ainsi que le projet² de directive sur l'harmonisation du droit d'auteur dans la société de l'information prévoit d'instaurer une exception automatique portant sur les « actes de reproduction provisoires » dès lors qu'ils sont « transitoires ou accessoires et constituent une partie intégrante et essentielle d'un procédé technique, ayant pour unique finalité de permettre une transmission dans un réseau entre tiers par un intermédiaire, ou une utilisation licite d'une œuvre ou d'un objet protégé, et qui n'ont pas de signification économique indépendante ».

Comme nous le verrons dans le chapitre suivant, le débat sur la copie électronique à usage privé est pourtant loin d'être clos. Ainsi peut-on se demander si les facilités que procure désormais la technologie numérique pour contrôler et gérer les droits intellectuels sur l'Internet ne vont pas, en réalité, réduire à peu de chose cette exception pour usage privé que la loi préserve encore et, plus largement, toutes les exceptions qu'aux États-Unis on reconnaît au nom du *fair use*. C'est que le recours croissant aux moyens de sécurité et de traçabilité paraît devoir être une des tendances fortes de l'évolution des pratiques de propriété intellectuelle dans les prochaines années. Mais ces nouveaux instruments très efficaces auront sans doute une influence très profonde – et peut-être dangereuse – sur l'équilibre des droits intellectuels dans le nouveau cadre de l'économie numérique.

79

Le développement des moyens électroniques de protection des droits

Les technologies et les systèmes de sécurité de l'information sont l'un des domaines les plus dynamiques des nouvelles industries de la communication et des réseaux. Leur développement s'explique logiquement par les besoins nouveaux qu'a fait apparaître la communication électronique : comment s'assurer que les données échangées sont exemptes de toute manipulation (exigence d'intégrité), que leur émetteur est bien qui il prétend être (authentification de l'origine) et que, le cas échéant, elles ne sont accessibles qu'aux personnes à qui elles sont destinées (confidentialité) ?

L'industrie informatique et des télécommunications a mobilisé depuis vingt ans les mathématiciens les plus

brillants afin qu'ils développent des outils sophistiqués susceptibles de garantir aux utilisateurs le niveau de confiance dont ils ont besoin. Pour l'essentiel, ces moyens de sécurité reposent actuellement sur deux types de technologies : les technologies de cryptographie* et les technologies de marquage électronique.

La cryptographie ou science des codes secrets permet de rendre inintelligible et infalsifiable un élément de contenu numérique et de réserver aux personnes qui possèdent un élément numérique secret (une « clé ») l'accès à ce qui a été chiffré. Le principe de la cryptographie est connu depuis fort longtemps, mais c'est dans les années soixante-dix que des mathématiciens américains et, sans doute quelques années avant eux, des scientifiques britanniques, ont mis au point une technologie permettant de pratiquer la cryptographie sans avoir besoin que chaque utilisateur partage avec chacun de ses interlocuteurs un élément secret commun, obligation qui jusqu'alors limitait fortement l'expansion du système. La nouvelle technologie mise au point fut nommée « cryptographie à clé publique » (ou encore, en termes plus techniques, « cryptographie asymétrique »), dans la mesure où les utilisateurs ne partagent pas leurs éléments secrets mais se contentent d'utiliser pour communiquer avec un tiers un élément numérique public que ce tiers a préalablement diffusé à tous (sur un annuaire de messagerie électronique, par exemple). Il fut à partir de ce moment-là possible à un grand nombre de personnes de communiquer entre elles de manière sécurisée sans avoir à se plier à des procédures préalables contraignantes. C'est donc sur la base de ces systèmes à clé publique que s'est bâtie la sécurité de tous les grands réseaux ouverts :

réseaux de cartes bancaires d'abord, puis de l'Internet lui-même. Aujourd'hui, lorsqu'un internaute se connecte en mode sécurisé sur un site Web, pour lui transmettre les coordonnées de son compte ou de sa carte bancaire, il met en œuvre sans le savoir un processus d'échange de clés utilisant notamment un algorithme à clé publique.

Le marquage électronique des contenus numériques est un volet complémentaire des technologies de sécurité. L'objectif n'est pas de masquer le contenu d'une information, mais plutôt de l'accompagner par un élément permettant d'identifier de manière fiable et irréversible certaines de ses propriétés (par exemple l'origine de cette information ou encore les conditions de sa diffusion et de son utilisation). Plusieurs moyens techniques peuvent être employés pour faire en sorte que ces éléments complémentaires, qui constituent une sorte d'« étiquette électronique » et dont le contenu est généralement lié – par une fonction mathématique particulière – au message lui-même, ne puissent pas être modifiés ou retirés par des tiers. L'usage des techniques de cryptographie à clé publique peut là encore être utile, puisqu'il est possible d'effectuer, avant l'envoi du message, le chiffrement de cette « étiquette », de telle façon qu'à l'arrivée le destinataire puisse procéder à son déchiffrement et vérifier son contenu sans que des tiers aient pu durant le transport altérer celui-ci, qui était chiffré et donc inaccessible, ou le remplacer, puisqu'alors le contenu de l'étiquette de remplacement ne serait plus en rapport avec le message qu'elle était censée accompagner. Ce procédé de chiffrement, non de l'ensemble du document numérique à sécuriser, mais de la seule « étiquette électronique » qui l'accompagne, est communément appelé « signature numérique » du

document par analogie avec la signature manuelle d'un document papier, qui renseigne sur son émetteur mais permet également de vérifier son authenticité.

D'autres moyens, qui peuvent d'ailleurs se combiner avec les techniques de signature numérique, sont utilisés pour marquer (on dit aussi « tatouer ») électroniquement les contenus. Il peut s'agir notamment d'introduire dans la structure même du code informatique du document des éléments d'information, de manière à les rendre impossibles à isoler et à extraire du document (donc indélébiles), voire invisibles pour les tiers non avertis. On ne parle plus alors de cryptographie, mais de « stéganographie », la science de ce qui est invisible. Plusieurs techniques sont aujourd'hui disponibles, dont celles du *watermarking** qui permettent, en matière d'image numérisée (fixe ou animée), d'insérer dans l'image, au niveau des « pixels » qui définissent les points constituant l'image, des transformations mathématiques dont les effets sont indétectables à l'œil nu.

82

Quels que soient les moyens mis en œuvre, il est rapidement apparu que ces différents instruments pouvaient assurer la protection des droits intellectuels sur les réseaux. Prenons le cas simple d'un service de diffusion sur abonnement : pour éviter que des tiers non abonnés puissent accéder aux contenus diffusés, le fournisseur de services peut chiffrer ce qu'il diffuse et ne communiquer qu'à ses seuls abonnés la clé de déchiffrement – c'est typiquement le modèle retenu par les télévisions à péage – ou simplement mettre en place un système de contrôle d'accès rigoureux, qui empêchera l'accès de son site à toute personne ne possédant pas un « certificat numérique » approprié, à savoir une sorte de carte d'identité électronique

dont le contenu a été signé par son émetteur — par exemple, le fournisseur de services lui-même — grâce à un procédé de cryptographie à clé publique.

Mais ces moyens techniques permettent aussi de gérer les droits intellectuels dans les situations les plus courantes de la diffusion sur le Net, lors de l'accès libre et gratuit à des contenus sur le Web. Il importe alors au diffuseur et aux détenteurs des droits intellectuels sur les contenus diffusés que cette consultation libre n'entraîne pas ensuite une reproduction et une rediffusion illicite et qu'elle se limite à la simple copie à usage privé. Il peut être très utile d'associer au contenu diffusé, grâce aux techniques de marquage évoquées plus haut, un élément indélébile permettant de connaître son origine, l'identité des détenteurs des droits et, le cas échéant, les conditions auxquelles il peut être consulté et reproduit. Une telle pratique permet alors d'informer efficacement l'internaute, qui ne peut plus ignorer la limite de ses droits, mais aussi, en cas de rediffusion illicite, d'établir rapidement l'origine du contenu reproduit. Ce système d'information électronique sur les droits intellectuels a d'ores et déjà reçu sa consécration juridique puisque le traité sur le droit d'auteur signé à l'OMPI, en décembre 1996, impose à tous les États signataires de sanctionner le fait, par tout utilisateur, de « supprimer ou modifier, sans y être habilité, toute information relative au régime des droits se présentant sous forme électronique », disposition qui a été transposée dans la loi américaine en matière de *copyright* dès 1997 et qui devrait l'être également dans la prochaine directive communautaire sur le droit d'auteur.

Si l'on ajoute au tatouage et à l'authentification des contenus diffusés un mécanisme d'authentification des

utilisateurs (en leur imposant pour accéder à certains contenus de produire un « certificat électronique » établissant leur identité, ou leurs coordonnées bancaires), il est alors techniquement possible de concevoir des systèmes très efficaces de protection et de surveillance des droits intellectuels sur les réseaux numériques. Les détenteurs de droits seront alors en mesure de connaître l'identité électronique et la localisation de tous ceux qui consultent ou reproduisent leurs contenus et d'organiser éventuellement un système de paiement à l'acte, puisque les pages visualisées ou copiées seront identifiées, et que l'on pourra même débiter automatiquement le compte bancaire de l'internaute considéré ou son porte-monnaie électronique.

84

Pour peu que les diffuseurs de contenus et les industriels commercialisant les matériels et les logiciels de communication se mettent d'accord, on peut aussi prévoir que certains contenus ne puissent pas être reproduits et rediffusés, ou seulement en un nombre limité d'exemplaires. Sur des marchés particuliers, comme celui des cassettes numériques ou des DVD, des producteurs de lecteurs ont intégré des logiciels de restriction de copie capables de détecter le marquage d'une œuvre et d'en restreindre automatiquement la reproduction au-delà d'un certain nombre de copies, ou encore de dégrader progressivement la qualité technique des copies successives. Une fois de plus, les nouvelles législations en cours d'adoption vont protéger de tels dispositifs, puisque le même traité de l'OMPI de 1996 (déjà repris par la loi américaine) impose de sanctionner les actes de « neutralisation des mesures techniques efficaces qui sont mises en œuvre par les auteurs [...] et qui restreignent l'accomplissement, à

l'égard de leurs œuvres, d'actes qui ne sont pas autorisés par les auteurs concernés ».

Les fournisseurs de contenus et les industriels de la sécurité de l'information travaillent donc à intégrer tous ces moyens de suivi et de gestion électronique des droits intellectuels dans de véritables systèmes intégrés, appelés en anglais ECMS, *Electronic Copyright Management Systems*, ou encore DRM, *Digital Rights Management*. La seule limite au développement à grande échelle de ces dispositifs de protection électronique des droits intellectuels réside dans la nécessité de les normaliser au niveau international, afin qu'ils soient mis en œuvre et reconnus à tous les niveaux de la chaîne de traitement et de diffusion de l'information : création des contenus (logiciels de traitement de texte, de PAO, de création de sites...), mise en ligne (logiciels serveurs), diffusion et consultation (navigateurs Web, logiciels de messagerie, de téléchargement* de fichiers), systèmes de paiement électronique, de contrôle d'accès...

85

Mais d'autres conséquences doivent être étudiées et prises en compte avant le déploiement de ces systèmes. Comme nous allons le voir, la normalisation au niveau international d'un ou de plusieurs systèmes de gestion électronique des droits intellectuels pourrait conduire à la fois à changer radicalement la nature du marché de l'information et de la culture et à créer des risques nouveaux pour la protection de la vie privée et des libertés publiques dans la future société numérique. La marchandisation généralisée de la communication et de la consommation de l'information, y compris s'agissant de contenus aujourd'hui non protégés par la propriété intellectuelle, pourrait être une conséquence extrême d'une certaine politique de

protection électronique des droits. La surveillance rigoureuse qu'imposerait une gestion automatisée et généralisée de chaque utilisation des contenus numériques pourrait conduire à ce que tout internaute soit en permanence identifié et suivi dans les moindres aspects de sa circulation sur les réseaux.

C'est en cela que les préoccupations juridiques et techniques relatives au respect et à l'adaptation des règles de propriété intellectuelle sur l'Internet débouchent en réalité sur un débat plus fondamental, mettant en jeu les nouveaux paradigmes qui gouverneront l'économie de l'information et la société numérique. Entre un éventuel dépérissement mondial des monopoles intellectuels au profit d'une libre économie de l'information et le souci légitime de fonder sur la propriété intellectuelle la rentabilité des investissements nécessaires aux industries des contenus et de la communication, s'esquissent les enjeux politiques, sociaux et culturels d'une nouvelle civilisation.