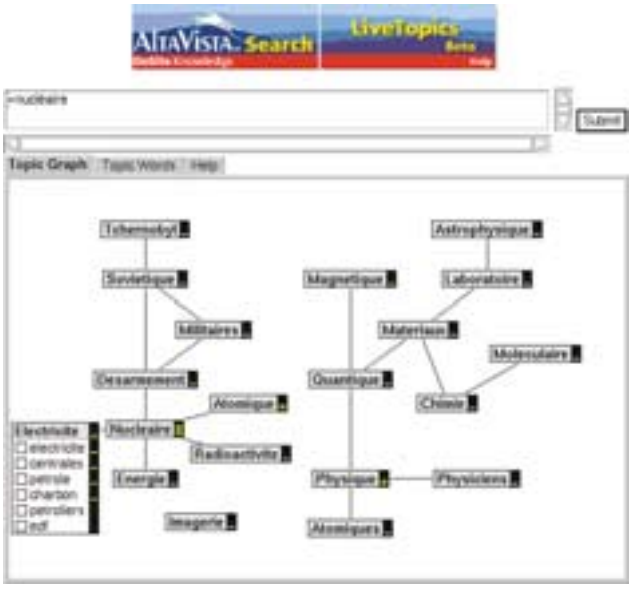
Cartographie thématique

Dans une approche différente de celle des programmes qui aident à visualiser la classification *a priori* des thèmes d'une recherche, tels ceux décrits dans cet article, nous avons conçu un logiciel, nommé *LiveTopics*, qui propose à l'utilisateur, submergé par l'avalanche de documents renvoyés par sa requête, une cartographie thématique et dynamique des documents. À l'aide de cette carte, l'utilisateur appréhende rapidement le contenu des documents. En incluant ou en excluant certains des thèmes de la carte, il affine sa recherche.

Ce logiciel est aujourd'hui proposé sur le moteur de recherche *AltaVista* de la Société *Digital Equipment*. Lorsque l'utilisateur reçoit plus d'une vingtaine de réponses, il peut demander à visualiser une synthèse thématique de l'ensemble des réponses. Par exemple, la recherche du mot «nucléaire» renvoie des thèmes variés où l'on retrouve ce qui concerne la physique, l'énergie, l'électricité et l'astrophysique *(voir la figure)*. L'utilisateur passe ensuite en revue chacun des thèmes et les mots qui s'y rapportent. Il peut alors modifier sa requête d'un simple clic de la souris, en incluant ou en excluant certains mots, et lancer une nouvelle recherche qui pourra de nouveau donner lieu à une analyse thématique.

Fondé sur une analyse statistique du texte intégral des documents, *LiveTopics* n'utilise aucune analyse linguistique ni sémantique, ce qui rend possible l'analyse de documents indépendamment de leur langue, pourvu que cette langue s'écrive avec des caractères latins. Une évolution vers des caractères d'autres langues est à l'étude, ainsi qu'une version de la technique adaptée au monde des réseaux d'entreprises.

François BOURDONCLE, École des mines de Paris



Dans le moteur de recherche *AltaVista* (http://www.altavista.digital.com/), la demande «nucléaire» renvoie 11 877 documents. Lorsque on lance *Live Topics*, une carte des thèmes apparaît. À gauche, on trouve le thème *Nucléaire* relié à *Énergie*, *Électricité*, *Radioactivité*, mais aussi le thème du désarmement, lié à *Soviétique*, *Tchernobyl* et *Militaires*. À droite de la carte apparaissent plutôt les thèmes liés à la recherche : *Quantique*, *Magnétique*, *Physique*, *Chimie*, etc. Notez le thème *Imagerie* qui est isolé du reste. Sur l'écran de droite, on trouve la liste des mots associés aux thèmes de la demande «nucléaire». On peut les exclure ou les inclure pour une nouvelle recherche.

Le groupement de documents n'est pas une panacée, car il n'explique pas comment les documents sont trouvés. En revanche, quand le formulaire d'entrée encourage les utilisateurs à décomposer leurs demandes en plusieurs groupes de mots clés apparentés, une interface graphique peut indiquer les voies de recherche obtenues et les endroits où elles sont apparues dans les documents trouvés. Si tous les sujets se retrouvent au même endroit, le document a plus de chances d'être pertinent, et le programme lui accorde une priorité supérieure. Alice peut n'avoir aucune idée précise des sujets qui doivent apparaître dans le document ou du degré de proximité qui doit les unir, mais elle a des chances de reconnaître ce qu'elle désire lorsqu'elle le voit et peut alors affiner sa demande. Cette technique, que j'ai nommée *TileBars*, peut guider les utilisateurs lorsqu'ils choisissent les documents qu'ils souhaitent examiner et les conduit plus rapidement aux endroits les plus pertinents.

L'étude de ces nouvelles interfaces utilisateur et techniques d'analyse de texte commence seulement. D'autres techniques combinent méthodes statistiques et empirisme pour résumer automatiquement des documents et les insérer dans un ensemble de catégories déjà existant. Elles proposent des synonymes pour des mots clés et répondent à des questions simples.

Marti HEARST est informaticien au Centre de recherche *Xerox*, à Palo Alto.

Ramana RAO, Jan O. PEDERSEN, Marti A. HEARST et Jock D. MACKINLAY et al., *Rich Interaction in the Digital Library*, in *Communications of the ACM*, vol. 38, n° 4, pp. 29-39, avril 1995.

Stuart K. CARD, George G. ROBERTSON et William YORK, *The WebBook and the Web Forager : An Information Workspace for the World-Wide Web*, in *Proceedings of the ACM/SIGHI Conference on Human Factors in Computing Systems*, Vancouver, avril 1996. Présent sur le réseau à l'adresse : http: / / www.acm.org / sigs / sigchi / chi96 / proceedings / papers / Card / skc1txt.html

Les systèmes sécurisés

MARK STEFIK

La mise en place de dispositifs de protection numérique des droits d'auteur permettra aux auteurs de publier sereinement leurs œuvres sur l'Internet.

La banalisation de l'informatique a rapidement conduit les utilisateurs d'ordinateurs à penser que toutes les œuvres numériques – les programmes informatiques, les livres, les revues, la musique et la vidéo – pouvaient être copiées. Certaines figures de l'informatique ont même proclamé que la simplicité de la reproduction marquait la fin des droits d'auteur : «l'information veut être libre», disaient-ils. Autrement dit, il serait impossible de s'opposer à la diffusion de l'information, et tout ce qui peut s'exprimer sous forme de bits pourrait être impunément reproduit.

Cette idée est à la base de la création du réseau Internet : dans la nouvelle ère numérique où nous entrons, l'accès à l'information numérisée serait universel, et l'œuvre de n'importe quel auteur devrait être accessible à n'importe qui, n'importe où et n'importe quand.

Toutefois, par expérience, les utilisateurs du réseau savent que ce dernier ne contient pas de grandes œuvres ni d'informations capitales ; ce qu'on y trouve est souvent de faible valeur. La raison en est que les auteurs ou les éditeurs ne peuvent vivre en faisant cadeau de leur travail. Il suffit aujourd'hui de taper quelques touches d'un clavier pour copier un paragraphe, une revue, un livre, voire l'œuvre d'une vie. La duplication incontrôlée a tant modifié l'équilibre du contrat social entre les créateurs et les consommateurs d'œuvres numériques que la plupart des éditeurs et des auteurs refusent de laisser circuler le meilleur de leurs travaux sous forme numérique.

Toutefois, en coulisse, la technique se prépare à modifier cet équilibre. Au cours des toutes dernières années, plusieurs sociétés, telles *Folio*, *IBM*, *Intertrust*, *NetRights*, *Xerox* ou *Wave Systems*, ont mis au point des programmes et des

Jeff Brice

machines qui permettent aux éditeurs de spécifier les modalités d'utilisation des œuvres numériques et de contrôler leur utilisation. Certains législateurs pensent que ce changement est si radical que les éditeurs auront un pouvoir excessif, et que les consommateurs et les bibliothécaires seront lésés.

Pourtant les besoins des consommateurs seront satisfaits, même avec les nouveaux systèmes : la technique introduisant davantage de sécurité, des œuvres de meilleure qualité pourront être proposées sur le réseau. Bien protégés, des auteurs célèbres auront peut-être envie de publier directement sur le réseau. L'accès à l'information ne sera peut-être pas gratuit, mais il pourrait être bien moins onéreux qu'aujourd'hui, car les coûts d'impression et de distribution sont considérablement réduits par la mise des informations sur le réseau ; les éditeurs pourraient répercuter ces économies aux consommateurs.

Les systèmes «sécurisés» sont la clé de cette mutation technique : ce sont des machines et des programmes dont le fonctionnement se conforme à des règles, nommées droits d'usage, qui définissent le coût d'accès aux œuvres numérisées et les modalités de leur utilisation. Un ordinateur sécurisé, par exemple, refuserait de faire des copies non autorisées ou de transmettre des documents sonores ou graphiques à un utilisateur qui n'aurait pas payé pour les acquérir.

Les types de systèmes sécurisés sont variés : des lecteurs sécurisés peuvent lire des livres numérisés, des magnétophones et des magnétoscopes sécurisés peuvent lire des enregistrements audio et vidéo, des imprimantes sécurisées peuvent faire des copies contenant des signes (des «filigranes») qui indiquent le droit d'utilisation et de reproduction accordé, et des serveurs sécurisés peuvent se charger de vendre des œuvres numériques sur l'Internet. Bien que complexes, les techniques d'élaboration des systèmes sécurisés ont une fonction simple : elles permettent aux éditeurs de distribuer leurs produits – sous forme cryptée –, de sorte que ceux-ci ne soient affichés ou imprimés que par des machines sécurisées. Les premiers systèmes sécurisés équiperaient des imprimantes ou des lecteurs numériques de poche – avec un surcoût pour l'utilisateur, qui accéderait alors à des documents bien plus intéressants qu'aujourd'hui. Puis, comme toujours, l'avènement des nouvelles techniques en ferait chuter les prix. Naturellement les éditeurs pourront encore donner gratuitement l'accès à certaines œuvres : les serveurs sécurisés les transmettront alors sans imposer les protocoles spécifiques des œuvres protégées.

Comment les systèmes sécurisés savent-ils les règles qui doivent être respectées ? La Société *Xerox* et d'autres ont tenté de décrire les montants des droits et les modalités précises d'utilisation dans un langage formel qui sera interprété par les systèmes sécurisés. Le recours à un tel langage est essentiel pour l'édition électronique : les vendeurs et les acheteurs ne pourront négocier et parvenir à des accords que si l'ensemble des actions autorisées ou interdites est explicitement défini. Les droits numériques sont de plusieurs types. Les droits de transport concer-

nent l'autorisation de copier, de transférer ou de charger. Les droits d'interprétation concernent l'autorisation de jouer et d'imprimer. Les droits de reproduction concernent l'extraction d'information, l'édition de cette information et son insertion dans d'autres publications. D'autres droits régissent la création et l'utilisation des copies de sauvegarde.

La sécurisation à l'œuvre

Les exigences de sécurité variant avec la nature des œuvres intellectuelles, les systèmes sécurisés permettent aux éditeurs de définir le degré de maîtrise qu'ils veulent conserver sur les documents écrits, sonores ou vidéo. Les œuvres numériques les plus précieuses peuvent être protégées par des systèmes qui détectent toute tentative de déverrouillage, déclenchent alors des alarmes et effacent l'information abusivement utilisée. À un niveau inférieur, les systèmes sécurisés pourraient seulement éviter les tentatives d'effraction banales en demandant un mot de passe. À un niveau encore plus élémentaire, ils marqueraient seulement les œuvres d'une signature numérique, de sorte le propriétaire soit associé à son œuvre de façon indélébile (certains logiciels de manipulation d'images apposent déjà ce type de filigrane numérique).

La plupart des ordinateurs sécurisés savent reconnaître un autre système sécurisé, faire respecter les droits d'usage et présenter les œuvres de sorte qu'elles ne puissent être copiées exactement ou qu'elles contiennent constamment la marque de leur origine. Pour exécuter les transactions en toute sécurité, deux systèmes sécurisés utilisent un canal de communications, tel le réseau Internet, pour s'échanger des preuves de leurs identités. On peut ensuite gérer les communications sur un canal sécurisé à l'aide d'un cryptage et de ce que l'on nomme un protocole d'authentification.

Par exemple, si un ordinateur *A* veut communiquer avec un ordinateur *B*, il doit prouver à *B* qu'il est un système sécurisé et que son identité est bien celle qu'il déclare sienne. L'interaction commence alors par l'envoi, de *A* à *B*, d'un certificat numérique qui confirme qu'il est enregistré en tant que système sécurisé. L'ordinateur *B* déchiffre alors ce certificat, mais il doit s'assurer que *A* est bien celui que le certificat atteste, et qu'il n'utilise pas frauduleusement un certificat volé : aussi, l'ordinateur *B* compose une chaîne de nombres aléatoires, qu'il chiffre à l'aide d'une clé publique contenue dans le certificat numérique envoyé par *A*. La clé publique permet à *B* d'envoyer des messages que seul *A* comprend lorsqu'il les déchiffre avec sa propre clé.

A doit ainsi déchiffrer le message renvoyé par *B* et retourner un message non chiffré contenant la chaîne aléatoire sélectionnée. Si la chaîne renvoyée en clair est bien celle qui avait été envoyée par *B*, ce dernier sait qu'il est en communication avec *A*, car seul *A* pouvait déchiffrer le message avec sa clé privée. Quelques étapes supplémentaires permettent ensuite aux deux ordinateurs d'effectuer la transaction prévue, telle que le transfert d'un livre sous une forme numérique.

Les systèmes sécurisés n'utilisent pas tous un protocole d'authentification, mais la plupart échangent des œuvres sous une forme cryptée. Ils peuvent aussi comporter d'autres systèmes de sécurité : des horloges infalsifiables qui empêchent un utilisateur d'exercer des droits périmés ; des mémoires inviolables qui enregistrent les opérations financières ; des connexions permanentes avec un bureau central lors des transactions.

Les systèmes sécurisés peuvent placer des filigranes d'identification qui permettront de localiser des copies ou des modifications non autorisées. Ces filigranes enregistrent la désignation de l'œuvre, le nom de l'acheteur et le code des appareils sur lesquels l'œuvre est utilisée. Dissimulée dans les blancs d'un texte, une telle information ne gênerait pas les utilisateurs honnêtes, mais elle ne pourrait être effacée par les fraudeurs.

Les éditeurs devraient continuer à surveiller la diffusion non autorisée de leurs œuvres, car on pourra toujours photocopier une page que l'on aura imprimée, ou filmer un écran d'ordinateur à l'aide d'une caméra vidéo. En revanche, les systèmes sécurisés empêchent la diffusion à grande échelle de copies parfaites des originaux numériques. En outre, certains filigranes permettront de suivre à la trace les copies piratées.

Grâce à ces systèmes, les pratiques commerciales de l'édition numérique ne devraient guère différer de celles de la diffusion des œuvres imprimées. Supposez que Christian veuille acheter un livre numérique proposé par un éditeur du réseau Internet. La copie du livre résulte d'une transaction entre le système du vendeur et l'ordinateur de Christian ; lors de la transaction, Christian doit notamment utiliser sa carte de crédit ou son argent numérique pour payer l'exemplaire du livre qu'il lira sur son ordi-

Virgin Records, Jason Goltz

1. ÉCOUTEZ AVANT D'ACHETER! Cette technique de vente pratiquée dans les magasins de disques pourrait apparaître sur le réseau Internet, grâce aux systèmes sécurisés, qui permettent de «tester» les œuvres numériques avant de les acheter.

nateur personnel ou sur tout autre dispositif de consultation. Toute la transaction, naturellement, est précédée d'un échange d'informations qui garantit au vendeur que la machine de Christian est sécurisée.

Applications des droits d'usage

Christian peut offrir son livre numérique comme il le ferait avec un livre papier : si son ami Jean-Baptiste lui demande le livre, Christian lui cède gratuitement ses droits, mais, à la fin de la transaction entre Christian et Jean-Baptiste, le livre se trouve sur le lecteur de ce dernier et il n'est plus sur celui de Christian. Jean-Baptiste peut alors lire le livre, et Christian ne le peut plus. Ainsi le nombre total d'exemplaires n'est pas modifié par le transfert ; les ordinateurs de Christian et de Jean-Baptiste, après avoir lu les droits insérés dans le fichier contenant le livre, effectuent le transfert sans que les utilisateurs interviennent.

Christian peut également prêter un livre à un ami. Si Raphaël veut lui emprunter un livre pour une semaine, Christian transfère le livre sur l'ordinateur de Raphaël, mais, tant que le livre est prêté, Christian n'y a pas accès. Une fois la semaine écoulée, l'ordinateur de Raphaël désactive la copie du livre, et celui de Christian récupère le droit d'utiliser le livre. Sans la moindre intervention des deux amis, le livre a été «rendu». Le droit de prêt est une clause essentielle à la constitution de bibliothèques numériques.

Les droits d'usage peuvent s'appliquer à la lecture des œuvres, à leur impression ou à la création d'œuvres dérivées. Certains droits peuvent être gratuits, et d'autres non, selon les volontés des auteurs et des éditeurs. Pour certaines œuvres, l'éditeur peut autoriser la copie, mais faire payer la lecture. Les droits peuvent être limités dans le temps ou dans l'usage ; ils peuvent concerner uniquement l'acquisition de l'ouvrage ou bien s'appliquer à chaque utilisation. L'éditeur peut faire des ristournes, des soldes, accorder des utilisations gratuites. Il peut limiter la diffusion aux personnes appartenant à des groupes, tels les membres d'un cercle de lecture, des personnes d'une classe d'âge ou d'un pays particulier.

Les systèmes sécurisés peuvent aussi respecter les clauses qui sont aujourd'hui en vigueur dans les bibliothèques et dans quelques autres institutions, autorisant, par exemple, un nombre raisonnable de copies ou de citations. Certaines catégories professionnelles – les bibliothécaires, les chercheurs, les enseignants – pourraient acquérir des licences leur permettant de faire gratuitement ou à prix réduit un certain nombre de copies d'une œuvre, à condition de respecter les droits d'auteur. Pour remédier aux copies illégales, on pourrait créer des caisses de compensation qui dédommageraient les éditeurs des manques à gagner.

Quels avantages les systèmes sécurisés procureront-ils aux utilisateurs? Pourquoi ces derniers devraient-ils accepter un système ne leur offrant pas, c'est le moins qu'on puisse dire, un contrôle absolu sur le matériel et les données en leur possession? Pourquoi devraient-ils payer alors qu'ils pourraient avoir tout gratuit? Parce que, si les droits de propriété intellectuelle ne sont pas respectés, les grandes œuvres ne seront jamais proposées sous forme numérique, ni gratuitement ni à titre

TRANSFERT

PRÊT

Bryan Christie

2. LE TRANSFERT D'UNE ŒUVRE NUMÉRIQUE d'un système sécurisé à un autre ressemble à un transfert d'argent entre deux comptes bancaires. L'argent ne peut se trouver simultanément sur les deux comptes. Les droits de propriété distinguent le droit de copier une œuvre numérique (ce qui accroît le nombre d'exemplaires) et le droit de transférer cette œuvre (ce qui conserve le nombre d'exemplaires). La copie d'une œuvre exige ordinairement une rémunération, tandis que son transfert est gratuit. Le prêt d'une œuvre numérique est une autre transaction, distincte de la copie et du transfert. Il est analogue au prêt d'un livre : il accorde temporairement la jouissance de l'œuvre à une autre personne ; le propriétaire de l'œuvre ne peut l'utiliser tant qu'elle est prêtée.

```
(Work:  (Rights-Language-Version: 1.06)
        (Description: "Title: 'Peter Atkins - Chaleur et désordre'
                Copyright 1994  Pour la Science")
        (Work-ID: "Vanity-Press-Registry-lkjdf98734")
        (Owner: (Certificate:
                        (Authority: "Centre français
                                du copyright")
                        (ID: "Pour la Science")))
(Rights-Group: "Regular"
(Bundle:
                (Fee:   (To: "123456789")  (House: "Visa"))
                (Access: (Security-Level: 2)) )
(Copy: (Fee:   (Per-Use: 5)))
(Transfer: )
(Play: )
(Print:
        (Fee: Per-Use: 10))
                (Printer:
                        (Certificate:
                                (Authority: "DPT"
                                (Type: "TrustedPrinter-6")))
        (Watermark:
                (Watermark-Str: "Title: 'Peter Atkins - Chaleur
                                et désordre'
                                Copyright 1994 by Pour la Science.
                                All Rights Reserved.")
                (Watermark-Tokens: user-id institution-location
                                render-name render-location
                                render-time) )))
```

Identification de l'œuvre : Peter Atkins Chaleur et désordre Pour la Science

Droits de copie, de transfert, d'utilisation et d'impression

Information pour suivre une œuvre

Jennifer C. Christiansen

3. LES DROITS D'USAGE, qui définissent les modalités de jouissance d'un livre numérique – ici, *Chaleur et désordre*, de Peter Atkins – protégé par un système sécurisé, sont écrits dans un langage interprétable par les ordinateurs sécurisés.

payant. Les systèmes sécurisés pallient le manque de contrôle en vigueur sur le réseau Internet. Ils permettent l'accès à des bibliothèques, mais aussi à des librairies, à des kiosques, à des cinémas, à des discothèques et à d'autres services dans le domaine de l'information numérique. Ils facilitent l'accès, en tout point du Globe et 24 heures sur 24, à des romans, à des films ou à des musiques de qualité. Mieux encore, cette approche technique de la protection des auteurs et des éditeurs pourrait éviter une législation qui risquerait d'asphyxier la diffusion numérique.

La mise en place de cette protection exigera des travaux techniques et des discussions commerciales : les systèmes sécurisés devront laisser les utilisateurs accéder facilement aux services, et les éditeurs devront imaginer des mesures garantissant la confidentialité des informations recueillies sur les utilisateurs. Le recours aux systèmes sécurisés suppose également que ce seront les ventes directes, et non la publicité, qui paieront la diffusion des œuvres digitales. La publicité ne prédominera probablement que pour les ouvrages grand public. En protégeant les droits d'auteur, les systèmes sécurisés permettront l'épanouissement de l'édition spécialisée : comparez, par exemple, les diverses collections de livres dans une bibliothèque et la relative indigence des programmes de télévision.

La compétitivité du marché est l'obstacle le plus important à l'instauration d'une protection des œuvres numériques. Plusieurs sociétés testent aujourd'hui des systèmes et des logiciels sécurisés, mais, à quelques exceptions près, ces programmes sont incompatibles, et leur usage n'est pas toujours autorisé. Si la technique peut déjà créer l'infrastructure du commerce numérique, les divers protagonistes de ce secteur, des acheteurs aux vendeurs en passant par les bibliothécaires et les législateurs, n'en retireront de grands bénéfices que s'ils acceptent de travailler ensemble.

Mark STEFIK est directeur de recherches au Centre de recherches *Xerox*, à Palo Alto.

Ann OKERSON, *Les droits d'auteurs des œuvres numériques*, in *Pour la Science*, septembre 1996.

Forum on Technology-Based Intellectual Property Management : Electronic Commerce for Content, in *Interactive Multimedia News* (numéro spécial), sous la direction de Brian Kahin et Kate Arms, vol. 2, août 1996.

Mark STEFIK, *Letting Loose the Light : Igniting Commerce in Electronic Publication*, in *Internet Dreams : Archetypes, Myths and Metaphors*, sous la direction de Mark Stefik, MIT Press, 1996.

Transferts rapides

JACQUES DUPRAZ

L'ATM est un mode de transfert rapide d'informations numériques qui conserve l'intégrité des messages quand ils transitent sur un réseau de télécommunications. Sera-t-il utilisé sur l'Internet ?

Ceux qui utilisent le réseau mondial savent combien le chargement des pages qui contiennent des images ou des films est lent ! Sur les autoroutes de l'information, lorsque le volume des échanges aura été multiplié par 10 ou par 100, les temps de téléchargement deviendront rédhibitoires. La technique de transfert asynchrone, désignée par l'acronyme anglais ATM, résoudrait le problème : alors que le débit des transmissions classiques est inférieur à quelques millions de bits par seconde (un bit est un chiffre binaire 0 ou 1), on a déjà réalisé des transmissions ATM à plus de deux milliards de bits par seconde.

Bientôt, outre le téléphone et la télévision, toutes les informations seront numérisées : documents, peintures, etc., sans mentionner les mondes virtuels du futur ! Ces informations seront accessibles, en permanence, à travers un réseau à haut débit, par toute personne disposant d'un ordinateur.

Les télécommunications ont beaucoup progressé grâce à l'introduction de l'optique : fibres optiques, lasers, etc. C'est l'optique qui offre les débits nécessaires à la prolifération des échanges et aux nouveaux services «large bande» : images, vidéo et données informatiques rapides (plus la bande est large, c'est-à-dire plus la gamme de fréquences transmises est grande, plus le débit est élevé ; une fibre optique a une bande passante cent millions de fois plus large qu'un câble téléphonique). Grâce à l'optique, on a aussi amélioré la qualité des transmissions numériques et on a simplifié les protocoles de transfert.

Une nouvelle étape s'annonce : le regroupement des informations numériques, quelle que soit leur nature, en paquets ; c'est la «paquetisation». L'ordinateur de l'utilisateur segmente les données à envoyer en blocs de longueur fixe ou variable. Chaque bloc devient un paquet par l'adjonction d'un en-tête qui contient toutes les données nécessaires à son transfert vers le destinataire. Deux techniques sont d'actualité : l'ATM qui utilise des paquets de longueur fixe, nommés cellules, et la technique de paquets de longueur variable utilisée sur Internet. Conçues en vue d'objectifs différents, elles sont à la fois complémentaires et concurrentes.

Vers les autoroutes de l'information

La première démonstration de l'ATM a eu lieu en France, en 1985, au Centre national d'études des télécommunications de Lannion (voir *Prélude, le réseau de communication du futur*, par Jean-Pierre Coudreuse, *Pour la Science*, n°122, décembre 1987). En 1988, l'Union internationale des télécommunications a recommandé l'usage de l'ATM pour l'infrastructure des futurs réseaux publics à «large bande». Il continue, depuis, à publier des documents de normalisation et de standardisation qui sont mondialement suivis.

En 1990, quelques industriels de l'informatique créent, aux États-Unis, le forum ATM, afin de promouvoir l'usage de l'ATM dans les réseaux privés et de publier des recommandations visant à faciliter l'interopérabilité d'équipements d'origines diverses. Le forum associe aujourd'hui près de 1 000 membres, parmi lesquels figurent les grands opérateurs publics et privés.

Tandis que les travaux de standardisation se poursuivent, les opérateurs vérifient sur le terrain la validité des options retenues. Fin 1992, de grands opérateurs publics européens lancent l'Europilote, qui devient le plus grand réseau mondial ATM. Il est destiné à l'expérimentation en vraie grandeur et à grande échelle des premiers services ATM et de leur gestion. Associant aujourd'hui 20 opérateurs et rebaptisé JAMES *(Joint ATM Expriment on European Services)*, le projet se poursuit avec l'expérimentation de services plus évolués, notamment de services commutés analogues au service téléphonique, et de services de paquets Internet transportés dans des cellules ATM.

Les grandes entreprises s'intéressent à l'ATM dans le cadre de la construction d'autoroutes de l'information. Ainsi, depuis avril 1997, le Société *Renault* utilise un réseau ATM mis en place par *France Télécom* pour travailler à distance (visioconférence, conception assistée par ordinateur) entre des centres de recherche situés en France et en Espagne. Des projets comparables se déroulent ailleurs dans le monde, notamment en Amérique du Nord.

La technique ATM

L'ATM est une technique conçue pour le transfert rapide d'informations numériques par les réseaux de télécommunications. Elle utilise des cellules de 53 octets (un octet comprend huit chiffres binaires) pour transporter des blocs de 48 octets avec un entête de 5 octets entre des sources et des récepteurs reliés par des liens de transmission. Ces cellules traversent des nœuds de commutation où elles sont aiguillées vers des directions différentes selon l'adresse inscrite dans leur entête. L'ATM opère en «mode connecté» : le chemin suivi par les cellules est déterminé avant leur transfert, et les ressources nécessaires, notamment en bande passante, sont réservées. Ainsi, l'émetteur est-il assuré que le message parviendra dans son intégrité.

À l'inverse, dans le protocole de transmission utilisé sur l'Internet