

# Sommaire

<b>Préface</b>	5
<small>PAR THIERRY BRETON, MINISTRE DE L'ÉCONOMIE, DES FINANCES ET DE L'INDUSTRIE</small>	
<b>Internet: la sortie de l'enfance</b>	7
<small>PAR ISABELLE FAQUE-PIERROTIN</small>	
<b>Le Forum des droits sur l'internet en 2005</b>	9
<b>Les enjeux de droit et de société en 2005</b>	21
 Première partie	
<b>LA CONCERTATION</b>	
<b>Les recommandations du Forum des droits sur l'internet publiées en 2005</b>	57
<b>Les enfants du net (II): pédo-pornographie et pédophilie sur l'internet</b>	59
<b>Liens commerciaux: prévenir et résoudre les atteintes aux droits des tiers</b>	132
<b>Commerce entre particuliers sur l'internet: quelles obligations pour les vendeurs et les plates-formes de mise en relation ?</b>	139
<b>La conservation électronique des documents</b>	188
 Deuxième partie	
<b>L'INFORMATION ET LA SENSIBILISATION</b>	229
<b>Rapport sur le projet de carte nationale d'identité électronique (CNIE)</b>	231
<b>Les autres publications du Forum des droits sur l'internet</b>	277
	3

Troisième partie

**LA MÉDIATION**

279

Quatrième partie

**LA COOPÉRATION INTERNATIONALE**

305

**Policy Statement on Internet Governance**

307

**Report on Protecting Minors from Exposure  
to Harmful Content on Mobile Phones**

313

Cinquième partie

**LES PERSPECTIVES DE L'ANNÉE 2006**

325

PAR ISABELLE FALQUE-PIERROTIN

**Table des matières**

331

# Préface

Depuis 2002, la priorité donnée aux TIC par le Gouvernement a eu pour conséquence une progression fulgurante de leur utilisation par les Français. En mai 2002, la France comptait 700 000 abonnés à Internet haut débit. Le Gouvernement avait alors fixé pour objectif qu'au terme de la législature, en 2007, la France en compte 10 millions et qu'elle entre pleinement dans l'ère numérique. Une dynamique vertueuse, la plus forte d'Europe, s'est enclenchée. La France a aujourd'hui 9 millions d'abonnés à haut débit, l'objectif de 10 millions sera donc dépassé dès 2006 ! Les services audiovisuels sur ADSL et bientôt sur téléphone mobile, se généralisent ; l'offre de services « triple play », Internet, audiovisuel, téléphone, à la disposition des Français se situe incontestablement à la pointe au plan européen. C'est d'ailleurs en France que les premières offres de ce type ont été lancées !

Le développement numérique de la France est désormais le premier en Europe ; il est comparable à celui des États-Unis. Les usages tels que le commerce électronique et les télédéclarations d'impôt explosent. Plus d'un Français sur quatre effectue ses achats en ligne.

Le cadre législatif et réglementaire français a été redessiné en 2003 et en 2004 avec les lois sur l'économie numérique et sur les télécommunications ou encore les textes sur l'administration électronique. Naturellement, des marges de progrès demeurent et nécessitent des mesures complémentaires, notamment sur la gestion des droits d'auteur dans la société de l'information qui sera examinée prochainement par le Parlement.

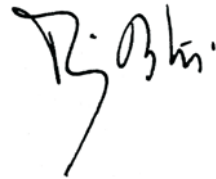
Internet, nouveau média, nous fait vivre une mutation économique et sociale majeure. Il est donc normal que de nombreux sujets restent encore devant nous, qu'il s'agisse de la couverture des communes en haut débit d'ici à 2007, de la protection du cyberconsommateur, de la lutte contre le spam ou la protection de l'enfance. Leur résolution ne saurait se concevoir sans une concertation appropriée avec l'ensemble des acteurs concernés : pouvoirs publics, entreprises, société civile.

Au cœur de cette concertation depuis sa création en 2001, le Forum des droits sur l'Internet a remarquablement su, grâce à son approche originale de la « co-régulation » contribuer à la recherche de réponses pertinentes aux nouvelles questions posées. La qualité de ses travaux et de ses recommandations a démontré qu'une forme participative d'élaboration des normes juridiques trouve pleinement sa place dans le monde de l'Internet, et favorise le développement de la confiance dans le

réseau. Aujourd'hui, le Forum va encore plus loin avec son service de médiation des litiges de l'Internet, qui propose aux internautes une voie de règlement amiable et souple.

J'ai eu l'honneur d'exprimer la position du Gouvernement français au Sommet mondial de la société de l'information qui s'est déroulé en novembre 2005 à Tunis. L'une de ses principales conclusions sur le délicat sujet de la gouvernance de l'Internet a été de créer un « forum » associant les gouvernements, le secteur privé, la société civile et les organisations multilatérales et internationales.

Pourrait-il y avoir de plus belle reconnaissance pour le Forum des droits sur l'Internet, qu'une démarche comparable à la sienne ait été adoptée au plan international pour avancer sur l'une des grandes questions de l'Internet ?

A handwritten signature in black ink, appearing to read 'T. Breton'.

Thierry BRETON

Ministre de l'Économie, des Finances et de l'Industrie

## **Internet: la sortie de l'enfance**

Le cadre juridique de l'internet est aujourd'hui fixé dans ses grandes lignes.

Dans les domaines du droit d'auteur, du commerce électronique, de la protection des mineurs, l'internet n'est pas un espace de non droit.

La France s'est dotée du plan Re/So 2007 et de nombreuses initiatives gouvernementales ont été prises pour accélérer l'appropriation des nouvelles technologies par le plus grand nombre et encourager la responsabilisation des acteurs.

Au plan européen, un certain nombre de directives ont été élaborées, et ont été ou sont en cours de transposition, encadrant l'internet.

Au plan international, les différents sommets mondiaux pour la Société de l'information, Genève en 2003 et Tunis en 2005, ont notamment permis la mise en place d'un dialogue entre les nations et d'un fonds pour lutter contre la fracture numérique.

Le Forum des droits sur l'internet a pris une part active à ces évolutions, depuis sa création en 2001. Ses travaux de concertation ont ainsi permis sujet par sujet, au plan national comme européen, d'aider à élaborer le pacte social entre acteurs publics et privés. Ses Recommandations se sont d'ailleurs, pour la plupart, traduites par des avancées législatives ou réglementaires et par une modification des pratiques des acteurs.

La médiation, également, nouvelle activité lancée fin 2003, contribue à cette progressive sécurisation du secteur puisqu'il s'agit, en s'inspirant d'une même philosophie de dialogue et de concertation, d'aider les parties à trouver une solution amiable à leurs différends en ligne, en équité et participer ainsi à la construction de la confiance.

En réalité, l'enjeu que ces dernières années ont mis en lumière est celui de l'interdépendance très forte et de la « co responsabilité » des acteurs publics et privés sur ces questions de régulation. Comment par exemple protéger l'enfant si l'on ne responsabilise pas toute la chaîne professionnelle (fournisseurs d'accès, de services), les parents, les associations, les enfants eux-mêmes. Un seul texte de loi n'y suffit pas!

À ce titre, la méthode de « corégulation » que pratique le Forum des droits sur l'internet est particulièrement efficace puisqu'elle permet, par la consultation préalable de l'ensemble des parties prenantes (l'État, les entreprises et les utilisateurs eux-mêmes), de travailler en amont d'un problème pour tenter de rechercher des solutions de consensus. Elle permet, concrètement, d'articuler l'intervention réglementaire des pouvoirs publics avec l'action d'autorégulation des acteurs privés. Cette méthode est née des caractéristiques mêmes du réseau Internet, ouvert et décentralisé.

Internet est aujourd'hui sorti de l'enfance.

Dès lors, la problématique de l'encadrement des contenus et des pratiques se pose différemment d'il y a cinq ans. L'heure est moins à la réflexion qu'à la gestion. L'objectif central est celui de sécuriser les usages grand public dans le cadre juridique existant.

Espace de droit construit ensemble, internet est devenu un véritable écosystème numérique qui appelle aujourd'hui de nouveaux outils de gestion, fondés sur la mise en œuvre de processus transversaux. La médiation, opérée par le Forum des droits sur l'internet depuis 2003 et le développement de chartes et de labels pour favoriser les bonnes pratiques en sont deux exemples concrets.

Isabelle FALQUE-PIERROTIN

*Conseiller d'État,  
Présidente du Conseil d'orientation  
du Forum des droits sur l'internet,  
Membre de la CNIL*

# **Le Forum des droits sur l'internet en 2005**

2005 a conforté la place du Forum des droits sur l'internet dans la régulation de l'internet.

Le Forum a poursuivi son développement, fondé sur l'accomplissement de ses quatre missions, respectivement de concertation, d'information, de médiation et de coopération internationale.

Sur saisine des pouvoirs publics, de ses membres ou de sa propre initiative, le Forum a travaillé sur un éventail très large de problématiques juridiques et de société liées à l'internet: protection de l'enfance sur l'internet, carte d'identité électronique, paiements sur l'internet, conservation électronique des documents...

## **Fonctionnement du Forum en 2005**

### Un renforcement de l'équipe de médiation

Le Forum fonctionne avec une équipe de douze permanents, dont plusieurs chargés de mission, juristes pour la plupart, spécialisés dans des secteurs comme le commerce électronique, la propriété littéraire et artistique ou encore la protection des mineurs et la lutte contre la cybercriminalité. En 2005, le Forum a développé son activité de médiation qui emploie désormais quatre personnes en interne et trois médiateurs externes.

### Un budget stable

Le Forum a mis en place de nouvelles activités et assuré son développement à subvention constante depuis 2001. La convention triennale avec l'État, renouvelée en mai 2004, fixe le cadre d'intervention du Forum des droits sur l'internet.

Outre la participation financière des pouvoirs publics (1,1 million d'euros par an), le budget du Forum est composé de fonds privés provenant essentiellement des cotisations des adhérents au Forum, qui contribuent à hauteur de 15 % au budget total du Forum.

Le Forum dispose d'un important réseau de membres, rassemblant près de 70 acteurs de l'internet. Les adhésions 2005 concernent des membres comme Cofidis, la SACD, l'IRCAM, la BNF ou encore l'AFOM.

### Renouvellement au sein des organes dirigeants

Le Conseil de surveillance s'est réuni deux fois en 2005.

Pour sa part, le Conseil d'orientation s'est réuni à cinq reprises en 2005.

L'Assemblée générale, qui s'est déroulée le 31 mai 2005 au siège du Forum en présence de ses membres, a permis l'élection de nouveaux représentants dans les

instances dirigeantes. L'Institut de recherche et coordination acoustique/Musique (IRCAM) entre ainsi au Conseil de surveillance; le Conseil d'orientation voit l'arrivée de Yahoo! France, la reconduction de l'Union des annonceurs (UDA) dans le collège des acteurs économiques ainsi que l'entrée d'Aquitaine Europe communication (AEC) dans le collège des utilisateurs.

*(Voir en annexe la composition du Conseil de surveillance et du Conseil d'orientation).*

## **Missions du Forum des droits sur l'internet**

Les actions de concertation entre les acteurs publics et privés sur les enjeux juridiques de l'internet

### **Les recommandations des groupes de travail**

Pour répondre à sa première mission consistant à organiser la concertation entre tous les acteurs, le Forum a installé de nouveaux groupes de travail en 2005.

À la demande du ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales, et sur une proposition de Thierry Breton dans le cadre du chantier Cybercriminalité du ministère, **un groupe de travail «Certificat citoyen»** a été créé en avril 2005. Il a pour mission de réfléchir à la création d'une marque de confiance qui valorisera les bonnes pratiques des fournisseurs d'accès et de services en matière de sécurisation des usages de l'internet: sensibilisation des utilisateurs, fourniture d'outils adaptés, coopération avec les autorités. À la demande du Premier ministre et du ministre en charge de la Famille lors de la Conférence de la Famille 2005, ces travaux prennent également en compte la **dimension familiale** des usages de l'internet. Le groupe rendra publiques ses recommandations en janvier 2006.

**Un groupe de travail «Classification des contenus multimédias mobiles»** a été mis en place en octobre 2005, à la demande de l'AFOM (l'Association française des opérateurs mobiles). Ce groupe de travail a pour objectif de mettre au point un schéma de classification des contenus accessibles depuis les portails et les kiosques des opérateurs, essentiel à la mise en œuvre de dispositifs de contrôle parental adaptés aux jeunes usagers. Ce schéma de classification doit recueillir l'approbation des différentes parties, pouvoirs publics, représentants des utilisateurs et des intérêts familiaux, opérateurs et éditeurs de contenus et services.

**En 2005, le Forum a rendu publiques quatre Recommandations, portant à 19 le nombre total de Recommandations émises depuis sa création:**

#### **Les enfants du net (II): pédo-pornographie et pédophilie sur l'internet, 25 janvier 2005**

Remise à Philippe Douste-Blazy, alors ministre des Solidarités, de la Santé et de la Famille, cette recommandation, qui complète une recommandation de 2004 sur l'exposition des mineurs aux contenus préjudiciables, porte sur les moyens de lutte



contre la pédo-pornographie et la pédophilie sur l'internet et propose un plan d'action, fruit du consensus des acteurs concernés.

**Liens commerciaux: prévenir et résoudre les atteintes aux droits des tiers, 26 juillet 2005**

Cette recommandation, adressée à l'ensemble des acteurs concernés, formalise les règles de bonne conduite pour les liens commerciaux permettant de prévenir et de résoudre, en dehors de toute procédure judiciaire, les éventuelles atteintes aux droits des tiers.

**Commerce entre particuliers sur l'internet: quelles obligations pour les vendeurs et les plates-formes de mise en relation?, 8 novembre 2005**

Cette recommandation s'attache à déterminer le rôle de chacun des intervenants dans la vente (utilisateurs, plates-formes), les obligations auxquelles ces derniers sont soumis et la manière dont ils peuvent les remplir.

**Conservation électronique des documents, 1<sup>er</sup> décembre 2005**

Cette recommandation, réalisée en collaboration avec la Mission pour l'économie numérique, précise la notion d'intégrité des documents électroniques au regard de la loi du 13 mars 2000. Elle fournit aux acteurs privés un guide pratique du processus d'archivage permettant de satisfaire à cet objectif d'intégrité.

**Plusieurs Recommandations émises par le Forum précédemment ont été suivies d'effets en 2005:**

**Données publiques**

Publiées le 14 avril 2003, les recommandations du Forum des droits sur l'internet en matière de diffusion des données publiques (régulation basée sur la refonte de la CADA, répertoire des données publiques, tarification transparente, etc.) ont été reprises dans l'ordonnance du 6 juin 2005 relative à «la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques». Attendu par de nombreux acteurs, ce cadre juridique permet au secteur de trouver un nouveau modèle conjuguant la nécessité d'informer les citoyens et la volonté de permettre aux acteurs privés de se développer sur le marché de l'information.

**Actes authentiques électroniques**

Les principales recommandations, publiées le 18 novembre 2003, sur le projet de décret relatif aux «actes authentiques électroniques» ont été reprises par les ministères dans les deux décrets du 10 août 2005 précisant les conditions d'établissement, de conservation et de copie des actes authentiques sur support électronique prévues à l'article 1317 alinéa 2 du Code civil.

**Vote électronique**

S'appuyant sur les recommandations du Forum des droits sur l'internet en matière de vote électronique publiées en septembre 2003, le Gouvernement a poursuivi le déploiement progressif et raisonné de cette nouvelle modalité de participation. Après

les expérimentations pour diverses élections professionnelles, le vote électronique devrait prochainement être opérationnel pour les élections ordinaires dans le secteur de la santé, voire pour certaines élections politiques.

### **Télétravail**

Les principales propositions du Forum ont été reprises dans le cadre de l'accord national interprofessionnel adopté par les partenaires sociaux en septembre 2005. Ces propositions (définition du télétravail, formalisation de la mise en télétravail par un avenant au contrat de travail...) avaient été formulées par le Forum dans le cadre de sa Recommandation «Le Télétravail en France» remise en décembre 2004 à Gérard Larcher, ministre délégué aux Relations du travail.

### **Protection de l'enfance**

Dès 2004, le Forum des droits sur l'internet a proposé la mise en œuvre d'une campagne nationale de sensibilisation du grand public sur la question de la protection de l'enfance sur l'internet (Recommandations «Les enfants du net: les mineurs et les contenus préjudiciables sur l'internet» de février 2004 et «Pédo-pornographie et pédophilie sur l'internet» de janvier 2005). Cette proposition a été retenue dans le cadre des travaux préparatoires à la Conférence de la Famille. Lors de la Conférence de la Famille, qui s'est tenue en septembre 2005, le Premier Ministre et le ministre en charge de la Famille ont annoncé la création d'une campagne nationale de sensibilisation des familles aux moyens de maîtriser les usages de l'internet. Le souhait exprimé par le Premier ministre que la campagne de communication soit prolongée par un programme pédagogique d'information est également conforme aux propositions du Forum.

Conformément aux recommandations du Forum des droits sur l'internet, les pouvoirs publics ont soutenu la création d'un «nœud français de sensibilisation» dans le cadre du plan d'action pour un Internet plus sûr (*SaferInternet*) de la Commission européenne. Le Forum est membre du Conseil scientifique du projet, intitulé «Confiance».

Enfin, donnant suite aux recommandations du Forum, les opérateurs de téléphonie mobile ont entrepris de développer de nouveaux outils de contrôle parental adaptés aux supports mobiles.

### **Liens commerciaux**

Les acteurs ont commencé à adapter leurs pratiques, suivant en cela la recommandation émise par le Forum des droits sur l'internet en septembre 2005.

### **Commerce entre particuliers sur l'internet**

Suite à la Recommandation publiée par le Forum en novembre 2005, les plateformes de mise en relation ont commencé à adapter leurs pratiques afin de se conformer aux propositions du Forum, notamment en terme d'identification du vendeur professionnel.

## Les actions d'information et de sensibilisation

### **Le site foruminternet.org**

Le site institutionnel du Forum ([www.foruminternet.org](http://www.foruminternet.org)) est l'outil de référence des professionnels et des acteurs de l'internet. Avec plus de 700 000 visiteurs et de 2 millions de pages vues, la fréquentation du site a connu en 2005 une augmentation de 57 % par rapport à l'année 2004.

Au cours de l'année 2005, de nombreuses actualités ont été rédigées et plusieurs forums de discussion mis en place. À la suite du mandat reçu du ministère de l'Intérieur, le Forum a ainsi ouvert et animé pendant quatre mois (de février à mai 2005) un forum de discussion recueillant le point de vue des internautes sur la carte nationale d'identité électronique. Les principaux enseignements des 3 000 contributions en ligne comme celles des six rencontres organisées en région ont été rendus publics en juin 2005 (synthèse sur [www.foruminternet.org/publications](http://www.foruminternet.org/publications)).

Une enquête sur les attentes des internautes vis-à-vis du site a été lancée en novembre 2005, afin d'orienter les travaux de refonte du site qui seront entrepris en 2006.

### **Le site droitdunet.fr**

Depuis son ouverture en 2003, [droitdunet.fr](http://droitdunet.fr), le site d'information grand public du Forum, est régulièrement mis à jour. De nouvelles fiches pratiques ont été mises en ligne en 2005, notamment sur les *blogs*, la propriété littéraire et artistique, les moyens de paiements sur l'internet ou encore le droit du travail.

La fréquentation du site a enregistré une augmentation de 24 % par rapport à l'année 2004, avec plus de 400 000 visiteurs et près de 2 millions de pages vues. Par ailleurs, le service a répondu, en 2005, à plus de 3 500 questions posées par les internautes.

### **La publication de rapports et de dossiers**

Le Forum publie des rapports et dossiers sur une base régulière.

Il a ainsi remis en juin 2005 son rapport au ministre de l'Intérieur, à la suite de la consultation publique menée à la demande de celui-ci, sur le « **Projet de carte nationale d'identité électronique** » (projet « INES », Identité nationale électronique sécurisée, avec données biométriques).

Le Forum a publié en mai 2005 son second rapport sur la **cyber-consommation**, consacré aux paiements sur l'internet. Ce rapport a été réalisé sur la base de l'audition de plus de 40 acteurs du paiement en ligne : institutions publiques, associations de consommateurs, intermédiaires techniques, prestataires. Le Forum a également collecté les témoignages de plusieurs centaines d'internautes sur le site [www.foruminternet.org](http://www.foruminternet.org).

En décembre, le Forum a publié le dossier « **Comprendre le projet de loi sur le droit d'auteur et les droits voisins dans la société de l'information** ». En amont de la discussion parlementaire, ce dossier présente le projet de loi et expose, en toute

indépendance, les enjeux qui y sont attachés en rappelant les positions des différents acteurs.

Ces rapports et dossiers sont disponibles sur le site du Forum à l'adresse : [www.foruminternet.org/publications](http://www.foruminternet.org/publications).

## La publication de guides pratiques

Le Forum a créé une collection de guides, outils pratiques conçus pour mieux informer le grand public sur les questions de droit et d'usage de l'internet.

Trois guides pratiques ont vu le jour en 2005.

Le guide de sensibilisation des jeunes internautes ***Musique et film: Adopte la Net attitude*** a été publié le 21 mars.

Le guide ***Achats en ligne: suivez le guide***, destiné aux cyber-consommateurs, a été diffusé en ligne et en version papier à 220 000 exemplaires, encarté dans l'hebdomadaire *MicroHebdo* daté du 17 novembre.

Ces deux guides ont été réalisés en partenariat avec les acteurs concernés et ont reçu le soutien des pouvoirs publics.

Enfin, le Forum a publié en novembre le guide ***Je blogue tranquille*** sur son site grand public [www.droitdunet.fr](http://www.droitdunet.fr). Dans le but d'informer le plus grand nombre, il y indique les principaux usages et rappelle les règles juridiques applicables aux blogs.

## Les événements

Le Forum a organisé en 2005 de nombreux événements :

- deux « rencontres » ont été organisées : « Que font « vraiment » nos enfants sur internet ? » le 26 avril au carrefour numérique de la Cité des sciences et de l'industrie et « Publicité sur l'internet : la ruée vers l'or, les règles du jeu » qui a rassemblé plus de 80 professionnels, le 12 septembre, au musée de la Publicité ;
- des « petits-déjeuners », format plus restreint autour de l'intervention d'une personnalité : Nicolas Curien, membre de l'Autorité de régulation des communications électroniques et postales (ARCEP), a été reçu le 13 octobre dans ce cadre, ainsi que François Loos, ministre délégué à l'Industrie, le 10 novembre ;
- des « matinées d'information juridique » réservées aux membres ont été organisées sur les « Paiements sur l'internet » le 25 octobre et sur le « Droit du travail et l'internet » le 15 décembre.

## La médiation

Cette mission, déployée par le Forum des droits sur l'internet auprès du grand public depuis 2004, consiste à proposer au particulier une solution amiable pour régler les différends qu'il peut rencontrer sur l'internet (litige commercial, lié à la fourniture d'accès, au respect de la vie privée...). Cette médiation extrajudiciaire est opérée par une équipe de médiateurs mise en place par le Forum et s'appuie sur une plate-forme technique en ligne.

Le service a rencontré depuis son ouverture auprès du public et des entreprises un véritable succès puisque, à la fin de l'année 2005, plus de 5 400 demandes avaient été présentées au service et un peu plus de 3 100 dossiers avaient été traités avec un taux de résolution de 89 % pour les dossiers clôturés. Ce service est très apprécié des internautes, comme l'a confirmé l'étude menée en 2005 par un cabinet indépendant, avec un taux de satisfaction de plus de 73 %.

Le Forum démontre ainsi que la médiation est une méthode qui se révèle tout à fait appropriée au règlement de certains problèmes rencontrés sur internet. Cette méthode complète les voies de recours existantes : justice, associations de consommateurs, autorités administratives de répression... Le Forum est d'ailleurs en contact régulier avec ces autres organismes pour proposer aux internautes la meilleure solution au règlement de leur différend dans un souci d'efficacité et de rapidité.

Le Forum a également pu démontrer que son mode de règlement en ligne des différends (« *Online dispute resolution* ») est opérationnel sans être pour autant exclusif d'autres modes de dialogue (courrier postal, téléphone, télécopie). La mixité de ces modes et la souplesse de leur utilisation dans un encadrement par ailleurs très précis du processus de médiation ont donné d'excellents résultats. Prenant acte de l'efficacité de ce service, le ministère de la Justice a souhaité le soutenir financièrement en 2005.

## La coopération internationale à travers le réseau européen de corégulation de l'internet

Le Forum a constitué fin 2003 un Réseau européen de corégulation de l'internet (EICN), regroupant des organismes de sept pays européens, structures publiques ou privées qui pratiquent ou promeuvent une approche multiacteurs sur les questions liées à l'internet ([www.internet-coregulation.org](http://www.internet-coregulation.org)).

L'EICN a rendu publics en juillet 2005 deux rapports, remis à Viviane Reding, Commissaire européen en charge de la société de l'information et des médias :

**Le rapport « *Protecting Minors from Exposure to Harmful Content on Mobile Phones* »**, consacré à la protection de l'enfance et la téléphonie mobile, a été coordonné par l'un des membres du Réseau, l'Oxford Internet Institute (UK). Suite à cette remise, la Commission européenne a convié le Réseau à prendre part à ses travaux portant sur la protection des mineurs dans les environnements multimédias mobiles.

**Le rapport « *Internet Governance* »** a été coordonné par le Forum et vise à proposer des règles de référence pour la régulation de l'internet. Ces travaux ont aidé à la réflexion du groupe de travail sur la gouvernance de l'internet (WGIG), constitué sous l'égide du Secrétaire général des Nations unies, qui a remis son rapport préparatoire au Sommet de Tunis en juillet 2005.

## **Annexes**

### Composition du Conseil d'orientation

#### **Collège des acteurs économiques**

**La FEVAD (Fédération des entreprises de vente à distance)**, représentée par **Marc LOLIVIER**

**France Telecom**, représenté par **Jean-Marc STEFFANN**

**L'UDA (Union des annonceurs)**, représentée par **Christine REICHENBACH**

**Yahoo! France**, représenté par **Christophe PARCOT**

#### **Collège des utilisateurs**

**L'ISOC (Internet SOCIety France)**, représenté par **Sébastien CANEVET**

**L'AEC (Aquitaine Europe communication)**, représenté par **Marcel DESVERGNE**

**La CLCV (Confédération de la consommation, du logement et du cadre de vie)**, représentée par **Reine-Claude MADER**

**L'UNAF (Union nationale des associations familiales)**, représentée par **Jean-Pierre QUIGNAUX**

#### **Personnalités qualifiées**

**Jean-François ABRAMATIC**, ancien président du W3C

**Pierre SIRINELLI**, professeur de droit

**Daniel KAPLAN**, consultant

**Isabelle FALQUE-PIERROTIN**, membre du Conseil d'État, présidente du Conseil d'orientation

#### **Observateurs**

**Direction du développement des médias (DDM)**, service du Premier ministre

**Direction générale des entreprises**, ministère de l'Économie, des Finances et de l'Industrie

Le Conseil d'orientation est investi des pouvoirs les plus étendus pour diriger, gérer et administrer l'association sous réserve de ceux statutairement reconnus au Conseil de surveillance et à l'Assemblée générale. Il valide les recommandations du Forum avant publication.

## Composition du Conseil de surveillance

### **Personnalité qualifiée**

**François TERRE**, professeur de droit, président du Conseil de surveillance

### **Collège des acteurs économiques**

**La Caisse des dépôts et consignations**, représentée par **Serge BERGAMELLI**

### **Collège des utilisateurs**

**L'IRCAM (Institut de recherche et coordination acoustique/musique)**, représenté par **Bernard STIEGLER**

Le Conseil de surveillance vérifie que l'activité de l'association correspond à son objet social. Il assure le contrôle des comptes de l'association et vérifie la régularité des opérations comptables. Il arrête les comptes de l'exercice clos.

## L'équipe du Forum des droits sur l'internet

Le Forum fonctionne avec une équipe composée des membres permanents suivants :

- **Déléguée générale : Isabelle FALQUE-PIERROTIN**
- **Secrétaire générale : Marie-Françoise LE TALLEC**
- **Assistante : Sophie OUZEAU**
- **Directrice de la communication : Corinne MULLER**
- **Chargés de mission : Jean GONIÉ** (e-gouvernement), **Stéphane GRÉGOIRE** (propriété littéraire et artistique), **Matthieu LERONDEAU** (cybercriminalité et protection de l'enfance), **David MELISON** (sites internet), **Benoit TABAKA** (commerce électronique)
- **Service de médiation : Marie-Françoise LE TALLEC** (responsable), **Laure BAËTÉ**, **Franck BERGERON**, **Claire-Isabelle VOILIN**

## Les adhérents du Forum des droits sur l'internet (décembre 2005)

### Collège des acteurs économiques

#### **Professions juridiques :**

SCP Charlet/Develay  
Jurisconcept  
Juritel  
Cabinet Latournerie Wolfrom et Associés  
Mouvement Jeune Notariat  
Cabinet Cyril Rojinsky

#### **Banques :**

Caisse des dépôts et consignations  
Cofidis SA  
Fédération bancaire française  
Société générale

#### **Commerce en ligne :**

eBay  
Fédération des entreprises de vente à distance (FEVAD)  
PayPal France SAS  
PriceMinister

#### **Enseignement :**

Centre national d'enseignement à distance (CNED)

#### **Industrie hi-tech/internet :**

Association française des opérateurs mobiles (AFOM)  
Association des fournisseurs d'accès (AFA)  
APROGED  
Groupe Berger-Levrault  
Security.com  
Certeurope  
Cirès  
La Fédération nationale des Tiers de confiance (FNTC)  
Fédération nationale de l'information d'entreprises et de la gestion de créances (FIGEC)  
Google France  
Groupement interprofessionnel de promotion des systèmes d'information médico-sociale (GIPSIM)  
LeGuide.com

### Collège des utilisateurs

#### **Associations :**

Association pour le développement de l'informatique juridique (ADIJ)  
Association des professionnels de l'information et de la documentation (ADBS)  
Aquitaine Europe communication (AEC)  
Association française de droit de l'informatique et de la télécommunication (AFDIT)  
Association française pour le nommage Internet en coopération (AFNIC)  
Association Internationale des Jeunes Professionnels de la communication (AIJPC)  
Association pour la promotion et la recherche en informatique libre (APRIL)  
Club du e-public  
CréaTIF  
Fondation internet nouvelle génération (FING)  
Free Software Foundation France (FSF)  
Internet SOCIety France (ISOC)  
Observatoire des usages de l'internet (OUI)

#### **Associations de consommateurs :**

Confédération de la consommation, du logement et du cadre de vie (CLCV)  
Union nationale des associations familiales (UNAF)

#### **Collectivités territoriales :**

Apronet  
Artesi  
Villes-Internet

#### **Droit de l'homme et libertés :**

Conseil représentatif des institutions juives de France (CRIF)  
Mouvement contre le racisme et pour l'amitié entre les peuples (MRAP)



## Collège des acteurs économiques

Microsoft  
Orange France  
Overture  
Syndicat de l'industrie des technologies de l'information (SFIB)  
Syndicat professionnel des médias de télécommunications (SPMT)  
Wanadoo  
Yahoo France

### Presse/média/culture :

Agence civile pour l'administration des droits des artistes et musiciens interprètes (ADAMI)  
Bureau de vérification de la publicité (BVP)  
France 5  
Institut national de l'audiovisuel (INA)  
Société des auteurs compositeurs dramatiques (SACD)  
Société des auteurs compositeurs éditeurs de musique (SACEM)  
Syndicat national de l'édition phonographique (SNEP)  
Union des annonceurs (UDA)  
Vivendi Universal

## Collège des utilisateurs

### Culture, enseignement et recherche :

Association du DESS en droit du multimédia et de l'informatique (ADMI)  
Bibliothèque nationale de France (BNF)  
Centre national de la recherche scientifique (CNRS)  
Institut de recherche et coordination acoustique/musique (IRCAM)  
Institut de recherches et prospectives postales (IREPP)  
Société française des sciences de l'information et de la communication (SFSIC)

## Barème des cotisations 2005

Type de structures	Cotisation 1	Cotisation 2	Cotisation 3	Cotisation 4
Personnes morales CA ou budget > 150 millions €				<b>16000 €</b>
Personnes morales CA ou budget > 30 millions €			<b>8000 €</b>	
Personnes morales CA ou budget > 200 000 €		<b>1000 €</b>		
Personnes morales CA ou budget < 200 000 €	<b>100 €</b>			

Les cotisations sont dues par tous les membres et sont annuelles. Elles sont forfaitaires, basées sur le chiffre d'affaires ou le budget de la structure adhérente. Elles sont payées en début d'année ou lors de l'adhésion en une seule fois et calculées sur le montant du budget/ chiffre d'affaires prévisionnel de l'année en cours.

## **Les enjeux de droit et de société en 2005**

Après une année 2004 qui a été celle de la construction du cadre juridique, l'année 2005 s'est essentiellement focalisée à parfaire et consolider cet édifice juridique. De nombreux textes législatifs et réglementaires sont intervenus, destinés à renforcer la confiance des internautes envers telle ou telle pratique de l'internet.

L'année qui vient de s'écouler marque néanmoins une étape clé. En effet, les premières applications des textes (comme la loi pour la confiance dans l'économie numérique) ou les discussions en cours, tendent à montrer une volonté forte de responsabiliser les intermédiaires techniques. Le débat autour de la propriété intellectuelle démontre cet état de fait. De même et alors que les textes avaient souhaité les faire relever d'un régime de responsabilité aménagé, les magistrats n'hésitent plus à recourir aux fournisseurs d'accès à l'internet ou aux hébergeurs pour suspendre un contenu ou filtrer totalement un site internet.

Ce tournant est la conséquence directe de la démocratisation de l'internet, déjà amorcée au cours des années précédentes. Les utilisateurs ont besoin dorénavant d'une plus grande assurance dans leur navigation. Ce besoin conduit les pouvoirs publics à une régulation plus forte tendant à limiter le caractère naturellement ouvert et sans limite de l'internet.

Cette problématique du contrôle de l'internet est au cœur des discussions finale du Sommet mondial pour la société de l'information. Lors de la réunion qui s'est tenue à Tunis en novembre 2005, les États ont acté la création d'un Forum international de la gouvernance. Cette structure composée de représentants des États, des acteurs économiques ainsi que de la société civile travaillera principalement sur des sujets relatifs aux usages et aux contenus de l'internet (*spamming*, liberté d'expression, cybercriminalité). Cette proposition reprend largement les recommandations formulées, dans le cadre du processus préparatoire au sommet, par le Forum des droits sur l'internet et le Réseau européen de corégulation de l'internet. À l'opposé, la gouvernance technique de l'internet demeure régie par l'ICANN, faute d'accord entre les États-Unis et les autres États sur ce point.

### **Lutte contre la cybercriminalité**

La conservation des données de connexion

#### **Le champ d'application du régime**

Deux régimes complémentaires coexistent en droit français en matière de conservation de données de connexion. Tout d'abord, l'article L. 34-1 du Code des postes et communications électroniques, institué par la loi sur la sécurité quotidienne du 15 novembre 2001, impose aux opérateurs de communications électroniques, et

notamment aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, d'effacer ou de rendre anonyme toute donnée relative au trafic. Ce principe d'effacement est tempéré par plusieurs exceptions permettant voire imposant la conservation des données à des fins de facturation, pour la sécurité des réseaux ou pour les mettre à disposition des autorités judiciaires. Ensuite, un second régime, issu à l'origine de la loi du 1<sup>er</sup> août 2000 et repris dans la loi du 21 juin 2004 pour la confiance dans l'économie numérique, impose aux fournisseurs d'accès à l'internet et aux hébergeurs de détenir et conserver «*les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires*».

Deux problématiques sont apparues en la matière: qui est tenu à cette obligation de conservation? Celle-ci est-elle complétée par une obligation de vérification des données conservées?

Répondant à la première interrogation, la Cour d'appel de Paris a indiqué, par un arrêt du 4 février 2005, qu'une entreprise pouvait être qualifiée de fournisseur d'accès à l'internet au sens de l'ancien article 43-7 de la loi du 30 septembre 1986, inséré par la loi du 1<sup>er</sup> août 2000. Elle est donc soumise, à ce titre, à l'ensemble des obligations pesant sur cet intermédiaire et notamment «*détenir et conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisitions judiciaires*». En l'espèce, la société World Press Online avait enregistré au début de l'année 2004, la rupture de deux contrats de représentation conclus avec des agents situés en Autriche et aux États-Unis. L'un des agents indiquait qu'après «*avoir reçu un mail anonyme affirmant que la société allait fermer, j'ai perdu confiance dans le projet*». Il s'avérait, en effet, que deux courriers électroniques mensongers avaient été envoyés à ces agents depuis une adresse de courrier électronique gratuite. L'enquête auprès du fournisseur d'adresse avait permis de communiquer l'adresse IP de l'expéditeur de ces messages, qui s'avérait être celle utilisée par un salarié de la BNP Paribas. World Press Online adressa donc à la banque une demande tendant à obtenir la communication de toute information permettant l'identification de l'expéditeur du message. En l'absence de réponse, elle décida de saisir la justice sur le fondement des articles 43-7 et 43-9 de la loi du 30 septembre 1986, alors applicables. Dans une ordonnance de référé du 12 octobre 2004, le Tribunal de commerce de Paris fit droit à sa demande.

L'article 43-7 précisait, en effet, que «*les personnes physiques ou morales dont l'activité est d'offrir un accès à des services de communication en ligne autres que de correspondance privée sont tenues, d'une part, d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner, d'autre part, de leur proposer au moins un de ces moyens*». L'article 43-9 ajoutait que ces prestataires «*sont tenus de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires*». Sur ces fondements, le tribunal ordonnait à la banque de «*communiquer l'identité et plus généralement toute information de nature à permettre l'identification de l'expéditeur du message électronique du 8 décembre 2003*».

En appel, les juges ont confirmé cette décision en précisant que *«la demande [...] ne se heurte à aucune contestation sérieuse alors qu'en sa qualité, non contestée, de prestataire technique au sens de l'article 43-7 de la loi du 1<sup>er</sup> août 2000, la société BNP est tenue, en application de l'article 43-9 de ladite loi, d'une part, de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisitions judiciaires»*. Ils ont donc ordonné à la banque de procéder à la communication des informations permettant d'identifier l'auteur du message. Les magistrats ont, néanmoins, atténué cette obligation en précisant que *«la loi du 1<sup>er</sup> août 2000 ne lui fait pas obligation de traiter les données qu'elle doit conserver et communiquer ni de procéder elle-même à l'identification de l'auteur du message litigieux»*. Jugée sous l'empire des anciennes dispositions, une solution identique aurait pu être retenue en application de l'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Cet article reprend en effet la définition posée à l'article 43-7 (au sein de l'article 6-I, 1°), et l'obligation corrélatrice visée – à l'origine – à l'article 43-9 (figurant dorénavant au sein de l'article 6-III).

Procédant également à une clarification, le projet relatif à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, présenté en Conseil des ministres le 26 octobre 2005, étend explicitement le champ d'application de l'article L. 34-1 du Code des postes et communications électroniques à d'autres prestataires. Ainsi, seraient soumises à ce régime, *«les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit»*.

Ce projet d'article tend à autoriser les services de renseignement et d'enquêtes à demander des informations techniques relatives aux connexions et navigations à partir de lieux publics ou commerciaux, via des bornes d'accès sans fil (WIFI), ou par l'intermédiaire d'un réseau distribué, communément appelé « cybercafé ». Concernant ceux-ci, l'exposé des motifs du projet de loi considère que leur problématique *«est d'offrir des accès à l'internet sans ménager de possibilités d'identifier les clients, ni de cerner les connexions individuellement. Ils utilisent cependant les réseaux existants pour véhiculer leurs informations. Par ailleurs, pour renforcer la confidentialité des navigations d'un client à un autre, toutes les traces sont souvent effacées sur le disque dur du terminal»*.

Concernant la vérification des données conservées, le Tribunal de grande instance de Paris a apporté une précision dans un jugement en date du 16 février 2005. Il a, en effet, retenu la responsabilité civile d'un hébergeur qui avait détenu et conservé des données d'identification fausses. *A contrario*, la même juridiction a pu estimer dans une précédente affaire en date du 2 février 2004 qu'un hébergeur n'était pas tenu à une telle vérification. Si cette divergence procède de décisions prises sous l'empire de la loi du 1<sup>er</sup> août 2000, il apparaît que les débats parlementaires préalables à l'adoption de la loi pour la confiance dans l'économie numérique ont clarifié cette question. Les parlementaires ont, en effet, refusé d'imposer une obligation de vérification des données aux hébergeurs: *«La réserve est d'ordre juridique et tient à la compatibilité d'une telle obligation au regard des dispositions de la directive communautaire du 8 juin 2000. Celle-ci ne prévoit en effet aucune obligation de ce type à la charge des*

*intermédiaires techniques de la société de l'information. Elle n'ouvre, par ailleurs, pas expressément aux États membres la faculté d'exiger la vérification de contenus».*

## **L'évolution du cadre européen applicable**

Outre ces clarifications en France, le régime juridique de la conservation des données de connexion fait l'objet de nombreuses discussions au plan européen. Le 12 juillet 2002, les quinze États membres de l'Union européenne adoptaient la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques qui impose aux États de se doter de législations encadrant la conservation des données relatives à l'établissement d'une communication. En France et comme il l'a été rappelé, cela fut fait par la loi du 15 novembre 2001 sur la sécurité quotidienne, modifiée en dernier lieu par la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Néanmoins, les décrets d'application n'ont pas encore été publiés au Journal officiel.

En complément à ce texte, la France, l'Irlande, la Suède et le Royaume-Uni ont présenté le 28 avril 2004 un projet de décision-cadre de l'Union européenne sur la rétention de données traitées et stockées en rapport avec la fourniture de services de communications électroniques accessibles au public ou de données transmises via des réseaux de communications publics, aux fins de la prévention, la recherche, la détection, la poursuite de délits et d'infractions pénales, y compris du terrorisme. Aux termes de l'article 4 de ce projet de texte communautaire, chaque État membre serait tenu de prendre les mesures nécessaires afin de veiller à ce que les données soient retenues pendant une période d'au moins douze mois et de maximum 36 mois après leur création. Le texte prévoyait que les États membres auraient la possibilité de fixer des périodes de rétention plus longues en fonction de critères nationaux pour autant qu'une rétention plus longue constitue une mesure nécessaire, appropriée et proportionnée dans une société démocratique. Dans un avis du 26 mai 2005, la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen a proposé le rejet de la proposition en procédure de consultation. Elle a émis de grandes réserves quant à la base juridique choisie (ce sujet relèverait de l'acquis communautaire, et ne saurait faire seulement l'objet d'une décision-cadre du Conseil) et la proportionnalité de la mesure. En outre, elle a souligné la possibilité d'une violation de l'article 8 de la Convention européenne des droits de l'homme.

Le 2 juin 2005, le Conseil de l'Union estimait, au contraire, pour ce qui est de la base juridique, que le Titre VI du traité de l'Union européenne devrait être la base juridique de la proposition. Sur les mesures mises en œuvre, le Conseil obtenait un accord entre les États afin d'adopter une approche progressive dans le traitement de ce sujet (en commençant par la rétention des données de communication de téléphonie fixe et mobile). Concernant la conservation des données de connexion internet, le Conseil a admis que les États membres qui ne seraient pas en mesure de collecter les données immédiatement pourraient bénéficier d'une période transitoire d'application de la décision-cadre. Enfin, en matière de durée de conservation, les États membres ont retenu une durée « normale » de conservation à 12 mois, une durée plus courte (6 mois) pouvant être prévue en cas de circonstances exceptionnelles.

Malgré ces éléments, le Parlement a rejeté une première fois le 7 juin 2005 le projet de décision-cadre en raison des incertitudes qui régnaient autour du choix de la base juridique et de la proportionnalité des mesures. Après examen du texte par la Commission des libertés publiques et malgré le contexte (attentats de Londres), le Parlement a définitivement rejeté le projet de décision-cadre sur la rétention des données le 27 septembre 2005. Le 12 octobre, le Conseil de l'Union a néanmoins estimé que la décision-cadre, qui est une option à laquelle un grand nombre de délégations sont favorables, devait «*rester sur la table. Toutefois, une majorité des délégations n'écartaient pas non plus l'idée d'adopter une directive*».

Considérant que le sujet relevait bien du 1<sup>er</sup> pilier de l'Union européenne et non du 3<sup>e</sup>, la Commission européenne a présenté le 21 septembre 2005 une proposition de directive sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE. Elle a vocation à s'appliquer aux données relatives au trafic et aux données de localisation concernant les personnes tant physiques que morales, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'appliquerait pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques.

En application de cette proposition de directive, les États membres devraient veiller à ce que soient conservées les données nécessaires pour retrouver et identifier la source d'une communication, retrouver et identifier la destination d'une communication, déterminer la date, l'heure et la durée d'une communication; déterminer le type de communication, déterminer le dispositif de communication utilisé ou ce qui est censé avoir été utilisé comme dispositif de communication ou localiser le matériel de communication mobile.

S'appuyant sur une analyse d'impact, la proposition de directive a souhaité adopter une approche équilibrée, à savoir des durées de conservation d'un an pour les données relatives au trafic concernant la téléphonie mobile et la téléphonie fixe, et de six mois pour les données relatives au trafic concernant l'utilisation d'internet. Les données conservées ainsi que toute autre information nécessaire concernant ces données devraient pouvoir, à leur demande, être transmises sans délai aux autorités compétentes. Transmise au Parlement, un premier examen de cette proposition a eu lieu le 13 décembre 2005.

---

***Le ministre de l'Intérieur, des Libertés locales et de la Sécurité intérieure, a confié au Forum des droits sur l'internet, le 26 avril 2005, la finalisation de deux propositions avancées dans le rapport du chantier sur la lutte contre la cybercriminalité. Ces propositions concernent la création d'un «certificat citoyen», qui serait attribué aux fournisseurs d'accès et de services internet et «permettrait de mesurer leur engagement contre la cybercriminalité, ainsi que leur contribution au développement de la civilité sur le cyberspace» (protection des mineurs, sécurité informatique...) et le renforcement la coopération entre l'État et l'industrie par la création d'un forum dédié à ces échanges.***

---

## La responsabilisation des intermédiaires techniques

L'année 2005 a permis aux juges de poursuivre l'application des dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, plusieurs affaires ayant mis en jeu le mécanisme de responsabilisation des intermédiaires techniques instauré par l'article 6 de la loi. En effet, l'article 6-I-8° de la loi prévoit que *«l'autorité judiciaire peut prescrire en référé ou sur requête, à [tout hébergeur] ou, à défaut, à [tout fournisseur d'accès à l'internet], toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne»*.

Cette disposition, qui fait écho aux principes fixés par le Nouveau Code de procédure civile, a été mise en œuvre par deux fois à l'occasion de la diffusion de contenus illicites sur la toile mondiale. Dans un premier temps, saisi par des associations de défense des droits de l'homme, le Tribunal de grande instance de Paris a dû s'interroger sur l'application de ce «référé LCEN» aux fournisseurs d'accès à l'internet en matière de déploiement de mesures de filtrage destinées à interdire l'accès à des contenus racistes, antisémites et appelant à la haine raciale hébergés sur le site de l'association AAARGH (Association des anciens amateurs de récits de guerres et d'holocaustes). Cette procédure judiciaire était entamée le 7 février 2005, en référé, avec une plainte déposée à l'encontre des hébergeurs dudit site négationniste et de divers fournisseurs d'accès à l'internet.

Dans une première ordonnance en date du 25 mars 2005, le juge relevait que les associations demanderesse situaient leur action dans le cadre des dispositions de l'article 6-I-8° de la loi pour la confiance dans l'économie numérique.

Le juge a souhaité, dans un premier temps, vérifier le fait que les prestataires d'hébergement du site contesté avaient bien été convoqués à l'audience. Devant l'absence de certaines pièces justificatives, le juge renvoyait à une deuxième audience le soin d'examiner la demande des associations. Une deuxième ordonnance du 20 avril 2005 venait répondre aux arguments soulevés par les fournisseurs d'accès à l'internet indiquant qu'il convient – avant toute action à l'encontre des prestataires techniques – d'identifier l'auteur ou l'éditeur du site. Le juge a rejeté cet argument soutenant qu'à la lumière des débats tenus *«préalablement à l'adoption de la loi n° 2004-575 du 21 juin 2004 [...], il s'agit d'examiner les demandes en considération du principe d'efficacité ayant inspiré le législateur dans la mise en place d'un dispositif qui s'adresse, non pas à l'éditeur ou aux auteurs ayant contribué à l'élaboration du contenu d'un site mis en cause, mais aux prestataires techniques»*.

Le juge poursuit en analysant le contenu incriminé. Il relève notamment que *«le caractère manifestement illicite du contenu mis en ligne par l'association AAARGH n'est contesté par aucun des fournisseurs d'accès, ni par l'AFA; que la société ThePlanet.com Internet Services, prestataire d'hébergement maintient pour sa part l'accès au service de communication en ligne AAARGH»*.

En outre, le juge précise que *«l'affichage du contenu de ce site et son architecture conduisent à retenir que c'est en totalité que celui-ci se présente comme manifestement illicite, toute distinction au niveau de la mesure de retrait entre telle ou telle publication se révélant, au moins sur le plan technique, à la fois impraticable et ineffi-*

«cace». En conséquence, le tribunal ordonne aux hébergeurs qu'il soit mis fin à l'accès au site en question afin de faire cesser le dommage. Il décide également de fixer une nouvelle audience destinée à vérifier si ces sociétés ont exécuté leurs obligations.

Dans une troisième et dernière ordonnance du 13 juin 2005, et devant la «nécessité de mettre fin sans atermoiement supplémentaire au dommage», le juge a ordonné aux fournisseurs d'accès à l'internet de prendre des mesures propres à faire cesser le dommage. L'argument, soulevé par les prestataires, tiré de «l'inefficacité des mesures» et du «risque de déménagements successifs [du site] dans des "paradis numériques"» est écarté et ne saurait «justifier un renoncement à agir».

En conséquence, mais sans astreinte, il a été fait obligation aux fournisseurs d'accès à l'internet de mettre en œuvre tous les moyens dont ils peuvent disposer en l'état actuel de leur structure et de la technologie pour empêcher l'accès au site, dont ils ne contestent d'ailleurs pas le caractère illégal. Ces mesures devaient être mises en œuvre dans un délai de 10 jours, avec l'obligation de rendre compte aux associations demanderesse des dispositifs techniques mis en place pour atteindre l'objectif assigné. Les demanderesse devaient, pour leur part, tenir les fournisseurs d'accès à l'internet informés de l'état des procédures engagées à l'encontre des hébergeurs et, le cas échéant, des mesures qui pourraient conduire à l'allègement ou à la levée du filtrage imposé. Notons que dans le cadre de cette procédure, le juge a tenu à faire une application stricte de la loi. Il a tout d'abord établi le caractère manifestement illicite du contenu, avant d'enjoindre aux hébergeurs de prendre les mesures propres à faire cesser le trouble. C'est uniquement devant l'absence de réaction de ces prestataires que le juge a ordonné aux fournisseurs d'accès à l'internet de déployer des mesures de filtrage. Suite à cette décision, les membres de l'AFA ont annoncé, dans un communiqué, qu'ils entendaient appliquer l'injonction qui leur était faite, tout en indiquant qu'ils faisaient appel de la décision.

Sur le même fondement de l'article 6-I-8° de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, une action a été engagée à l'encontre de prestataires étrangers hébergeant un site permettant aux internautes français de faire des paris sportifs en ligne. Constatant qu'une société établie à Malte proposait un service de paris sportifs en ligne, le Pari mutuel urbain (PMU) saisissait la justice. Dans une première ordonnance du 8 juillet 2005, le Tribunal de grande instance de Paris ordonnait à la société Zeturf de mettre fin à son activité de prise de paris en ligne sur les courses hippiques organisées en France, et ce sous astreinte provisoire de 15000 €. Par notification en date du 1<sup>er</sup> septembre 2005 à l'hébergeur français du site, le PMU portait à la connaissance du prestataire le caractère illicite du site en cause, tel qu'en avait décidé le juge. En réponse, l'hébergeur lui indiquait avoir procédé «aux opérations qui lui incombaient afin que la connexion à l'internet des serveurs Zeturf par elle hébergés soit interrompue». Seulement, quelques heures après, le site était transféré chez un nouvel hébergeur britannique qui, à la demande du PMU, suspendait le service.

Réagissant, la société de paris en ligne décida de faire procéder à l'hébergement de ses services par des prestataires maltais. Le PMU porta à la connaissance de ces hébergeurs le caractère illicite du site, ceux-ci refusant alors de suspendre les pages incriminées. Le PMU s'adressa donc, à nouveau, au Tribunal de grande instance de



Paris afin d'obtenir une injonction du juge en faveur d'une suspension du site incriminé. Dans une nouvelle ordonnance du 2 novembre 2005, le juge a ordonné aux prestataires de «*rendre l'accès au site Zeturf impossible tant qu'y sera maintenue l'activité de paris en ligne, et ce sous astreinte provisoire de 1 500 € par jour de retard*».

## La responsabilité de l'éditeur du site

Deux décisions rendues, l'une par la Cour d'appel de Paris et l'autre par la Cour de cassation, sont venues préciser la responsabilité de l'éditeur d'un site à la suite de la publication, sur son site, d'un message ou de propos dont il n'est pas auteur.

Dans l'affaire jugée, le 10 mai 2005, par la Chambre criminelle de la Cour de cassation, le responsable d'un syndicat était poursuivi à la suite de la publication sur son site de propos diffamatoires à l'encontre d'un directeur régional de la Poste. Ces propos avaient été mis en ligne sur le site par l'un des syndicalistes qui suivait le mouvement de revendication. Dans sa décision, la Cour de cassation a posé un principe. Elle a estimé que «*le réseau internet constituant un moyen de communication audiovisuelle au sens de l'article 2 de la loi du 30 septembre 1986 relative à la liberté de communication, la responsabilité pénale du propriétaire d'un site et de l'auteur des propos injurieux ou diffamatoires diffusés sur ce site peut être engagée dans les conditions prévues par l'article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle*». En conséquence, les juges suprêmes ont confirmé la responsabilité première du directeur de la publication, à savoir le responsable du syndicat.

Notons que la Cour de cassation, assimile l'internet à un moyen de communication audiovisuelle. Or, la loi du 21 juin 2004 a autonomisé l'internet à travers la notion de communication au public en ligne, distincte de la notion de communication audiovisuelle. Néanmoins, les faits étant antérieurs à l'entrée en vigueur de la loi pour la confiance dans l'économie numérique, la Cour de cassation ne pouvait tenir compte de cette modification, sans conséquence pour ce qui est de l'application de l'article 93-3 qui demeure applicable pour les propos diffusés sur l'internet.

Dans une seconde affaire, jugée par la Cour d'appel de Paris le 10 mars 2005, les juges ont eu à examiner la responsabilité de l'exploitant d'un forum de discussion à la suite de la publication de propos provoquant à la discrimination, à la haine ou à la violence à l'égard de groupes ou de personnes à raison de leur appartenance respective à une ethnie, une nation, une race ou une religion déterminée. Les juges ont retenu la responsabilité première de l'exploitant en application de l'article 93-3 de la loi du 29 juillet 1982, non pas en sa qualité de directeur de la publication, mais en sa qualité de producteur.

En effet, l'article 93-3 prévoit qu'au «*cas où l'une des infractions prévues par le chapitre IV de la loi du 29 juillet 1881 sur la liberté de la presse est commise par un moyen de communication audiovisuelle, le directeur de la publication ou [...] le codirecteur de la publication sera poursuivi comme auteur principal, lorsque le message incriminé a fait l'objet d'une fixation préalable à sa communication au public*». Or, le forum de discussion n'étant pas modéré, les juges ont considéré qu'il n'y avait pas fixation préalable du message. En conséquence, la responsabilité du directeur

de la publication ne pouvait être retenue. Pour la première fois et par une lecture *a contrario*, les juges assimilent la modération à une fixation préalable au sens de la loi.

Suite à ce constat, les juges d'appel ont fait application d'une jurisprudence constante de la Cour de cassation prévoyant qu'il «*résulte de l'article 93-3 que lorsqu'une infraction prévue par le chapitre IV de la loi du 29 juillet 1982 est commise par un moyen de communication audiovisuelle, à défaut de poursuites contre l'auteur du message illicite, le producteur du service peut être poursuivi comme auteur principal, même si ce message n'a pas été fixé préalablement à sa communication au public*». Les magistrats ont donc appliqué le deuxième alinéa de l'article 93-3. Ils retiennent la responsabilité de l'exploitant du forum de discussion au titre de son activité de producteur, ce dernier ne pouvant «*invoquer son défaut de vigilance pour échapper à sa responsabilité pénale, étant observé qu'aucun directeur de la publication n'avait été désigné et que les auteurs de messages n'ont pas été identifiés*». Les juges indiquent, en outre, qu'il incombait au concepteur du site «*de contrôler le contenu des messages enregistrés par les internautes*».

En pratique, cette décision responsabilise l'exploitant d'un forum de discussion non modéré a priori, en cas de publication de messages pour lesquels les auteurs ne sont pas identifiables. Rendue sous l'empire d'une loi ancienne, cette jurisprudence doit encore être confirmée. En effet, les débats parlementaires préalables à l'adoption de la loi pour la confiance dans l'économie numérique ont indiqué le souhait d'intégrer dans la catégorie des hébergeurs certains responsables de forums de discussion. Or, l'article 6 de cette loi précise explicitement que les hébergeurs ne peuvent être considérés comme «*producteurs*» au sens de l'article 93-3 de la loi du 29 juillet 1982.

---

***Le Forum des droits sur l'internet a publié le 31 octobre 2005 un dossier «Je blogue tranquille» destiné à informer les internautes des usages et des règles juridiques applicables aux blogs.***

---

## **Protection de l'enfance**

La protection de l'enfance a été une thématique au cœur de l'activité gouvernementale française lors de l'année 2005 avec l'adoption de plusieurs mesures, notamment lors de la Conférence de la famille du 22 septembre 2005.

### L'accompagnement des familles dans leur usage des nouvelles technologies

L'internet constitue un média au cœur des familles françaises. 51 % des foyers sont équipés, dont 42 % connectés à Internet. Plus de 3 millions d'adolescents possèdent un «*blog*». Si l'internet est sans conteste un élément d'enrichissement, d'information, d'éducation et de service pour les familles, il peut également présenter des risques, en particulier pour les enfants (visualisation de contenus préjudiciables, risque de rencontres de personnes malintentionnées, etc.). Les parents ne pouvant rester en marge de ce phénomène et laisser seul leur enfant découvrir cet outil d'information et de communication, il paraît nécessaire de mener des actions de sensibilisation. Il

s'agit de donner aux familles des repères sur la qualité des outils, des services et des contenus proposés et de bénéficier d'outils de sécurisation de la navigation de l'enfant, simples, performants et évolutifs.

À cette fin, le Gouvernement a décidé de lancer, en 2006, une campagne de sensibilisation, en proposant des séquences télévisées d'information courtes mettant en scène des situations réelles, vécues par les familles. Cette campagne télévisée sera prolongée par la diffusion, dans des lieux d'accueil répartis sur l'ensemble du territoire, d'un programme pédagogique proposé gratuitement aux familles, ainsi que par la mobilisation des supports habituels d'information.

---

***Le Forum des droits sur l'internet a remis le 25 janvier 2005 au ministre de la Famille ses secondes recommandations portant sur la protection de l'enfance sur l'internet. Ce rapport établit, pour la première fois en France, une analyse objective et raisonnée des risques d'atteintes sexuelles sur mineurs par le biais de l'internet. Il distingue les deux phénomènes que sont, d'une part, la diffusion de contenus pédo-pornographiques sur l'internet et le risque de contacts pédophiles, d'autre part.***

***Par ailleurs, dans le cadre de la Conférence de la famille qui s'est tenue le 22 septembre 2005, le Premier ministre, Dominique de Villepin, a confié au Forum des droits sur l'internet la mission d'établir le cahier des charges d'un label « Famille ».***

***Enfin, et à la demande des principaux opérateurs français de téléphonie, le Forum a mis en place un groupe de travail ayant pour mission d'élaborer, en concertation avec les partenaires concernés, une grille de classification des contenus multimédias mobiles, protectrice des mineurs.***

---

## La systématisation de l'offre de logiciels de filtrage

Depuis 2000, la loi oblige les fournisseurs d'accès à proposer à leurs internautes des logiciels de protection. Cinq ans après, seuls 15 % des parents disent les avoir mis en place. Prenant en compte cette pratique, une table ronde a été organisée le 16 novembre 2005 par le ministre délégué à la Sécurité sociale, aux Personnes âgées, aux Personnes handicapées et à la Famille avec les fournisseurs d'accès Internet, les opérateurs de téléphonie mobile et les associations familiales et de protection de l'enfance. À l'issue de la réunion, les participants ont signé divers engagements destinés à offrir un ensemble de solutions de contrôle parental qui seront offertes gratuitement aux familles.

Ainsi, les fournisseurs d'accès Internet se sont engagés à fournir à leurs abonnés un outil de contrôle parental performant, facile à installer, et sans surcoût pour l'utilisateur. Le logiciel de contrôle parental devra répondre à un cahier des charges très précis en termes de fonctionnalités. Il offrira notamment des services différenciés (listes blanches, listes noires), selon que l'utilisateur est un enfant ou un adolescent. Le logiciel sera disponible dans tous les kits de connexion à Internet au cours du 1<sup>er</sup> trimestre 2006. Tous les nouveaux abonnés se verront ainsi systématiquement sensibilisés aux risques d'internet et il leur sera fait une proposition d'installation d'un

logiciel de contrôle parental. Parallèlement, les fournisseurs d'accès et les pouvoirs publics se sont engagés à mener des campagnes de communication afin de sensibiliser enfants et parents à ces problématiques et leur permettre d'installer gratuitement ces outils de protection. Les pouvoirs publics se sont, enfin, engagés à discuter avec les éditeurs de ces logiciels en ce qui concerne leur prix et leurs fonctionnalités.

En Europe, le Royaume-Uni et plusieurs pays nordiques (Danemark, Suède, etc.) ont institué, au cours de l'année 2005, des mesures de filtrage par défaut, visant notamment les contenus pédo-pornographiques. Ces mesures résultent d'un partenariat entre les autorités judiciaires et des associations de protection de l'enfance qui élaborent des listes de sites ou de fichiers susceptibles de contenir des images pornographiques mettant en scène des mineurs.

## La responsabilité des créateurs de sites pornographiques accessibles aux mineurs

Complétant la jurisprudence naissante en la matière, la Cour d'appel de Paris a condamné, le 22 février 2005, deux exploitants d'un site internet pornographique pour ne pas avoir pris les mesures tendant à empêcher à des mineurs de pouvoir accéder à ces contenus. En effet, l'article 227-24 du Code pénal, réprime de trois ans d'emprisonnement et de 75 000 euros d'amende, «*le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message*» lorsque ce message est susceptible d'être vu ou perçu par un mineur.

En l'espèce, au cours de l'année 1999, la brigade de répression du proxénétisme de la Préfecture de police de Paris avait constaté qu'un site internet proposait la vente de divers articles érotiques et notamment des cassettes pornographiques dont la publicité était assurée par la diffusion des jaquettes. Lors de l'accès au site, une page d'avertissement apparaissait indiquant que «*ce site est réservé exclusivement aux adultes*». Dès lors que le visiteur cliquait depuis cette page sur le lien «*j'entre*», il accédait aux différentes rubriques.

En première instance, les administrateurs du site étaient condamnés. La Cour d'appel confirme cette condamnation en estimant que «*le caractère pornographique des publicités diffusées sur le site internet en cause n'est pas contesté et le descriptif d'accès à ce site [...] démontre sans équivoque que des mineurs peuvent visionner ces messages et images simplement en se présentant comme étant majeurs et donc sans contrôle efficace*». Or, ajoutent les magistrats, «*l'obligation légale de précaution, par la mise en place de dispositif garantissant l'impossibilité matérielle pour les mineurs d'avoir connaissance des messages, incombe à l'émetteur ou diffuseur et non à celui qui est à même de les recevoir*».

Cette décision confirme la jurisprudence initiée par la Cour d'appel de Paris en avril 2002. Néanmoins, dans cette nouvelle décision, les juges parisiens laissent entrevoir une solution pour les créateurs de sites commercialisant des produits pornographiques. Ils relèvent, en effet, que «*des mesures techniques simples pouvaient être adoptées afin, sinon d'interdire le site aux mineurs, du moins d'ôter tout caractère*

*choquant aux images, techniques d'ailleurs en place sur le site en cause – titre et images mosaïqués dès le début de l'année 2000*». Ainsi, il s'agirait de modifier les images des jaquettes de vidéos pornographiques avant leur mise en ligne, afin d'effacer tout contenu pornographique.

## **Propriété intellectuelle**

À la fin de l'année 2005, le Parlement a débuté l'examen du projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information. Examiné après déclaration d'urgence, ce texte procède à la transposition de la directive communautaire n° 2001/29/CE du 22 mai 2001. Ce texte communautaire est destiné à adapter un cadre commun de réglementation du droit d'auteur et des droits voisins dans les pays de l'Union européenne en considération des évolutions technologiques liées à la société de l'information. Il vise également à mettre en œuvre les traités de l'Organisation mondiale de la propriété intellectuelle (OMPI) du 20 décembre 1996 qui ont été adoptés par l'Union européenne et sont en attente de ratification par l'Union. Ces traités prévoient un certain nombre de mesures qui se retrouvent dans le texte communautaire et le projet de loi français comme les mesures techniques de protection. La directive aurait dû faire l'objet d'une transposition à la fin de l'année 2002. En l'absence, la France s'est vue notifier un avis motivé de carence de la part de la Commission européenne le 13 juillet 2005.

Le projet de loi français porte sur quatre thèmes. Le premier adapte le droit d'auteur aux évolutions technologies engendrées par la société de l'information. Le deuxième concerne les droits d'auteur et droits voisins des agents de l'État, des collectivités territoriales et des établissements publics à caractère administratif. Ce dispositif nouveau conduit à la reconnaissance de droit d'auteur et de droits voisins aux fonctionnaires et organise le transfert de ces droits à l'État pour permettre l'accomplissement de la mission de service public. Le troisième intéresse les sociétés de perception et de répartition des droits (autrement appelées sociétés de gestion collective) et le quatrième chapitre est destiné à instituer et à organiser le dépôt légal des sites internet.

Ce projet de loi, présenté au Conseil des ministres le 12 novembre 2003, a suscité de nombreuses interrogations et des positions exprimées avec force conviction dans des sens opposés. La question du *peer-to-peer*, bien que non abordée par le projet de loi est apparue comme focalisant bien des arguments.

En Europe, divers États ont adopté des textes comparables. Tel est le cas de la Norvège qui, au printemps 2005, a pénalisé les atteintes aux droits portant sur des œuvres numériques et la fourniture d'outils permettant le contournement de mesures de protection technique.

---

***Le Forum des droits sur l'internet a publié en décembre 2005 et en amont du débat parlementaire, un dossier présentant les principales dispositions du projet de loi relatif au droit d'auteur et aux droits voisins dans la société de l'information.***

---

## Les poursuites diligentées à l'encontre des éditeurs de logiciels d'échange de fichiers

La Cour Suprême des États-Unis d'Amérique a rendu le 27 juin 2005 une décision d'importance sur la question des échanges *peer-to-peer*. Sans condamner en tant que telle la technique même de ces échanges, la Cour a retenu la possible responsabilité de deux distributeurs de logiciels de *peer-to-peer*. Deux éditeurs de logiciels d'échanges pair à pair, Grokster Ltd. et StreamCast Networks Inc, diffusent des logiciels (Grokster et Morpheus) permettant aux utilisateurs de réaliser le partage direct de fichiers hors de tout système centralisé. Les deux sociétés tirent leurs rémunérations de la publicité commerciale mais non de la distribution des logiciels eux-mêmes qui sont proposés gratuitement aux utilisateurs. Un volume très important de fichiers circule grâce aux logiciels des deux sociétés. Il n'est pas contesté qu'une part très importante des échanges concerne des objets protégés par un copyright.

Ces éditeurs de logiciels d'échange *peer-to-peer* avaient vu leur responsabilité écartée par les juridictions fédérales de l'État de Californie dans l'affaire qui les opposait à Metro-Goldwyn-Mayer Studios Inc et à nombre d'autres sociétés détentrices de droits tant dans le domaine du cinéma que de la musique. Leur responsabilité avait alors été engagée sur le fondement d'une responsabilité secondaire issue de la *common law* se décomposant en une contrefaçon par complicité (*contributory infringement*) et une responsabilité du fait d'autrui (*vicarious liability*) lorsque la personne dispose du droit ou du pouvoir d'empêcher la contrefaçon primaire et retire un bénéfice financier. «*One infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise the right to stop or limit it.*»

C'est sous le couvert de la jurisprudence de 1984 connue sous le nom de Sony ou Betamax que les juges d'appel avaient pu écarter la responsabilité secondaire des défendeurs. En effet selon cette jurisprudence de la Cour suprême, n'est pas engagée la responsabilité de ceux qui diffusent des matériels utilisés en partie pour réaliser des actes illicites dès lors que ces mêmes matériels peuvent être utilisés pour réaliser des actes licites. Cependant, la Cour suprême estime que la juridiction inférieure n'a pas correctement interprété la jurisprudence Sony. L'erreur consiste à écarter la responsabilité des éditeurs au seul motif que leurs produits étaient susceptibles d'un nombre substantiel d'utilisations non contrefaisantes. «*One who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, going beyond mere distribution with knowledge of third-party action, is liable for the resulting acts of infringement by third parties using the device, regardless of the device's lawful uses.*»

Ainsi, le juge d'appel aurait dû examiner le comportement des éditeurs. Cette analyse l'aurait conduit à prendre en considération que les éditeurs : s'étaient positionnés pour récupérer la clientèle du défunt Napster, n'avaient jamais développé d'outils de contrôle permettant de limiter les contrefaçons et avaient tiré un profit de la vente d'espace publicitaire en corrélation avec le volume d'utilisation des logiciels. En conséquence, les éditeurs peuvent être tenus pour responsables selon la Cour suprême mais apparemment en raison de leur stratégie commerciale et non par le simple fait de distribuer un logiciel de *peer-to-peer*. L'affaire sera donc réexaminée et le débat certainement relancé

outré-Atlantique. Quelques mois après cette décision, le site Grokster a accepté, en novembre 2005, de procéder à la fermeture de son service.

Côté Pacifique, la Cour suprême australienne a également tranché le 5 septembre 2005, le différend opposant l'industrie culturelle aux éditeurs du logiciel d'échange de fichiers Kazaa. Bien que les juges n'aient pas déclaré le logiciel illégal, ils ont considéré que la plate-forme incitait les internautes à s'échanger des fichiers en violation des droits de propriété intellectuelle et elle l'a donc condamnée à mettre en œuvre des systèmes de filtrage de ses contenus.

## Les poursuites diligentées à l'encontre des utilisateurs des réseaux *peer-to-peer*

Entamées au cours de l'année 2004, plusieurs poursuites judiciaires ont abouti à des décisions rendues par de nombreux tribunaux correctionnels. Une analyse de celles-ci montre une hétérogénéité dans le traitement judiciaire à la fois du téléchargement mais également de l'échange de fichiers. La première condamnation d'un internaute date du 2 février 2005. Elle a été ordonnée par le Tribunal correctionnel de Pontoise. Alexis B. était poursuivi pour avoir diffusé plus de 10 000 fichiers musicaux par l'intermédiaire de réseaux *peer-to-peer*. En matière d'incrimination, l'élément matériel de l'infraction ressortait du « *téléchargement d'environ 10 000 œuvres musicales provenant d'autres ordinateurs connectés pour la plupart et de la mise à disposition des internautes de ces fichiers téléchargés* ». Par ailleurs, l'élément légal consistait, quant à lui, dans le transfert de programmes ou de données d'un ordinateur vers un autre. Cette action, précisent les magistrats, constitue « *un acte de reproduction, chaque fichier d'une œuvre numérisée étant copié pour être stocké sur le disque dur de l'internaute qui le réceptionne et d'un acte de représentation consistant dans la communication de l'œuvre au public des internautes par télédiffusion* ».

Pour autant les juges ont souhaité faire « *une application très modérée de la loi pénale* ». En effet, relèvent-ils, « *ce remarquable outil de communication et d'échanges qu'est internet s'est développé sur une incompréhension lourde de conséquences. Nombre d'internautes ont considéré ou cru qu'il s'agissait d'un univers, lieu de liberté où les règles juridiques élémentaires ne s'appliquaient pas. Or, les utilisateurs de ce système doivent prendre conscience notamment de la nécessaire protection des droits des auteurs, compositeurs ou producteurs des œuvres de l'esprit* ». Alexis B. a été condamné à verser 3 000 euros d'amende avec sursis et 20 000 euros de dommages-intérêts.

Par un jugement du 21 avril 2005, le Tribunal correctionnel de Meaux a condamné quatre internautes qui échangeaient des fichiers contenant des œuvres protégées par le droit d'auteur. Le juge relève qu'il « *résulte de l'article L. 122-5 du Code de la propriété intellectuelle que lorsque l'œuvre a été divulguée, l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, à l'exception des copies d'un logiciel autres que la copie de sauvegarde* ». Ainsi, « *dès lors qu'il n'est pas établi que les copies réalisées sur CR-ROM ont été utilisées de façon collective, elles ne peuvent constituer le délit de contrefaçon, exceptées les copies de logiciels et les copies échangées entre les prévenus qui sortent ainsi de l'usage privé* ».

Poursuivant l'analyse, les magistrats relèvent que « *chacun des prévenus a reconnu avoir téléchargé des fichiers musicaux et vidéos retrouvés sur leurs disques durs ou sur CD Rom, grâce à des logiciels d'échange peer-to-peer leur permettant d'accéder à des fichiers stockés par d'autres internautes, sous réserve que, dans le même temps, ils mettent à disposition des autres internautes une partie de leurs fichiers. Ils ont admis que chaque fichier téléchargé avait été ainsi, au moins à une certaine période, proposé en téléchargement sur ce réseau* ». Une telle mise à disposition « *par télédiffusion d'œuvres dont ils ne détenaient pas les droits est constitutive du délit de contrefaçon prévu à l'article L. 335-4 du Code de la propriété intellectuelle* ».

Enfin, le Tribunal de grande instance de Chateauroux a condamné le 16 novembre 2005 un internaute à deux mois de prison avec sursis pour avoir mis à disposition d'autres internautes des fichiers musicaux sur les réseaux *peer-to-peer*.

Parallèlement à ces condamnations en matière d'échange de fichiers, plusieurs magistrats ont eu à connaître la simple question du téléchargement. Confirmant le jugement rendu par le Tribunal correctionnel de Rodez à la fin de l'année 2004, la Cour d'appel de Montpellier, par son arrêt du 10 mars 2005, a relaxé un internaute qui était poursuivi pour avoir téléchargé des fichiers par l'intermédiaire de réseaux *peer-to-peer*. Les juges relèvent que « *le prévenu a déclaré avoir effectué les copiés uniquement pour un usage privé; qu'il n'est démontré aucun usage à titre collectif* ». On ne peut déduire « *de ces seuls faits que les copies réalisées ne l'ont pas été en vue de l'usage privé visé par le texte* ». En conséquence, les juges confirment la relaxe. Les industries culturelles, parties à l'affaire, se sont pourvues en cassation.

Cette question du statut du téléchargement rejaille également dans le cadre d'actions où diverses incriminations sont poursuivies. Ainsi, dans le cadre d'une procédure dite du « *plaider coupable* », le Président du Tribunal de grande instance du Havre a homologué, en septembre 2005, la proposition de peine formée par le Procureur de la République à l'encontre d'un internaute poursuivi pour échange et téléchargement de fichiers musicaux. Le tribunal a confirmé la peine de 500 euros d'amende pour l'échange de fichiers. Le procureur n'avait pas, au préalable, retenu l'infraction de reproduction de fichiers.

Enfin, le Tribunal correctionnel de Bayonne a apporté, en novembre 2005, une dernière précision estimant qu'un internaute ayant échangé des fichiers musicaux ne pouvait être poursuivi que sur le fondement de la mise à disposition de ceux-ci et non pas pour une éventuelle atteinte au droit de reproduction ou pour recel d'œuvres contrefaisantes.

En Europe, des poursuites similaires ont été intentées contre les utilisateurs des réseaux d'échange de fichiers. Ainsi, au Royaume-Uni, des poursuites ont été engagées, en août 2005, à l'encontre de cinq internautes identifiés à l'aide de leurs fournisseurs d'accès à l'internet. Ils n'avaient pas accepté la proposition de transaction émise par l'industrie musicale britannique, tendant au règlement amiable du différend.

## Les questions relatives aux liens hypertextes

Au cours de l'année 2005, plusieurs décisions sont venues confirmer la première tendance jurisprudentielle en matière de responsabilité des prestataires de services



publicitaires en cas d'usage, par un tiers et sans autorisation, d'une marque déposée. Ainsi, dans un jugement du 4 février 2005, Louis Vuitton Malletier a fait condamner la société Google qui avait permis à des internautes de créer des liens commerciaux vers des sites proposant des produits contrefaisants. Dans leur décision, les juges relèvent que les prestations de services publicitaires de type «liens commerciaux» sortent du champ des prestations offertes par les intermédiaires techniques, fournisseurs d'accès, hébergeurs de sites ou prestataires de stockage, et par conséquent de leur régime de responsabilité limitée. Par ailleurs, les courts textes qui révèlent, dans une formulation ramassée, le contenu des sites regroupés sous l'expression «liens commerciaux», présentent le caractère d'une communication réalisée à titre onéreux et destinée à promouvoir directement des produits offerts à la vente sur des sites qui ont une activité commerciale, et constituent en conséquence des textes à caractère publicitaire.

Les juges en ont déduit que la société qui agit comme titulaire du support publicitaire et propose aux annonceurs de faire figurer leurs annonces sous une rubrique dont l'intitulé, «liens commerciaux» engage donc sa responsabilité dans la réalisation de la présentation trompeuse de ces publicités et de leur diffusion.

Cette responsabilité du prestataire a été confirmée par la Cour d'appel de Versailles dans un arrêt du 10 mars 2005 opposant le moteur de recherche Google à l'agence de voyages en ligne «Bourse des vols». En l'espèce, le cyber-marchand contestait l'utilisation de sa marque et sa dénomination sociale par un autre voyageur afin de faire afficher des «liens commerciaux» en faveur de ce concurrent. Tout d'abord, les juges relèvent qu'une société exerçant la double activité de moteur de recherche et de prestataire de positionnement payant ne peut se prévaloir du bénéfice des dispositions légales ou jurisprudentielles applicables aux intermédiaires techniques lorsque c'est en sa seule qualité de prestataire de positionnement payant que sa responsabilité est recherchée. Ainsi, le prestataire de positionnement payant engage sa responsabilité dès lors qu'il n'a pas effectué un contrôle préalable des mots-clés réservés par ses clients afin d'interdire l'utilisation de mots-clés manifestement illicites (contraires aux bonnes mœurs, contrefaçon de marques notoires, etc.). Les juges précisent néanmoins que le prestataire ne saurait être tenu à une obligation de surveillance générale concernant la sélection de mots-clés par les exploitants de sites référencés.

Par ailleurs, la cour d'appel a considéré que l'impuissance du prestataire de positionnement payant à empêcher les agissements répréhensibles de ses clients ou à faire cesser leurs conséquences dommageables ne constitue pas un cas de force majeure susceptible de l'exonérer de sa responsabilité dès lors qu'il est avéré que d'autres prestataires dans le domaine du positionnement payant, confrontés à la même difficulté, ont su y remédier rapidement, et que le prestataire est parvenu, quoiqu'avec retard, à le faire également. En conséquence, la cour confirme la condamnation du moteur de recherche. En particulier, elle estime que dans le cas de l'utilisation illicite de marques en tant que mots clés par un client d'un prestataire de positionnement payant, le préjudice économique pour le titulaire des marques est une perte de chance, dans la mesure où il n'avait aucune garantie que les internautes détournés vers d'autres sites seraient tous devenus ses clients. Dans ces conditions, le préjudice doit être évalué en se fondant sur «*le volume global du tourisme en ligne, l'évolution du chiffre d'affaires du titulaire des marques et le taux d'utilisation du moteur de recherche exploité par le prestataire de positionnement payant*».

## Les enjeux de la protection d'une œuvre dans le contexte international

Par deux décisions, la justice française a dû analyser l'application du droit de la propriété intellectuelle à la suite d'agissements perçus depuis le territoire français mais diffusés sur des sites internet étrangers.

Tout d'abord, le Tribunal de grande instance de Paris a examiné, le 7 janvier 2005, une affaire dans laquelle une société française contestait l'utilisation, par une société libanaise, d'une marque sur son site internet. Les juges relèvent que les conditions d'application des dispositions de l'article L. 713-3 du Code de la propriété intellectuelle incriminant la contrefaçon par imitation d'une marque doivent être appréciées à l'aune de l'article 5-1 de la Directive (CE) n° 89/104 du 21 décembre 1988 dont elles constituent la transposition, et qui dispose que *«Le titulaire [d'une marque enregistrée] est habilité à interdire à tout tiers, en l'absence de son consentement de faire usage, dans la vie des affaires: [...] b) d'un signe pour lequel, en raison de son identité ou de sa similitude avec la marque et en raison de l'identité ou de la similitude des produits ou des services couverts par la marque et le signe, il existe, dans l'esprit du public, un risque de confusion qui comprend le risque d'association entre le signe et la marque»*. Ainsi, la contrefaçon suppose qu'il soit fait usage de la marque imitée dans la vie des affaires, laquelle a été définie par la Cour de justice des Communautés européennes, dans son arrêt du 12 novembre 2002, comme désignant une *«activité commerciale visant à un avantage économique»*.

Or, il apparaît que le site incriminé, certes accessible en France, est exclusivement rédigé en langue anglaise même en «cliquant» sur le drapeau français. Par ailleurs, *«les contacts affichés renvoient tous à des adresses situées au Liban sans la moindre précision quant aux modalités permettant d'obtenir une commercialisation du produit en France»*. En conséquence, les juges estiment que dans ces conditions, *«il n'est pas établi que la société fait, depuis son site Internet libanais, une offre à la vente de ses produits à destination de la France, de sorte qu'aucun acte d'exploitation de quelque nature que ce soit de la marque opposée n'est accompli par cette société sur le territoire français de nature à justifier une mesure d'interdiction sur ce territoire»*. La contrefaçon par imitation de la marque n'est donc pas caractérisée et le juge a rejeté l'ensemble des demandes.

Dans une affaire jugée le 11 janvier 2005 par la Cour de cassation, la société Hugo Boss poursuivait la société Reemtsma, afin de lui voir interdire tout usage des marques «Boss». À l'occasion de son pourvoi, la société Boss indiquait que *«constitue un usage de marque en France, l'utilisation d'une marque sur un support accessible en France, tel qu'un site internet»*. En effet, la Cour d'appel avait refusé de faire droit à ses demandes estimant qu'il n'y avait pas infraction car le site incriminé,

rédigé en langues étrangères et dont il résultait que les produits n'étaient pas disponibles en France, n'aurait pas visé le public de France.

Confirmant cette décision des juges du fond, la Cour de cassation affirme dans son arrêt que *« ayant relevé qu'il se déduit des précisions apportées sur le site lui-même que les produits en cause ne sont pas disponibles en France, la cour d'appel en a exactement conclu que ce site ne saurait être considéré comme visant le public de France, et que l'usage des marques «Boss» dans ces conditions ne constitue pas une infraction à l'interdiction prononcée par jugement du 23 juin 2000 »*. Les juges suprêmes confirment donc l'arrêt d'appel.

## **Commerce électronique**

À l'occasion de ses vœux aux «forces vives» en janvier 2005, le Président de la République s'est prononcé en faveur d'un renforcement de la protection des consommateurs, notamment lors de leurs achats sur l'internet. Ainsi, il a estimé que, pour favoriser la consommation, il est nécessaire d'assurer une bonne concurrence, suffisamment régulée afin de *« donner plus de pouvoir d'achat et de pouvoir économique aux consommateurs »*. Ainsi, il a considéré qu'il fallait donner *« aux Français la possibilité, sans être pénalisés, de changer rapidement de banque, d'assureur, d'opérateur de téléphonie, de fournisseur d'accès Internet »*. Une telle solution remettrait en cause la pratique actuelle de plusieurs opérateurs imposant des durées minimales d'abonnement de 12 ou 24 mois selon les offres proposées sur le marché.

Par ailleurs, et s'inspirant des règles existantes en droit anglo-saxon, le Président de la République s'est prononcé en faveur d'une transposition des principes de la *class action* en droit français. En effet, selon lui, il *« faut donner aux consommateurs les moyens de faire respecter leurs droits: aujourd'hui, ils sont démunis parce que, pris séparément, aucun des préjudices dont ils sont victimes n'est suffisamment important pour couvrir les frais d'une action en justice »*. Dans cet optique, il a demandé au Gouvernement *« de proposer une modification de la législation pour permettre à des groupes de consommateurs et à leurs associations d'intenter des actions collectives contre les pratiques abusives observées sur certains marchés »*.

En droit anglo-saxon, cette procédure permet à un particulier d'agir en vue d'obtenir un jugement au profit d'un ensemble de personnes appartenant à une catégorie sociale ou économique (les consommateurs). Pour certains, *« une telle procédure [...] constitue, à la disposition des groupes de pression, l'instrument d'une action politique plutôt que juridictionnelle »* (Guinchard S. et a., *Droit processuel*, Précis, Dalloz, 2003). En France, après plusieurs débats en 1986/1987, cette procédure n'avait finalement pas été introduite dans notre droit.

Outre ces annonces, l'année 2005 a été l'occasion pour le pouvoir législatif ou réglementaire de renforcer la protection du consommateur en créant, dans notre droit positif, plusieurs dispositions protectrices de celui-ci.

---

***Le Forum des droits sur l'internet a publié le 19 mai 2005 son second rapport en matière de cyber-consommation abordant la problématique des***

## L'encadrement de la tacite reconduction des contrats de consommation

Par une loi du 28 janvier 2005 tendant à conforter la confiance et la protection du consommateur, le législateur a souhaité fixer de nouvelles règles au mode de reconduction des contrats. Le texte a créé un nouvel article L. 136-1 au sein du Code de la consommation. Cette disposition indique que *«le professionnel prestataire de services informe le consommateur par écrit, au plus tôt trois mois et au plus tard un mois avant le terme de la période autorisant le rejet de la reconduction, de la possibilité de ne pas reconduire le contrat qu'il a conclu avec une clause de reconduction tacite»*.

À défaut d'information, *«le consommateur peut mettre gratuitement un terme au contrat, à tout moment à compter de la date de reconduction. Les avances effectuées après la dernière date de reconduction ou, s'agissant des contrats à durée indéterminée, après la date de transformation du contrat initial à durée déterminée, sont dans ce cas remboursées dans un délai de trente jours à compter de la date de résiliation, déduction faite des sommes correspondant, jusqu'à celle-ci, à l'exécution du contrat. À défaut de remboursement dans les conditions prévues ci-dessus, les sommes dues sont productives d'intérêts au taux légal»*.

En pratique, ce texte pose le principe d'une information *«par écrit»* du consommateur préalablement à la reconduction tacite de son contrat. Néanmoins, la loi ne précise pas les modalités d'intervention de cet écrit (papier, courrier électronique, affichage sur le site internet, etc.). Entrées en vigueur le 1<sup>er</sup> août 2005, ces dispositions ne s'appliquent qu'aux contrats en cours à cette date.

## L'archivage des contrats électroniques

Premier texte d'application de la loi pour la confiance dans l'économie numérique, un décret du 16 février 2005 apporte des précisions en matière d'archivage des contrats électroniques. Aux termes de l'article 27 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, il est créé un article L. 134-2 au sein du Code de la consommation prévoyant que *«lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret, le contractant professionnel assure la conservation de l'écrit qui le constate pendant un délai déterminé par ce même décret et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande»*. Afin d'être opérationnelle, cette disposition nécessitait l'adoption d'un décret qui a été publié le 18 février 2005 au Journal officiel.

Le texte fixe tout d'abord à 120 euros le montant à partir duquel, l'archivage du contrat doit avoir lieu. L'objectif recherché par cette obligation est double: permettre au consommateur d'accéder aux conditions générales et particulières de la vente ou de la prestation de service et assurer au cyber-marchand une certaine sécurité juridique limitant la remise en cause des conventions conclues.

L'article 2 du décret précise que le délai de conservation est fixé à 10 ans à compter de la conclusion du contrat «*lorsque la livraison du bien ou l'exécution de la prestation est immédiate*». Dans le cas contraire, «*le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci*». Ces nouvelles dispositions sont entrées en vigueur le 19 février 2005.

---

***Le Forum des droits sur l'internet a publié le 1er décembre 2005 une Recommandation sur la conservation électronique des documents.***

---

## La nouvelle responsabilité civile des transporteurs postaux

Suite directe de la loi pour la confiance dans l'économie numérique, les parlementaires ont procédé, par la loi du 20 mai 2005, à une modification du régime de responsabilité applicable aux services postaux, et plus exactement à la Poste. Celle-ci était auparavant irresponsable pour tous les envois «non spéciaux» en vertu du Code des postes et communications électroniques. Ce principe avait été vivement critiqué, en particulier par les cyber-marchands, soumis depuis la loi du 21 juin 2004 à un régime de responsabilité de plein droit. La loi réécrit l'article L. 7 du Code des postes et des communications électroniques en prévoyant que «*la responsabilité des prestataires de services postaux au sens de l'article L. 1 est engagée dans les conditions prévues par les articles 1134 et suivants et 1382 et suivants du code civil à raison des pertes et avaries survenues lors de la prestation*». Il s'agit ici d'une application des règles du droit commun. En cas d'inexécution contractuelle (vis-à-vis de l'expéditeur) ou de faute (vis-à-vis du destinataire), le transporteur pourra voir sa responsabilité être engagée et retenue.

Pour autant, le texte fixe une limite à cet engagement. En effet, «*cette responsabilité tient compte des caractéristiques des envois et des tarifs d'affranchissement selon des modalités fixées par un décret en Conseil d'État qui détermine des plafonds d'indemnisation*». En clair, plus un colis est envoyé selon un envoi «simple», moins l'indemnisation sera importante.

Le nouvel article L. 8 du Code prévoit un régime identique pour «*les dommages directs causés par le retard dans la distribution d'un envoi postal*».

Complétant ce mécanisme, l'article L. 9 du Code impose une obligation d'information aux prestataires sur les tarifs, les limitations éventuelles de la responsabilité contractuelle, le délai de prescription d'un an à compter du lendemain du jour du dépôt de l'envoi (fixé à l'article L. 10) et les conditions particulières de la vente.

Compte tenu de l'alignement sur le régime contractuel de droit commun, cette nouvelle disposition va permettre au prestataire d'instituer des clauses limitatives de responsabilité. À ce titre, selon la jurisprudence Chronopost de la Cour de cassation, le prestataire ne pourra pas se dégager de l'exécution d'une obligation substantielle du contrat. Pour contourner les éventuelles limitations contractuelles, l'utilisateur aura la possibilité d'invoquer la faute lourde du prestataire postal. Selon une récente jurisprudence de la Chambre mixte de la Cour de cassation (Cass. Mix., 22 avril 2005, n° 02-18326; Cass. Mix., 22 avril 2005, n° 03-14112), une telle faute ne peut résulter

du seul retard de livraison (deuxième arrêt) même si le transporteur ne peut pas fournir d'explication sur celui-ci (premier arrêt). Le cocontractant du transporteur devra donc «*établir un ensemble de faits révélant la négligence ou l'incurie du transporteur*» (E. Chevrier, *La fin de l'affaire Chronopost ?* D. 2005, p. 1224).

## La dématérialisation de certaines formalités et procédures contractuelles

La loi pour la confiance dans l'économie numérique (LCEN) avait autorisé le pouvoir exécutif à procéder par voie d'ordonnance pour l'adaptation des dispositions législatives subordonnant la conclusion, la validité ou les effets de certains contrats à des formalités autres que celles mentionnées à l'article 1108-1 du Code civil, à savoir l'exigence d'un écrit pour la validité d'un acte juridique et celle d'une mention manuscrite, en vue de permettre l'accomplissement de celles-ci par voie électronique. Prise en application de cette habilitation, une ordonnance du 16 juin 2005 pose plusieurs règles.

Tout d'abord, l'ordonnance crée trois nouveaux articles (1369-1 à 1369-3 du Code civil) qui précisent les modes de mise à disposition ou de communication des conditions contractuelles ou de toute information sur les biens et services. En pratique, l'article 1369-1 prévoit que «*la voie électronique peut être utilisée pour mettre à disposition les conditions contractuelles*» ou opérer «*l'information sur les biens ou services*».

L'article 1369-2 énonce ensuite que «*les informations qui sont demandées en vue de la conclusion d'un contrat ou celles qui sont adressées au cours de son exécution peuvent être transmises par courrier électronique si leur destinataire a accepté l'usage de ce moyen*». À noter que ce texte est sans incidence sur l'application de l'article L. 34-5 du Code des postes et des communications électroniques fixant le régime de la prospection directe par courriel. En effet, le nouvel article du Code civil indique clairement que les informations communiquées par courriel doivent avoir été «*demandées*»: l'envoi résulte donc d'une sollicitation de l'internaute. Ce nouvel article ne fait pas référence à la notion de consentement, notamment prévu par la loi du 21 juin 2004 pour la confiance dans l'économie numérique ou la loi du 6 janvier 1978, mais prévoit juste que le destinataire doit avoir «*accepté l'usage de ce moyen*», ce qui sous-entend qu'une telle acceptation pourrait figurer dans les conditions générales de vente.

Dernier article de la section, l'article 1369-3 du Code civil prévoit que lorsque les informations sont destinées à un professionnel, celui-ci «*ne peut refuser ce mode de communication*», comme le précise le rapport sur l'ordonnance, dès lors qu'il a communiqué son adresse électronique, le texte prévoyant que «*les informations [...] peuvent lui être adressées [...] dès lors qu'il a communiqué*» son adresse.

Ensuite, une nouvelle section, composée des articles 1369-7 à 1369-9 du Code civil, traite de l'équivalent électronique de l'envoi par lettre simple ou par lettre recommandée dans le cadre de la conclusion ou de l'exécution d'un contrat.

L'article 1369-7 du Code civil adapte tout d'abord le cas où l'envoi d'un écrit par lettre simple est prescrit. Ainsi, le recours à un mode électronique sera possible dès lors

qu'un procédé électronique, dont la fiabilité est présumée s'il satisfait à des exigences qui seront fixées par un décret en Conseil d'État, garantit la datation de l'envoi.

Ce texte pourrait influencer les dispositions de l'article L. 312-7 du Code de la consommation qui prévoit, en matière de crédit immobilier, que «*le prêteur est tenu de formuler par écrit une offre adressée gratuitement par voie postale à l'emprunteur éventuel ainsi qu'aux cautions déclarées par l'emprunteur lorsqu'il s'agit de personnes physiques*».

Allant plus loin, l'article 1369-8 du Code civil pose les conditions de l'envoi d'une lettre recommandée, avec ou sans accusé de réception, par voie de courrier électronique. Deux cas sont prévus par cette nouvelle disposition : l'envoi sous forme électronique et la réception sous format papier et l'envoi et la réception sous forme électronique. Dans ce deuxième cas, le texte prévoit que le destinataire qui ne serait pas un professionnel doit avoir accepté explicitement l'usage de ce moyen.

Dans tous les cas, le procédé utilisé par l'expéditeur doit permettre de l'identifier, de garantir l'identité du destinataire et d'établir que la lettre a été remise ou non à ce dernier. De même, la date d'expédition voire celle de réception pourront être présumées si le procédé auquel a eu recours l'expéditeur répond aux conditions qui seront fixées par un décret en Conseil d'État.

Lorsque la lettre recommandée est assortie d'un accusé de réception, celui-ci peut être adressé à l'expéditeur par voie électronique ou par tout autre dispositif permettant sa conservation.

Enfin, le nouvel article 1369-9 adapte l'exigence de remise matérielle de certains documents au cocontractant en prévoyant (à l'exception des hypothèses visées aux articles 1369-1 et 1369-2) que cette remise est effective lorsque le destinataire en accuse réception après avoir pu en prendre connaissance. De même, la simple remise d'un écrit électronique à l'intéressé vaut lecture si une disposition prévoit que l'écrit doit être lu au destinataire.

Par ailleurs, deux dernières dispositions sur certaines exigences de forme sont créées au sein du Code civil. Tout d'abord l'article 1369-10 prévoit que lorsque l'écrit sur papier est soumis à des conditions particulières de lisibilité ou de présentation, l'écrit sous forme électronique doit répondre à des exigences équivalentes. Tel est le cas par exemple de l'article L. 112-3 du Code des assurances qui prévoit que «*le contrat d'assurance et les informations transmises par l'assureur au souscripteur mentionnées dans le présent code sont rédigés par écrit, en français, en caractères apparents*».

Ensuite, le deuxième alinéa de l'article 1369-10 prévoit que l'exigence d'un formulaire détachable est satisfaite par un procédé électronique qui permet d'accéder au formulaire et de le renvoyer par la même voie. En pratique, cela signifie que l'écrit devra contenir une adresse électronique (courriel/lien hypertexte) permettant d'accéder à un formulaire et de le renvoyer. Une telle obligation est ainsi prévue par les articles L. 121-24 (démarchage) et L. 311-15 (crédit) du Code de la consommation.

En outre, l'article 1369-11 prend en compte les dispositions imposant l'envoi en plusieurs exemplaires. Ce texte précise que «*l'exigence d'un envoi en plusieurs*

*exemplaires est réputée satisfaite sous forme électronique si l'écrit peut être imprimé par le destinataire».*

Enfin, l'article 2 de l'ordonnance modifie l'article 1325 du Code civil qui impose pour les contrats synallagmatiques, la rédaction d'autant d'actes sous seing privé qu'il existe de parties intéressées. Cette obligation sera dorénavant regardée comme satisfaite pour les contrats électroniques lorsque l'acte est établi et conservé conformément aux articles 1316-1 et 1316-4 et que le procédé permet à chaque partie de disposer d'un exemplaire ou d'y avoir accès.

Parallèlement à cette mesure, deux décrets du 10 août 2005 sont venus préciser les conditions d'établissement, de conservation et de copie des actes authentiques sur support électronique prévus à l'article 1317 alinéa 2 du Code civil. Très attendus par les professionnels, les décrets n° 2005-972 et 2005-973 modifient respectivement le décret du 29 février 1956 relatif au statut des huissiers de justice et le décret du 26 novembre 1971 relatif aux actes établis par les notaires. À cet égard, il convient de rappeler que le Forum des droits sur l'internet avait recommandé l'adoption de décrets par profession dans son avis sur le projet de décret actes authentiques électroniques rendu le 18 novembre 2003. Ces décrets rendent effective la possibilité d'établir des actes authentiques sur support électronique y compris à distance en complément du traditionnel support papier.

Les systèmes techniques permettant l'établissement des actes authentiques électroniques sont soumis à l'agrément des instances professionnelles supérieures de chaque profession, ce qui permettra de garantir l'interopérabilité des systèmes au sein des professions.

Les actes authentiques électroniques dressés par les officiers publics sont signés au moyen d'une signature électronique sécurisée (décret n° 2001-272) mais certains actes conservent les vestiges de « l'acte papier » puisque *« pour leur signature, les parties et les témoins doivent utiliser un procédé permettant l'apposition sur l'acte notarié, visible à l'écran, de l'image de leur signature manuscrite »*.

Ainsi que l'avait recommandé le Forum des droits sur l'internet, la conservation des actes électroniques est assurée par un minutier central placé sous le contrôle de chaque profession concernée. Cette conservation se fait dans des conditions garantissant l'intégrité et la lisibilité de l'acte mais aussi sa traçabilité. L'accès à l'acte est réservé à la personne qui le détient ou l'enregistre dans le minutier central.

Des copies authentiques ou des expéditions des actes peuvent être délivrées quel que soit le support initial de l'acte ou le support final de la copie, confirmant ainsi l'équivalence des supports. Cependant certaines procédures nécessitent encore une « re-matérialisation » de l'acte.

Enfin, il est à noter que ces dispositions s'appliqueront à compter du 1<sup>er</sup> février 2006, délai permettant aux professionnels concernés d'équiper leurs offices.



## La lutte contre les pratiques commerciales illicites ou abusives

En France et à un moment où l'achat d'ordinateurs est en constante augmentation, le ministre en charge de la consommation est venu analyser, par deux réponses ministérielles, la pratique consistant à commercialiser à des particuliers des ordinateurs pré-équipés de certains logiciels (système d'exploitation, traitement de texte, lecteurs multimédias).

Cette analyse est opérée au regard des dispositions de l'article L. 122-1 du Code de la consommation qui prévoit qu'il «*est interdit de refuser à un consommateur la vente d'un produit ou la prestation d'un service, sauf motif légitime, et de subordonner la vente d'un produit à l'achat d'une quantité imposée ou à l'achat concomitant d'un autre produit ou d'un autre service ainsi que de subordonner la prestation d'un service à celle d'un autre service ou à l'achat d'un produit*». Le ministre a rappelé que «*le matériel informatique et les logiciels étant des éléments distincts, l'article L. 122-1 du code de la consommation qui interdit de subordonner la vente d'un produit à l'achat d'une quantité imposée ou à l'achat concomitant d'un autre produit ou d'un autre service ainsi que de subordonner la prestation d'un service à celle d'un autre service ou à l'achat d'un produit s'applique en matière de commercialisation de micro-ordinateurs et de logiciels*». Une exception, prévue par la jurisprudence pourrait être invoquée, «*lorsque la pratique commerciale peut être considérée comme présentant un intérêt pour le consommateur*». Or, si lors de l'arrivée de l'informatique dans les ménages français, le pré-équipement du matériel en logiciel était bénéfique à celui-ci, «*l'élargissement rapide de ce marché et l'information croissante des consommateurs pour tout ce qui concerne les technologies informatiques infléchissent désormais la demande dans le sens d'une diversification de l'offre dans toutes les formes de distribution*».

La commercialisation d'ordinateurs avec des logiciels pré-installés ne présente donc plus aujourd'hui «*d'intérêt pour le consommateur*» et pourrait donc relever de l'incrimination de vente subordonnée. Cette qualification entraîne deux conséquences pour tout vendeur : instaurer des mécanismes de remboursement des licences que le client souhaite refuser et l'informer de cette possibilité de renonciation. Le vendeur pourra également choisir une autre option : proposer dans son offre commerciale les produits complets et chacun des éléments composant le lot (ordinateur « nu », logiciels). Les vendeurs qui ne suivraient pas ces interprétations, si elles étaient confirmées par les juges, risquent 1 500 euros d'amende par infraction constatée. À noter que l'interprétation ainsi donnée par le ministre ne lie pas les magistrats qui pourraient éventuellement avoir à connaître de litiges portant sur ces sujets.

Outre ce rappel de la loi, l'administration a également participé à la poursuite de certains acteurs impliqués dans la diffusion de fausses informations ou en matière de publicité mensongère. Ainsi, et apportant un élément complémentaire à l'important édifice jurisprudentiel créé autour de la société Pere-Noel.fr, un jugement correctionnel du Tribunal de grande instance de Lyon en date du 3 février 2005 a précisé la notion de publicité mensongère. Ce jugement faisait suite à la décision de la DGCCRF de déférer à la justice les plaintes reçues d'internautes à la suite de l'ouverture de la procédure de liquidation judiciaire. En effet, sur l'ensemble des plaintes reçues, 285

personnes restaient non indemnisées par la société au 13 mai 2003 date de l'ouverture de la procédure collective. Sur ces 285 personnes, 169 s'étaient portés partie civile dans l'affaire.

Sur le fondement de l'article L. 121-1 du Code de la consommation qui prohibe toute publicité de nature mensongère ou pouvant induire en erreur un consommateur, les juges ont relevé que *«le délai de livraison annoncé et vérifié par la consultation des pages internet du site de cette société est donné pour»* extrêmement rapide, entre deux et dix jours *«et avait bien pour objet de stimuler la décision d'achat à ce site de commerce électronique le délai apparaissant d'ailleurs un des éléments principaux et mis en avant pour recourir plus particulièrement à la vente en ligne»*. Il a constitué en outre, ont précisé les magistrats, *«une condition de vente des produits électroniques présentés sur le site Pere-Nœl.fr et cette indication renseignait également sur l'aptitude du revendeur à assurer un service efficace et performant et, par voie de conséquence, engageait l'internaute à contracter auprès d'un professionnel supposé être particulièrement efficace»*.

Or, le délai de livraison annoncé s'était avéré faux pour les 485 plaignants ayant saisi la DGCCRF en six mois, ce qui représentait 60 clients par mois. Dans ces conditions, les juges ont considéré que l'élément matériel de l'infraction était constitué. Quant à l'élément moral, les magistrats ont retenu les déclarations de l'ancien PDG de Pere-Nœl. fr qui avait indiqué aux enquêteurs avoir des difficultés d'obtenir certains produits phares. Dans une telle situation, il lui appartenait *«de modifier les délais indiqués afin de tenir compte des difficultés de certains produits et ainsi permettre aux clients de posséder l'information exacte à ce sujet et non une information que le prévenu connaissait pour fausse»*. L'ancien directeur a donc été condamné à 18 mois de prison avec sursis mais également à rembourser, sur ses fonds propres, les clients lésés pour un montant total dépassant les 80 000 euros.

Dans un autre secteur, la 31<sup>e</sup> chambre correctionnelle du Tribunal de grande instance de Paris a condamné le 11 janvier 2005, les dirigeants de deux sociétés spécialisées dans la commercialisation de semences. Ils étaient poursuivis pour avoir continué à faire la promotion de certains de leurs produits traités au Gaucho postérieurement à l'interdiction édictée par le ministère de l'Agriculture. En particulier, il était apparu que les sites continuaient après 1999 de vanter l'utilisation du Gaucho et les vertus des semences de tournesol qui avaient été traitées par ce produit. Au cours de l'audience, les deux dirigeants avaient indiqué que l'information diffusée sur leur site, postérieurement à l'interdiction, l'était par négligence.

Dans cette décision, les juges relèvent que la publicité portant sur un produit dont l'autorisation de mise sur le marché a été retirée, et comportant donc des allégations mensongères en conseillant aux acquéreurs potentiels un produit non conforme à la réglementation, constitue une infraction de publicité mensongère. Ils notent également qu'est sans incidence sur le caractère délictuel de cette publicité, le fait qu'il n'ait pas été possible d'effectuer un achat en ligne ou même de passer une commande par l'intermédiaire du site comportant cette publicité. Pour les magistrats, le défaut de vigilance dans la mise à jour du site de son responsable, professionnel averti, suffit à caractériser l'intention délictuelle. En conséquence, les deux dirigeants

ont été condamnés à 5000 euros d'amende et à verser 1 euro de dommages et intérêts à l'Union nationale de l'apiculture française.

## Le régime de responsabilité de l'affilié et de l'affilieur

Par un jugement du 19 mai 2005, le Tribunal de grande instance de Strasbourg a traité la question – de plus en plus centrale – de la responsabilité de l'affilieur du fait des agissements de ses affiliés. Comme le rappelait le premier rapport du Forum des droits sur l'internet en matière de cyber-consommation du 30 mars 2004, l'affiliation est, pour un site commercial, une technique de promotion et de distribution qui consiste à gérer des partenariats online permettant la constitution d'un réseau de sites partenaires rémunérés à la performance. Elle est donc basée sur un système d'échange entre l'initiateur du programme d'affiliation et un affilié. L'initiateur du programme cherche à accroître sa visibilité, ses ventes. L'affilié, de son côté, cherche à valoriser son audience et à obtenir des revenus supplémentaires grâce à son site. Il met donc en place des liens vers le site de l'initiateur du programme d'affiliation: boutons et bannières, moteurs de recherche, lien texte, lien dans sa lettre d'informations... En échange, l'initiateur du programme d'affiliation le rémunère selon différentes formules qui lui permettent de ne payer que pour les résultats réellement obtenus (pourcentage sur les ventes réalisées). Cette activité peut présenter un risque pour l'affilieur dès lors que celui-ci n'est plus maître de l'utilisation de ses produits par l'affilié. Le jugement du Tribunal de grande instance de Strasbourg en donne une illustration.

En l'espèce, des internautes avaient fait figurer dans le code source de sites pornographiques une marque déposée et ceci sans autorisation de son titulaire. Celui-ci décida de saisir la justice à l'encontre de l'affilieur de ces sites. Pour autant les juges strasbourgeois rejettent l'engagement de la responsabilité en la matière. Ils estiment que *« dans le cadre des contrats d'affiliation passés avec les propriétaires des sites [incriminés], leur responsabilité n'est pas [...] engagée faute pour les demandeurs de démontrer qu'ils ont fourni à leurs partenaires le contenu contrefaisant ». De même, « faute de démontrer que les défendeurs disposaient de la maîtrise de ces sites ou avaient le pouvoir d'influer sur leur contenu, la responsabilité de ces derniers ne peut pas non plus être engagée sur le fondement de l'article 1382 du Code civil »*. Les affiliés ne sont responsables que du contenu qu'ils fournissent à leurs affiliés et non pas de la manière dont ces contenus sont utilisés.

Cette décision semble s'inscrire à rebours d'un arrêt de la Cour d'appel de Paris du 24 juin 2004 qui concernait également des sites pornographiques. Dans cette précédente affaire, l'affilieur proposait aux internautes d'installer sur leurs sites des kits de connexion permettant de surfer – de manière surtaxée – sur certains contenus. En particulier, il proposait « la vidéo porno de Loana », mettant en scène une personne blonde prénommée ainsi. Or certains affiliés décidèrent de créer des sites internet dédiés à Loana P. (la « Loana du loft ») et d'installer dessus ces kits de connexion. Celle-ci décida de saisir la justice et fit condamner l'affilieur. Les juges d'appel relevèrent que *« l'apport d'un site à caractère pornographique, dont les images de présentation pouvaient créer une confusion dans l'esprit de l'internaute et le conduire à penser qu'il s'agissait de Loana P., dans le cadre d'un contrat avec des partenaires*

*visant à conduire l'internaute à se connecter audit site pornographique, est constitutif, à défaut de consentement de sa part, d'une faute à l'égard de l'appelante*». L'affilieur était donc condamné sur le fondement de l'article 1382 du Code civil alors même – pour reprendre les éléments donnés par les juges strasbourgeois – qu'il n'avait ni la maîtrise dans la présentation des kits de connexion, ni le pouvoir d'influer sur celle-ci.

Cet arrêt de juin 2004 semble être un cas particulier. L'affilieur semblait avoir joué sur le contexte médiatique afin de créer une confusion dans l'esprit du public. C'est sans doute cette recherche de confusion dans l'offre proposée que les juges avaient souhaité sanctionner, celle-ci devenant alors indépendante de la présentation qui en était faite par les affiliés.

## La vente de produits pharmaceutiques et para-pharmaceutiques en ligne

Au cours de l'année 2005, les juges français ont statué, pour la première fois, sur la possibilité de vendre des spécialités para-pharmaceutiques sur l'internet au regard des principes fixés par les droits français et communautaire. En juin 2000, des produits de marque pour lentilles de contact étaient mis en ligne sur l'internet par Juva Santé. Or, l'article L. 4211-1-2° et 4° du Code de santé publique réserve aux seuls pharmaciens la préparation des produits destinés à l'entretien ou l'application des lentilles oculaires de contact, ainsi que la vente en gros, la vente au détail et toute dispensation au public des mêmes produits. Par dérogation de l'article L. 4211-4 du même Code, les opticiens-lunetiers peuvent également procéder à la commercialisation des produits destinés à l'entretien des lentilles oculaires de contact.

Face à ce régime juridique, Juva Santé invoquait – notamment auprès de ses revendeurs – *«la disparition du monopole de distribution des produits d'entretien pour lentilles de contact bénéficiant du marquage CE»* au regard notamment de la directive 93/42/CE puisque la loi française *«imposerait une condition supplémentaire à la réalisation de la fabrication, de la mise sur le marché et de la mise en vente de produits»*. Seulement, la Cour d'appel de Paris, dans un arrêt du 2 mars 2005, a repoussé ces arguments. Les magistrats ont estimé que *«la réglementation du monopole de la vente en France des produits pharmaceutiques par les établissements pharmaceutiques et les pharmaciens, même étendu comme en l'espèce aux opticiens-lunetiers dans ce cas particulier, ne masque aucune restriction interdite entre les États membres de la Communauté économique européenne et n'est contraire à aucune disposition du traité instituant la Communauté européenne [...] les restrictions qui peuvent en résulter relevant de l'exception prévue par l'article 30 de ce traité selon lequel les dispositions des articles 28 et 29 relatifs aux restrictions quantitatives et aux mesures d'effet équivalent ne font pas obstacle aux interdictions ou restrictions justifiées notamment par des raisons de protection de la santé ou de la vie des personnes»*.

En conséquence – et nonobstant les dispositions de la directive du 8 juin 2000 relative au commerce électronique qu'écartent les juges – la société Juva Santé ne pouvait pas fournir en ligne, comme grossiste, des produits d'entretien de lentilles de contact à des magasins ne répondant pas aux critères fixés par le droit français. Cette faute était donc susceptible d'engager sa responsabilité délictuelle; la faute pénale n'étant

pas abordée du fait du caractère purement civil de l'action entreprise par le syndicat professionnel requérant. Cet arrêt est intéressant à plus d'un titre.

Tout d'abord, il s'agit de la première décision française amenée à apprécier – suite à de la vente en ligne – la compatibilité du droit français aux principes du droit communautaire. Mais surtout, elle intervient postérieurement à l'arrêt *Doc Morris* (CJCE, 11 décembre 2003) qui avait estimé que l'article 30 du traité CE ne saurait être invoqué pour justifier une interdiction absolue de vente par correspondance des médicaments qui ne sont pas soumis à prescription médicale dans l'État membre concerné. En pratique, les conclusions de la CJCE étaient inapplicables en l'espèce, le litige étant franco-français; l'interdiction émise par la législation française étant alors opposable aux acteurs situés sur notre territoire. À l'inverse, si les produits incriminés étaient commercialisés depuis un autre territoire de l'Union européenne, les magistrats français n'auraient pas été en mesure de prononcer une sanction à l'encontre de tels revendeurs, les produits pour lentilles de contact étant pour l'heure non soumis à prescription médicale.

## **Droit du travail**

### La vie privée numérique du salarié

Au visa des articles 8 de la CEDH, 9 du Code civil, 9 du NCPC et L. 120-2 du Code du travail, la chambre sociale de la Cour de cassation a affirmé dans un arrêt du 17 mai 2005 que, *«sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé»*. La décision se situe à l'évidence dans le prolongement du fameux arrêt Nikon du 2 octobre 2001 et contribue à dessiner les contours de la notion de *«respect de l'intimité de la vie privée du salarié au temps et au lieu de travail»*.

Rattachant le respect des correspondances à l'intimité de la vie privée, les magistrats de la chambre sociale avaient en 2001 considéré que *«l'employeur ne peut [...] prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur»*. Ce principe, posé dans des termes généraux, avait suscité de nombreuses interrogations sur les limites du respect accordé à l'intimité de la vie privée du salarié au sein de l'entreprise.

La nouvelle décision de la Cour de cassation ne concerne pas les correspondances mais les fichiers qualifiés de «personnels» par le salarié et stockés sur son poste informatique. En l'occurrence, un employeur avait trouvé des photos érotiques dans le bureau de son employé dans des circonstances non précisées. Estimant se trouver dans des circonstances exceptionnelles, il avait procédé à un contrôle du contenu du disque dur du salarié sans en informer celui-ci. À cette occasion, il avait découvert un ensemble de dossiers personnels étrangers aux fonctions du salarié et licencié en conséquence celui-ci pour faute grave.

Dans un arrêt du 6 novembre 2002, la Cour d'appel de Paris estima rapportée la preuve de la faute grave. D'après elle, l'accès aux fichiers était intervenu régulièrement dès lors que l'employeur se trouvait dans «*des circonstances exceptionnelles l'autorisant à contrôler le contenu du disque dur de l'ordinateur*». L'arrêt est aujourd'hui censuré au motif que l'ouverture des fichiers, effectuée en l'absence de l'intéressé, n'était justifiée par aucun risque ou événement particulier.

La Cour ouvre la possibilité à l'employeur d'ouvrir les fichiers stockés sur un support mis à la disposition du salarié et identifiés comme personnels sous certaines conditions. La solution rendue dans la présente affaire s'avère donc plus nuancée que celle, très générale, de l'arrêt Nikon. La question de l'interpénétration de la sphère du travail et de la sphère privée a été abordée par le Forum des droits sur l'internet dans ses Recommandations sur les «*Relations du travail et internet*» du 17 septembre 2002 et sur «*le Télétravail en France*» du 14 décembre 2004. Concernant les fichiers personnels, le Forum a appelé à un contrôle proportionné et limité, avec une gradation des niveaux de contrôle (technique, en volume et, sous réserve de garanties procédurales, sur le contenu).

La décision de la Cour de cassation répond à ce souci et, en continuité avec la jurisprudence Nikon, rééquilibre les rapports entre la protection de la vie privée du salarié et le pouvoir de contrôle de l'employeur. C'est une décision de nature à rassurer les entreprises.

Plusieurs zones d'ombre méritent cependant d'être éclaircies et notamment, l'information du salarié sur ce type de contrôle et la notion de «*risque ou d'événement particulier*».

## La liberté d'expression des syndicats

Avant sa modification par la loi du 4 mai 2004 relative au dialogue social et à la formation professionnelle, l'article L. 412-8 du Code du travail prévoyait que les tracts syndicaux étaient librement diffusés aux salariés au sein de l'entreprise aux heures d'entrée et de sortie du travail et que le contenu de ceux-ci est librement déterminé par l'organisation syndicale. Il apparaissait que les modalités de distribution de ces tracts papiers prévues par la loi ne se prêtaient que de manière artificielle aux fonctionnalités de l'internet.

Appelée à juger cette question, la 14<sup>e</sup> chambre de la Cour d'appel de Paris avait considéré, le 31 mai 2002, que la diffusion d'un tract syndical sur la messagerie professionnelle des salariés qui «*n'est par hypothèse utilisable que pendant les heures de travail et non aux heures d'entrée et de sortie du travail*» n'était pas conforme aux dispositions de l'article L. 412-8. Confirmant ce principe, le Tribunal de grande instance de Paris avait estimé dans une décision du 25 avril 2003 «*qu'en diffusant des informations syndicales par le vecteur de cette messagerie, le syndicat SUD est sorti du cadre de la communication syndicale prévue à l'article L. 412-8 du Code du travail*». C'est ce principe qu'a confirmé la Cour de cassation dans son arrêt du 25 janvier 2005. En effet, cette dernière a estimé que «*La diffusion de tracts et de publications syndicaux sur la messagerie électronique que l'entreprise met à la*

*disposition des salariés n'est possible qu'à la condition, soit d'être autorisée par l'employeur, soit d'être organisée par voie d'accord d'entreprise».*

Néanmoins, depuis ces faits, la réglementation a évolué. La loi n° 2004-391 du 4 mai 2004 relative à la formation professionnelle tout au long de la vie et au dialogue social a modifié l'article L. 412-8 du Code du travail en autorisant, par la voie de l'accord d'entreprise, la mise à disposition d'informations de nature syndicale sur un intranet et l'envoi de tracts par courrier électronique. Le texte précise que *«cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne pas entraver l'accomplissement du travail. L'accord d'entreprise définit les modalités de cette mise à disposition ou de ce mode de diffusion, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à préserver la liberté de choix des salariés d'accepter ou de refuser un message»*. Cette évolution fait notamment suite aux recommandations du Forum des droits sur l'internet faites dans le cadre de son rapport «Internet et relations du travail» rendu public en septembre 2002.

Ces nouvelles dispositions ont d'ores et déjà fait l'objet de quelques précisions. Ainsi, le Tribunal de grande instance de Nanterre, dans une ordonnance de référé du 26 octobre 2004, a pu juger *«qu'en application de l'article L. 412-8 du Code du travail les publications et tracts de nature syndicale ne peuvent être diffusés, ni sur un site syndical mis en place sur intranet de l'entreprise, ni sur la messagerie électronique de l'entreprise, sauf accord d'entreprise»*, reprenant ainsi le principe aujourd'hui fixé par la Cour de cassation.

Parallèlement à cette décision de la Cour de cassation, le Tribunal de grande instance de Bobigny est venu apporter, le 11 janvier 2005, des éléments complémentaires quant à la liberté d'expression des syndicats. Ainsi, si l'article L. 412-8 du Code du travail autorise la distribution de tracts aux travailleurs de l'entreprise, *«la communication du tract par internet à tout moment, partout et à tous, notamment aux personnes étrangères à l'entreprise, est incompatible avec le texte sus visé qui veut en réserver la diffusion aux salariés»*. Sur ce fondement, les juges ont ordonné le retrait des tracts contestés du site internet du syndicat. Cette mesure était, en outre, justifiée par le fait que le tract contenait *«des informations sur l'évolution des salaires, le chiffre d'affaires des panels et la rentabilité des créations publicitaires, que la société avait intérêt à ne pas révéler au public extérieur à l'entreprise»*.

Le tribunal a en profité pour rappeler les principes applicables en matière d'expression des syndicats. Ainsi, si le salarié dispose dans l'entreprise et en dehors de celle-ci de sa liberté d'expression, ce dernier demeure soumis à des obligations qui découlent du contrat de travail qu'il a conclu. En particulier il est tenu pendant la durée de son contrat à une obligation de fidélité qui lui impose une règle de discrétion. Ce principe s'applique également aux syndicats *«qui représentent les salariés au sein d'une entreprise [et] ne peuvent s'affranchir de cette règle de discrétion, laquelle dans le cas contraire serait réduite à néant»*.

## La diffusion d'offres d'emploi en ligne

Publiée au Journal officiel le 19 janvier 2005, la loi de programmation pour la cohésion sociale du 18 janvier 2005 confère une base légale aux sites internet publiant des offres et des demandes d'emploi. Jusqu'à ce texte, les dispositions de l'article L. 311-4 du Code du travail faisait interdiction à toute personne de faire connaître ses offres ou demandes d'emploi par voie d'affiche ou par tout autre moyen de publicité. Cette interdiction générale connaissait des exceptions pour les insertions d'offres et demandes d'emploi dans la presse.

Dorénavant, si les nouvelles dispositions de l'article L. 311-4 du Code du travail précisent que la vente d'offres ou de demandes d'emploi, quel que soit le support utilisé, est interdite, cette interdiction de principe est tempérée par la possibilité de réaliser une insertion, à titre onéreux, d'offres ou de demandes d'emploi dans une publication ou un autre moyen de communication payant.

Par ailleurs, toute offre d'emploi publiée ou diffusée doit être datée. À chaque publication d'offre d'emploi, l'employeur sera tenu de faire connaître son nom ou sa raison sociale et son adresse au responsable du site internet. Les sites ne seront plus tenus de communiquer immédiatement l'ensemble des offres aux services de l'Agence nationale pour l'emploi

## Administration électronique

Poursuivant le travail entrepris depuis plusieurs années, le Gouvernement français a acté au cours de l'année 2005 plusieurs mesures en faveur du développement de l'administration électronique.

---

***Suite à un mandat donné par le ministre de l'Intérieur, le Forum des droits sur l'internet a remis le 16 juin 2005 son rapport synthétisant le débat public organisé sur le projet de carte nationale d'identité électronique (projet INES, Identité nationale électronique sécurisée, avec données biométriques).***

---

## La fixation du nouveau régime d'accès aux documents administratifs et de diffusion des données publiques

Par une loi de simplification du droit en date du 9 décembre 2004, le Gouvernement avait été habilité, par le Parlement, à modifier et à compléter, par ordonnance les dispositions de la loi n° 78-753 du 17 juillet 1978 ainsi que les autres dispositions législatives portant sur l'accès à des documents administratifs ou à des données publiques. L'objectif était notamment d'assurer la transposition de la directive 2003/98/CE du Parlement européen et du Conseil, du 17 novembre 2003, concernant la réutilisation des informations du secteur public. Cette ordonnance a été promulguée le 6 juin 2005.

Tout d'abord, le texte modifie plusieurs dispositions relatives au régime d'accès aux documents administratifs. Il s'agit en réalité de clarifier la rédaction de certains articles



de la loi n° 78-753 du 17 juillet 1978 et de codifier des pratiques existantes. Ainsi, font l'objet d'une consécration textuelle les pratiques déjà existantes de la communication partielle des documents, moyennant l'occultation de mentions non communicables et de la mise à disposition des documents administratifs par voie électronique. Ensuite, la principale innovation résultant de cette ordonnance est la création au sein d'un chapitre consacré à la réutilisation des informations publiques.

Le champ retenu par l'ordonnance inclut la réutilisation des informations détenues ou produites par l'État, les collectivités territoriales, les organismes chargés d'une mission de service public. Ne sont cependant pas dans le champ ainsi défini les informations élaborées ou détenues dans le cadre d'une mission de service public industriel et commercial et ceux sur lesquelles des tiers détiennent des droits de propriété intellectuelle. Les informations des établissements culturels ou d'enseignement suivent quant à elles un régime particulier, laissé à la libre appréciation des établissements en cause. Enfin, les échanges d'informations entre autorités administratives ne sont pas soumis au régime de la réutilisation.

Lorsque la réutilisation des informations publiques est autorisée, la directive pose un certain nombre d'exigences minimales destinées à assurer l'effectivité de la réutilisation et le respect des règles de concurrence. S'agissant des prescriptions destinées à assurer l'effectivité de la réutilisation, l'ordonnance pose le principe de la liberté de réutilisation des informations, à des fins commerciales ou non, et comporte des obligations pour les administrations. À cet égard, elle prévoit, dans les conditions déterminées par le pouvoir réglementaire, la désignation par chaque administration d'une personne responsable de la réutilisation. Elle place le régime de la réutilisation sous le contrôle de la Commission d'accès aux documents administratifs (CADA) et impose que les décisions négatives, telles que les refus de licence de réutilisation, soient motivées et écrites. Les administrations sont au surplus astreintes à la transparence quant au mode de calcul des redevances, quant aux principales informations susceptibles de réutilisation qui figurent dans un répertoire *ad hoc* et quant à d'éventuels détenteurs de droits de propriété intellectuelle.

S'agissant du respect de la libre concurrence, l'ordonnance transpose sans aménagement les contraintes relatives aux droits exclusifs et reprend les exigences posées par la directive en matière tarifaire. La directive interdit, en effet, que le montant de la redevance perçue à l'occasion d'une réutilisation excède la totalité des coûts supportés par l'administration, majorés d'un retour sur investissement raisonnable. Ce plafond s'applique également au montant que représente la totalité des redevances perçues pour la réutilisation d'une même information. Se conformant à cet encadrement, l'ordonnance autorise la perception d'une redevance, pour les réutilisations commerciales ou non, dont le montant peut inclure les coûts supportés par l'administration productrice ou détentrice des informations, et notamment les coûts de mise à disposition et d'éventuelle anonymisation des informations. La délivrance préalable d'une licence est requise lorsque la réutilisation donne lieu à la perception d'une redevance et l'administration tient des licences types à la disposition des intéressés.

Enfin, l'ordonnance comporte des dispositions d'accompagnement qui garantissent l'équilibre général du dispositif. Il est tout d'abord rappelé que la réutilisation des informations comportant des données à caractère personnel se fait dans le respect de

la loi informatique et libertés et, à cet égard, un régime particulier est créé. Ce régime repose sur le consentement de la personne intéressée ou à défaut sur une alternative passant, soit par l'anonymisation des données, soit par un régime résultant d'un texte ad hoc. Par ailleurs, le texte confère à la CADA le pouvoir d'infliger des sanctions administratives, pouvant aller jusqu'à une amende de 300 000 euros, modulées en fonction des finalités de la réutilisation, lorsque la réutilisation a été faite en méconnaissance de l'obligation de licence, des prescriptions de la licence ou lorsqu'elle révèle une altération non autorisée des données publiques. Ce pouvoir de sanction garantit en particulier le respect du principe de séparation des régimes de l'accès aux documents administratifs et de la réutilisation des informations.

L'ordonnance reprend ainsi les principales recommandations édictées par le Forum des droits sur l'internet dans sa recommandation du 14 avril 2003, en particulier sur le rôle nouveau de régulation qu'elle reconnaît à la CADA.

Enfin, complétant ce premier régime, la loi du 26 octobre 2005 a opéré la transposition de la directive 2003/4/CE concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil. L'article L. 124-8 du Code de l'environnement prévoit l'intervention d'un décret précisant les catégories d'informations relatives à l'environnement qui doivent faire l'objet d'une diffusion publique. Ce principe rejoint les recommandations du Forum des droits sur l'internet. Le Forum préconisait que l'État diffuse gratuitement et de manière exhaustive les données publiques citoyennes, celles nécessaires aux citoyens pour l'exercice de leurs droits. Cela intégrait notamment certaines données environnementales comme celles relatives à la qualité de l'air.

## Le renforcement de l'accessibilité des personnes handicapées

Complétant le faible dispositif légal, institué par la loi du 21 juin 2004 pour la confiance dans l'économie numérique, la loi du 12 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées est venue imposer aux autorités publiques des obligations complémentaires.

Les sites des services de l'État, des collectivités territoriales et des établissements publics qui en dépendent doivent, dorénavant, être accessibles aux personnes handicapées. Cette accessibilité concerne l'accès à tout type d'information sous forme numérique quels que soient le moyen d'accès, les contenus et le mode de consultation. Les recommandations internationales pour l'accessibilité de l'internet doivent être appliquées pour les services de communication publique en ligne.

Un décret en Conseil d'État doit encore fixer les règles relatives à l'accessibilité et préciser, par référence aux recommandations établies par l'Agence pour le développement de l'administration électronique, la nature des adaptations à mettre en œuvre ainsi que les délais de mise en conformité des sites existants, qui ne peuvent excéder trois ans, et les sanctions imposées en cas de non-respect de cette mise en accessibilité. Le décret énoncera en outre les modalités de formation des personnels intervenant sur ces sites.

## La création du service public de changement d'adresse

Dans la loi de simplification du droit du 9 décembre 2004, le Parlement avait habilité le Gouvernement à prendre des mesures pour faire en sorte que les Français puissent déclarer, en une seule opération, leur changement d'adresse ou leur changement de situation familiale aux autorités administratives ainsi que, le cas échéant, à tout organisme chargé d'une mission de service public et à des organismes de droit privé. Une ordonnance du 28 avril 2005 a pris en compte ces mesures.

Répondant à une forte demande de la part des usagers, le Gouvernement a ouvert un portail sur l'internet constituant un point d'accès commun permettant aux usagers d'avertir de leur changement d'adresse, en une seule fois, les administrations et organismes participant au service public. Il s'agit des administrations de l'État, des collectivités territoriales, des établissements publics nationaux à caractère administratif, des organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale, du code rural ou du code du travail et des personnes morales chargées du service public de la fourniture de services postaux, de communications électroniques, d'électricité, de gaz ou d'eau.

Par ailleurs, seront admises à participer au service public et sur leur demande, les personnes morales chargées d'une mission de service public, celles qui assurent la fourniture de services postaux, de communications électroniques, d'électricité, de gaz ou d'eau et enfin les personnes morales qui délivrent des prestations rendues obligatoires par des dispositions législatives ou réglementaires. En pratique, le service de changement d'adresse concerne dans un premier temps les caisses d'allocations familiales, l'assurance-chômage, l'assurance-vieillesse, l'assurance-maladie, le service national et les services des impôts. Il sera ensuite élargi progressivement aux autres administrations concernées.

La complexité de la transmission du changement d'adresse aux entités désignées est à la charge de l'administration, dans le respect de la législation relative à la protection des données personnelles.

## Le développement du vote électronique

Le Gouvernement a exprimé, à plusieurs reprises, un avis favorable à une adaptation des modalités de vote aux évolutions technologiques. Plusieurs expérimentations à grande échelle ont été conduites durant l'année 2004, qu'il s'agisse de l'utilisation d'un système de vote par internet pour les élections des membres de cinq chambres de commerce et d'industrie ou de la mise en place de kiosques électroniques pour l'élection des membres des conseils d'université de Nantes et Lyon-II, dans le cadre d'un projet associant les ministères de l'intérieur français et italien. Au total, près de 500 000 électeurs étaient concernés par ces deux expérimentations, organisées sous le contrôle d'experts indépendants et de la CNIL, qui ont été marquées par une augmentation de la participation. La préparation de ces scrutins a été l'occasion, pour les autorités, d'appréhender, en grandeur nature, les difficultés inhérentes au système de vote électronique et de trouver les moyens de les surmonter. À ce titre, le ministre de l'Intérieur, répondant à un parlementaire, indiquait qu'avant «*la généralisation du vote électronique, il convient de s'assurer que cette technique respecte la confidentialité du vote ainsi que son carac-*

*rière personnel et présente des garanties de sécurité aptes à le mettre à l'abri de toute suspicion». En particulier, «les matériels et logiciels utilisés devront respecter le secret du vote et la sincérité du scrutin, conformément aux principes énoncés par la Commission nationale de l'informatique et des libertés dans sa délibération n° 03-036 du 1<sup>er</sup> juillet 2003 relative à la sécurité des systèmes de vote électronique».*

Soutenant, cette volonté politique, plusieurs textes sont venus compléter, en 2005, le dispositif juridique français applicable en matière de vote électronique. Ainsi, un décret du 21 mars 2005 prévoit la possibilité de voter à distance par voie électronique pour les élections au Conseil de l'Ordre des pharmaciens. Une disposition analogue a été introduite dans le projet de loi ratifiant l'ordonnance n° 2005-1040 du 26 août 2005 relative à l'organisation de certaines professions de santé et à la répression de l'usurpation de titres et de l'exercice illégal de ces professions et modifiant le code de la santé publique. L'article 2 souhaite ainsi introduire la possibilité d'élire les conseillers départementaux des ordres des professions médicales par voie électronique.

Par ailleurs, un décret du 18 juillet 2005 prévoit la mise en œuvre du vote électronique pour l'élection des juges des tribunaux de commerce. En particulier, le texte prévoit que les préfets devront adresser aux électeurs une instruction relative aux modalités d'accès au système de vote électronique auquel l'électeur doit se relier pour voter ainsi que les instruments permettant l'expression du vote selon des modalités garantissant sa confidentialité.

Enfin, plusieurs sénateurs ont déposé le 14 novembre 2005 une proposition de loi organique tendant à modifier la loi organique n° 76-97 du 31 janvier 1976 sur le vote des Français établis hors de France pour l'élection du Président de la République. Il s'agirait d'élargir le vote par correspondance aux élections présidentielles et aux référendums.

Enfin, de nouvelles expérimentations sont d'ores et déjà annoncées. L'article 9 de l'ordonnance n° 2004-603 du 24 juin 2004 relative aux mesures de simplification dans le domaine des élections prud'homales a prévu que, lors du prochain renouvellement du mandat des conseillers prud'homaux, qui aura lieu en 2008, le vote électronique sera mis en œuvre à titre expérimental.

Première partie

## **La concertation**

**Les recommandations  
du Forum des droits sur l'internet  
publiées en 2005**

# Les enfants du net (II): pédo-pornographie et pédophilie sur l'internet

*Recommandation publiée le 25 janvier 2005*

## Introduction

L'internet, ce jeune média, est un nouvel espace de sociabilités. Il concerne aujourd'hui plus de 23 millions de Français et est particulièrement populaire auprès des jeunes. Comme d'autres médias, et comme d'autres espaces sociaux, il est susceptible d'être le lieu de la préparation et le théâtre de la représentation d'abus sexuels sur des mineurs.

Des opérations de police de grande ampleur sont régulièrement entreprises à l'encontre de personnes utilisant l'internet pour échanger des images pornographiques mettant en scène des mineurs. La presse se fait également l'écho de cas d'atteintes sexuelles commises sur des mineurs contactés par leurs agresseurs sur le réseau. En Grande-Bretagne, un rapport récent cite pédo-pornographie et pédophilie sur l'internet comme certaines des menaces de nature criminelle les plus préoccupantes sur l'internet<sup>1</sup>.

Face à ce phénomène, certains États et instances internationales se sont déjà mobilisés: l'UNESCO a organisé une première réunion d'experts sur ces thèmes en 1999<sup>2</sup>; et depuis plusieurs années, la lutte contre la diffusion d'images pédo-pornographiques sur l'internet figure à l'agenda des réunions du G8.

Cependant, pédo-pornographie et pédophilie sur l'internet continuent d'inquiéter. Le relatif anonymat – on pourrait parler de pseudonymat – qui a cours sur le réseau, ainsi que la facilité avec laquelle les techniques numériques permettent la reproduction et la diffusion à vaste échelle de tous types de contenus (textes, images, images animées...) alimentent ces craintes. Chacun connaît un enfant, un proche qui aurait été confronté à une situation ou un contenu préoccupant. Les rumeurs les plus diverses circulent et entretiennent auprès de certains un climat de méfiance face au réseau, perçu parfois comme le lieu de tous les dangers et de toutes les transgressions.

**L'internet offre des libertés, des potentialités nouvelles à nos enfants. On ne peut plus revenir en arrière et imaginer un monde sans le réseau. Si celui-ci est porteur de nouveaux risques, parmi lesquels la pédo-pornographie ou la pédophilie comptent parmi les plus graves, nous devons les mesurer et organiser un plan de lutte. C'est l'objet du présent rapport.**

---

1. Sherridan Morris, *The future of netcrime now*, Home Office Online Report 62/04.

2. *Sexual Abuse of Children, Child Pornography and Paedophilia on the Internet: An international challenge – Expert Meeting*, UNESCO, Paris, 18-19 January – [http://www.unesco.org/webworld/child\\_screen/](http://www.unesco.org/webworld/child_screen/).

Ce travail poursuit la réflexion du Forum des droits sur l'internet sur les usages des jeunes utilisateurs de l'internet. Il fait suite à un précédent rapport concernant «l'exposition des mineurs à des contenus préjudiciables<sup>3</sup>», remis en février 2004 aux ministres délégués à la Famille et à la Recherche et aux Nouvelles technologies.

## Champ des recommandations

Pour bien comprendre les risques d'atteintes aux mineurs qui peuvent se réaliser sur l'internet, et que certains communément appellent «pédophilie sur internet», il convient de distinguer deux phénomènes :

La diffusion et le recel de pornographie infantile (ou pédo-pornographie) sur l'internet ;

L'utilisation du réseau internet aux fins de préparer ou de commettre des atteintes sexuelles sur des mineurs (corruption et tentative de corruption de mineurs, atteinte ou agression et tentative d'agression sexuelle, viol et tentative de viol, proxénétisme...).

Ces deux phénomènes sont distincts, mettent en cause des acteurs différents et appellent probablement des solutions de lutte spécifiques. Ils sont étudiés dans deux parties séparées.

L'analyse se concentre sur les contenus et les usages accessibles depuis les terminaux informatiques (micro-ordinateurs), qui constituent aujourd'hui de loin les points d'accès au réseau les plus communément employés. Cependant, l'accès et les usages de l'internet depuis les nouveaux terminaux, principalement les téléphones mobiles, dont les dernières générations proposent toutes sortes d'applications interactives, soulèvent des questions voisines ; celles-ci sont esquissées au sein de ce rapport et devront faire l'objet d'un travail ultérieur.

Enfin, il est clair que le rapport ne s'est pas cantonné à étudier ces phénomènes sur le web, mais prend en compte l'ensemble des protocoles de l'internet, les risques affectant les espaces interactifs (chats, forums...) ou les usages les plus nouveaux de l'internet (P2P..) étant les plus mal connus.

## Méthodologie

Les présentes analyses et recommandations résultent de la concertation, au sein du groupe de travail «Protection de l'enfance» du Forum des droits sur l'internet, de représentants des parties concernées par ce débat : représentants de l'administration (ministère de la Justice, Direction du développement des médias, Défenseur des enfants), des utilisateurs de l'internet et associations de protection des droits des enfants (Internet Society, Union nationale des associations familiales, Voix de l'Enfant) et des acteurs économiques (Association des fournisseurs d'accès et de services internet, MSN France, Orange France)<sup>4</sup>.

---

3. Le Forum des droits sur l'internet, *Les Enfants du Net (I) : Les mineurs et les contenus préjudiciables sur l'internet*, La Documentation française, 2005.

4. La liste complète des membres du groupe de travail figure en annexe du présent rapport.

Le groupe de travail a procédé à l'audition de nombreux experts et acteurs concernés, au premier rang desquels des membres et responsables des forces de police et de gendarmerie<sup>5</sup>.

Ce rapport a fait l'objet d'une consultation des membres du Forum des droits sur l'internet du 21 décembre 2004 au 11 janvier 2005. Il a été définitivement adopté par le Conseil d'orientation du Forum le 21 janvier 2005, et rendu public le 25 janvier 2005.

## **La diffusion et le recel de pédo-pornographie sur l'internet**

En France, l'article 227-23 du Code pénal punit «*le fait [et sa tentative], en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique*», ainsi que la diffusion, la détention, l'importation ou l'exportation de telles images ou représentations, quel qu'en soit le support de diffusion<sup>6</sup>.

La notion de pédo-pornographie peut poser certaines difficultés d'appréciation. En 2002, la Cour d'appel de Paris décrivait comme «*pornographiques*» les contenus d'un site internet figurant «*des organes génitaux féminins offerts, des organes génitaux masculins en érection et des actes de pénétration génitale, buccale, anale*»<sup>7</sup>. En 1999, la Chambre criminelle de la Cour de cassation avait considéré que le caractère pornographique de documents «*mettant en scène des enfants ou adolescents, nus, jambes écartées, exhibant les organes sexuels, parfois en érection*»<sup>8</sup> n'était pas contestable.

La décision-cadre du Conseil de l'Union européenne du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie définit la pédo-pornographie comme la représentation visuelle «*d'un enfant réel*», «*une personne réelle qui paraît être un enfant*», ou «*des images réalistes d'un enfant qui n'existe pas*» «*participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne*»<sup>9</sup>.

Pour l'Office international de police criminelle (Interpol), qui doit fédérer les définitions de la pédo-pornographie en vigueur auprès de ses différents membres, la pédo-pornographie peut être définie comme «*la description visuelle de l'exploitation sexuelle d'un enfant centrée sur le comportement sexuel de l'enfant ou sur ses parties génitales*»<sup>10</sup>.

---

5. La liste complète des personnes entendues au cours de ces travaux figure en annexe du présent rapport.

6. Art. 227-23 du Code pénal.

7. CA Paris, 2 avril 2002, E.L. c/ Ministère Public.

8. Cass. crim., 9 juin 1999, n° 98-80052.

9. Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie. *JOUE* n° L 13 du 20/01/2004. pp. 44-48. À noter qu'une décision-cadre lie les États membres quant au résultat à atteindre et laisse les instances nationales décider de la forme et des moyens pour ce faire, et ne s'inscrit pas dans le droit positif des États.

10. *Recommendations on Offences Against Minors*, Interpol, 61<sup>e</sup> Assemblée générale (1995).



Par ailleurs, certains contenus non strictement pornographiques, mais ouvertement érotiques ou faisant l'apologie de la pédophilie, qui n'entrent pas dans la qualification pénale française, devront être évoqués.

## Évaluation générale du phénomène

### **Un phénomène d'importance observé sur la plupart des protocoles de l'internet**

Le premier constat qui s'impose en matière de diffusion et de recel de pédo-pornographie sur l'internet est que le volume, la typologie et la géographie des contenus sont mal connus. Des sources diverses, de fiabilité inégale, ne permettent pas de quantifier avec précision les faits et leur évolution dans une perspective française, mais indiquent des ordres de grandeur et des tendances : statistiques judiciaires, renseignements issus des signalements d'internautes auprès de services d'initiative publique ou privée, nationaux ou internationaux, statistiques établies à la suite de la recherche proactive de contenus, en France ou à l'étranger.

#### **La perception diffuse d'un phénomène de réelle importance**

Régulièrement, des opérations de police d'une ampleur inédite sont engagées à l'encontre de diffuseurs et de receleurs d'images pédo-pornographiques sur l'internet, parfois à une échelle mondiale. En France, la première grande opération, intitulée « Forum 51 », a été lancée par la gendarmerie nationale en juin 2001. Elle faisait suite à plus d'un an d'enquête sur certains canaux IRC (*Internet Relay Chat*), et a donné lieu à 75 interpellations en France. Lancée à l'initiative du *Federal Bureau of Investigation (FBI)* américain en 1998 dans 14 pays<sup>11</sup>, l'opération « Cathédrale » aurait permis la découverte de 750 000 images pédo-pornographiques, l'identification de 1 263 victimes et l'appréhension de 108 suspects. En 2001, l'opération « Candyman » a mis au jour, à l'initiative du FBI américain, 3 groupes de discussion et d'échanges de fichiers basés sur le *web* et comptant 6 700 membres. Cette enquête a donné lieu à plus d'une centaine d'arrestations. Engagée dès 1999, et étendue à un niveau international en 2001, l'opération « Avalanche » a permis de faire cesser les opérations de la société *Landslide Productions*, basée à Fort Worth au Texas, qui diffusait sur plusieurs sites payants des images pédo-pornographiques importées, notamment, de Russie et d'Indonésie, et de saisir les coordonnées de 250 000 clients de cette société, localisés dans 37 États américains et 60 pays différents. Suite de l'opération « Avalanche » en Grande-Bretagne, l'opération « Ore » a conduit à l'interpellation, en janvier 2003, de 1 600 suspects sur le seul territoire britannique.

M. Yvon Tallec, chef du parquet des mineurs auprès du Tribunal de Grande Instance de Paris, constate « *une explosion* » récente et dans des proportions jusqu'alors inconnues du nombre de signalements de cas de détention, de recel et de diffusion de contenus pédo-pornographiques sur les supports informatiques. Le parquet parisien

---

11. États-Unis, Australie et pays d'Europe.

est parfois saisi plusieurs fois par jour de tels signalements<sup>12</sup>. À elle seule, la Division nationale de la répression des atteintes aux biens et personnes (DNRAPB) de la Direction générale de la police judiciaire (DGPN), qui centralise la réception des signalements de diffusion ou de téléchargement de fichiers pédo-pornographiques sur l'internet en provenance de l'étranger, a reçu près de 3 000 de ces signalements au cours de l'année 2003. Elle mène de 40 à 50 interpellations par an sur la base de ces signalements, et défère autant de dossiers auprès du parquet de Nanterre<sup>13</sup>. Le groupe « technologies de l'information » de la Brigade de protection des mineurs (BPM) de la Direction régionale de la police judiciaire (DRPJ) de Paris a traité en 2003 96 affaires, majoritairement liées à des cas de diffusion et de recel de pornographie enfantine sur l'internet. Ce même groupe, dont les effectifs ont été renforcés, prévoyait de traiter près de 300 affaires l'année suivante, en 2004. Le chef d'escadron Éric Freyssinet, chef du département Informatique-Électronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN), prévoit également la hausse du nombre d'affaires, suite aux dernières affaires de masse instruites en France, et grâce à une coopération internationale de plus en plus active<sup>14</sup>.

La base centrale d'images pédo-pornographiques mise en place au sein de l'OIPC-Interpol recense 200 000 images saisies sur l'internet. Ce chiffre fournit un reflet atténué du nombre d'images en circulation permanente sur l'internet. Les enquêteurs auditionnés en préparation de ces travaux estiment que ce chiffre est en constante progression. Au 7 septembre 2004, le Centre national d'analyse des images pédo-pornographiques (CNAIP) français avait recensé 471 501 photographies de nature pédo-pornographique<sup>15</sup>.

En « bout de chaîne », les statistiques issues du casier judiciaire ne décrivent que le nombre de condamnations prononcées pour une infraction particulière. Elles indiquent que 4 personnes ont été condamnées pour « détention de l'image d'un mineur présentant un caractère pornographique » en 2002, année de la création de l'infraction. Entre 2000 et 2002, 64, puis 22, puis 88 personnes ont été condamnées pour « recel de bien provenant de la diffusion d'image d'un mineur à caractère pornographique », sans que l'on puisse distinguer dans quelle mesure ces deux infractions sont liées à l'utilisation de l'internet. 3, 16 puis 10 personnes ont été condamnées sur le fondement de la « diffusion de l'image d'un mineur présentant un caractère pornographique en utilisant un réseau de télécommunications » (art. 227-23, al. 3 du Code pénal). Il est à noter que, considérant le délai moyen d'instruction des délits, ces chiffres fournissent très vraisemblablement un reflet des poursuites engagées dans les années 1998 à 2000.

---

12. Yvon Tallec, audition du 8 juin 2004.

13. Marcel Faure, audition du 27 avril 2004.

14. Éric Freyssinet, entretiens des 14 et 18 octobre 2004.

15. Jacky Durand, « Villepin pour une lutte Net et sans bavure », *Libération*, Paris, 8 septembre 2004. Ce chiffre comprend les photographies et les images résultant du « découpage » de films pédo-pornographiques.

### **Les indications issues des signalements et de la recherche de contenus pédo-pornographiques**

Le témoignage de M<sup>me</sup> Catherine Chambon, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) placé auprès du ministère de l'Intérieur, tend à confirmer le grand nombre de sources de pédo-pornographie sur l'internet et la relative faiblesse du nombre de cas connus de diffusion de tels contenus depuis la France ou par un ressortissant français. Au 15 avril 2004, après 29 mois d'existence, le point de signalement interministériel de contenus pédo-pornographiques, que gère l'OCLCTIC<sup>16</sup>, avait enregistré 14 000 signalements. Une moyenne stable de 10 à 12 % des contenus signalés avait paru de nature pédo-pornographique aux enquêteurs, après examen des contenus signalés. L'Office a transmis 800 signalements auprès d'autorités étrangères et réalisé 7 signalements à des parquets français la première année (2001). Aucun contenu hébergé en France n'a depuis été signalé à un parquet par l'Office<sup>17</sup>.

L'association de droit néerlandais *InHope* fédère les vingt points de signalement opérés, dans quatorze pays d'Europe, aux États-Unis, en Corée du Sud, en Australie et à Taiwan, par des acteurs associatifs et industriels. L'ensemble des points de signalement membres du réseau *InHope* ont recueilli entre mars 2003 et février 2004 96 217 signalements de contenus considérés par les déclarants comme pédo-pornographiques. Le Point de contact de l'Association française des fournisseurs d'accès et de services internet (AFA)<sup>18</sup>, membre fondateur d'*InHope*, est le correspondant du réseau en France. Le site [Pointdecontact.net](http://Pointdecontact.net) a reçu 1 777 signalements de contenus considérés comme pédo-pornographiques par les déclarants entre septembre 2002 et août 2003 inclu, et 1 390 signalements de ce type de septembre 2003 à août 2004 inclu. Entre mars et août 2004, 66,45 % de l'ensemble des signalements de contenus tenus pour illicites par les « signalants » ont été considérés et traités comme tels par l'équipe en charge de la gestion du point de contact<sup>19</sup>. En Grande-Bretagne, la *hotline* de l'*Internet Watch Foundation*, membre elle aussi du réseau *InHope*, a reçu en 2003 plus de 15 000 signalements de contenus pédo-pornographiques<sup>20</sup>.

Aux États-Unis, la *CyberTipline* du *National Center for Missing and Exploited Children* (NCMEC) a vu le nombre des signalements de contenus pédo-pornographiques qui lui sont adressés évoluer de 1 393 en 1998 à 26 759 en 2002<sup>21</sup>. Il convient toutefois de noter que, lus en tendance, les chiffres rapportés par les points de contact renvoient une image de l'évolution de la diffusion de contenus pédo-pornographiques sur l'internet largement déformée par l'évolution de la visibilité de ces points de contact et du « réflexe » consistant à leur signaler les contenus illicites.

Depuis 1996, les membres de l'association Le Bouclier identifient les documents pédo-pornographiques et leurs diffuseurs sur l'internet, tout particulièrement sur

---

16. Voir : <http://www.internet-mineurs.gouv.fr/>

17. Catherine Chambon, audition du 27 avril 2004.

18. Voir : <http://www.pointdecontact.net/>

19. Sources : Association des Fournisseurs d'Accès et de Services Internet (AFA).

20. Internet Watch Foundation, *Annual Report 2003*, London, 2003.

21. Voir Figure 1.

le *web*. Une étude portant sur les années 1996 à 2002 synthétise le produit des recherches de l'association. D'après ce document, Le Bouclier aurait dénombré 261 653 « sites pédophiles » en 2002, contre 4 300 seulement en 1996. Les sites commerciaux devanceraient les sites de particuliers et « militants ». Certaines imprécisions de nature méthodologique concernant, notamment, la nature exacte de ces sites (pédo-pornographie, images tendancieuses représentant des enfants dénudés, apologues de la pédophilie) doivent toutefois faire considérer ces chiffres alarmants avec circonspection<sup>22</sup>.

*Arcobaleno Telefono*, une autre association basée en Italie, procède également à la recherche active de contenus pédo-pornographiques sur le *web*. Elle déclare avoir identifié et signalé aux autorités 17 016 sites à caractère « pédophile et pédo-pornographique » en 2003, un chiffre en très forte augmentation comparé à celui de 2002. Ces chiffres, qui ne sont certifiés par aucune autorité et dont la pertinence ne peut être garantie, sont encore cités à titre indicatif.

### **Applications et protocoles exploités au profit de la diffusion de pédo-pornographie**

La plupart des signalements adressés aux points de contact portent sur des contenus rencontrés sur le *web*. Les contenus pédo-pornographiques accessibles depuis cette « vitrine » de l'internet ne représentent toutefois que la partie la plus visible d'un ensemble plus vaste d'images échangées.

Entre 1998 et 2003, le point de signalement américain du NCMEC<sup>23</sup> a reçu 76 000 signalements, dont 77 % concernaient le *web*, et 1 % seulement les réseaux *P2P*. Ce dernier chiffre paraît toutefois en rapide évolution au fur et à mesure que les usages des réseaux *P2P* gagnent en popularité : en 2001, 156 des signalements de contenus pédo-pornographiques adressés au NCMEC concernaient les réseaux *P2P*. En 2002, 757 de ces signalements s'y rapportaient. Les statistiques du NCMEC indiquent également une augmentation régulière des signalements se rapportant au *web* (de 18 052 à 26 759 entre 2001 et 2002) et, surtout, au courrier électronique (de 1 128 à 6 245 entre 2001 et 2002), sous la pression, sans doute, de l'augmentation du nombre de messages publicitaires pornographiques non sollicités diffusés via le réseau. On remarque enfin d'après ces indicateurs que le nombre de signalements se rapportant aux autres protocoles (*newsgroups* – groupes de discussion, *chat rooms* – salons de discussion, messagerie instantanée, FTP – transferts de fichiers) évolue dans de moindres proportions<sup>24</sup>.

---

22. Le Bouclier, « Pédocriminels impunis ». Extrait partiel des résultats de l'étude des sites Internet pédophiles menée par l'association Le Bouclier de 1996 à 2002 portant sur 261 653 sites », 2003.

23. Voir : <http://www.cybertipline.com/>

24. Cité par United States General Accounting Office, *File-Sharing Programs. Peer-to-Peer Networks Provide Ready Access to Child Pornography*, *Ibid*, p. 8.

Figure 1

**Signalements transmis par le NCMEC aux organismes gouvernementaux chargés de réprimer la diffusion de pornographie enfantine (FBI, Division criminelle du Département de la Justice, Douanes)**

Technology	Number of tips				
	1998	1999	2000	2001	2002
Web sites	1 393	3 830	10 629	18 052	26 759
E-Mail	117	165	120	1 128	6 245
Peer-to-peer	-	-	-	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknow	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
<b>Total</b>	<b>2 338</b>	<b>5 569</b>	<b>12 024</b>	<b>21 025</b>	<b>35 676</b>

Source: Exploited Child Unit, National Center for Missing and Exploited Children

En 2003, les signalements adressés à l'*Internet Watch Foundation*, concernaient en très grande majorité des contenus accessibles sur le web, et plus rarement sur les groupes de discussion (*Usenet*) et certains services communautaires<sup>25</sup>.

Une étude de février 2003 du *General Accounting Office* (GAO) américain établit que les réseaux *peer-to-peer* (P2P) constituent un canal de plus en plus souvent utilisé pour l'échange d'images pédo-pornographiques<sup>26</sup>: sur 341 images téléchargées et examinées par les douanes américaines à la suite de requêtes portant sur trois mots clés fréquemment associés aux contenus pédo-pornographiques, 149 images (soit 44 % environ) se sont avéré être de nature pédo-pornographique. Ces éléments permettent au GAO de conclure que les applications d'échange de fichiers de pair à pair permettent un accès aisé à ces contenus.

Le nombre de sites *web* pédo-pornographiques hébergés en France est faible. Aussi les enquêtes de l'IRCGN, par exemple, s'orientent plus souvent, selon le chef de son département informatique<sup>27</sup>, vers les réseaux P2P et sur les différents espaces publics de l'internet: forums sur *Usenet* (*newsgroups*), *Internet Relay Chat* (*IRC*), *chats* sur le *web*, forums sur le *web*, *chats* proposés par certains fournisseurs de services internet...

25. Internet Watch Foundation, *op. cit.*

26. United States General Accounting OFFICE, *File-Sharing Programs. Peer-to-Peer Networks Provide Ready Access to Child Pornography, Report to the Chairman and Ranking Minority Member*. GAO-03-351, Committee on Government Reform, House of Representatives, Washington, DC, February 2003.

27. Eric Freyssinet, entretiens des 14 et 18 octobre 2004.

Selon M. Philippe Jarlov, gendarme spécialisé de la section des recherches de Bordeaux, le réseau *UnderNet*, l'un des réseaux IRC les plus étendus, compterait ainsi de 15 à 20 salons de discussion consacrés aux échanges d'images pédo-pornographiques ou de propos «pédophiles». Ce gendarme déclare identifier chaque année, sur le protocole IRC, 10 à 20 diffuseurs de fichiers pédo-pornographiques localisés en France, et chaque semaine de 10 à 15 utilisateurs de réseaux P2P localisés en France et offrant des images pédo-pornographiques au téléchargement<sup>28</sup>. Il convient de noter qu'une part non négligeable de ces diffuseurs ont pu se faire les relais involontaires de ces contenus: en téléchargeant en masse des groupes de fichiers sur les réseaux IRC ou P2P, certains utilisateurs sont susceptibles d'enregistrer et de redistribuer aussitôt certains contenus illicites, sans même avoir pris connaissance de la nature de ces contenus.

On peut conclure de cet ensemble de sources et de commentaires que la pédo-pornographie est bien présente sur l'internet, le nombre de sources et de personnes impliquées se chiffrant en dizaine de milliers dans le monde. Certaines applications (IRC, P2P) semblent avoir la préférence des diffuseurs et receleurs de matériels pédo-pornographiques, mais tous les protocoles de l'internet et ses espaces publics sont mis à profit par ces derniers, sans toutefois que ces contenus y soient systématiquement visibles. Si les éléments manquent pour affirmer avec certitude que l'internet est le vecteur d'un commerce accru de pédo-pornographie, il est peu contestable que ces contenus y sont plus accessibles que par les médias traditionnels. Ces observations, toutefois, ne permettent pas de saisir quelle économie sous-tend l'échange de ces contenus illicites, ni d'ailleurs la part des contenus accessibles gratuitement face à celle des services payants. Il est en revanche certain que, comme dans la plupart des modèles connus de circulation de biens immatériels, l'échange gratuit de fichiers entre «collectionneurs» coexiste avec des services rémunérés. La fréquence du recours à la cryptologie aux fins de dissimuler les fichiers pédo-pornographiques échangés, enfin, reste impossible à estimer, même si plusieurs enquêtes ont confirmé l'usage de cet ensemble de techniques au sein de certains réseaux d'échange d'images pédo-pornographiques.

## **Les serveurs d'images pédo-pornographiques sur le web concentrés géographiquement**

Les statistiques officielles décrivent mal la progression de la diffusion et du recel d'images pédo-pornographiques sur l'internet, et ne donnent qu'un aperçu flou de l'origine de ces contenus. Il convient à nouveau, pour s'en faire une idée, de croiser des informations issues de plusieurs sources.

Les signalements de contenus pédo-pornographiques transmis aux *hotlines* désignent le plus souvent des images accessibles sur le web. Ces dernières représentent la «partie émergée» et souvent marchande de l'échange et du recel de pédo-pornographie sur l'internet.

---

28. Philippe Jarlov, audition du 14 septembre 2004.

D'après M<sup>me</sup> Chambon, chef de l'OCLCTIC, ces contenus sont schématiquement localisés pour un tiers aux États-Unis, pour un tiers en Fédération de Russie, et pour un dernier tiers dans une variété d'autres pays<sup>29</sup>.

Le rapport annuel de l'*Internet Watch Foundation* confirme ce constat : 55 % des contenus pédo-pornographiques qui ont été signalés à la *hotline* britannique étaient hébergés aux États-Unis, 23 % en Russie, 6 % en Europe, 4 % au Brésil et 4 % en Corée du Sud.

Enfin, l'association italienne *Telefono Arcobaleno* situe les 17 016 sites « pédophiles et pédo-pornographiques » qu'elle a signalés aux autorités dans 33 pays, et en premier lieu aux États-Unis (61,72 %), en Corée du Sud (7,95 %), en Russie (7,24 %) et au Brésil (7,24 %). 43 serveurs (soit 0,25 % de son activité) localisés en France ont été signalés par l'association.

Les sites pédo-pornographiques sont souvent décrits comme extrêmement « mobiles » et susceptibles, lorsqu'ils sont identifiés par les services de police et de gendarmerie, de changer très rapidement de serveur d'hébergement et d'adresse.

Ces éléments d'appréciation, qui concernent pour l'essentiel les contenus pédo-pornographiques accessibles sur le web, ne donnent à nouveau qu'une image imprécise de la localisation de l'ensemble des serveurs de fichiers pédo-pornographiques. En particulier, ils ne rendent pas compte de l'échange de matériels pédo-pornographiques entre individus via d'autres applications de l'internet, qui constitue sans doute une part importante des infractions commises en France.

## **Faut-il craindre que l'internet banalise la pédo-pornographie ?**

Un rapport consacré en 2003 par la Direction générale des droits de l'homme du Conseil de l'Europe sur « l'impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains aux fins d'exploitation sexuelle » rapporte qu'aux États-Unis, le nombre d'affaires liées à l'utilisation de l'internet traitées par l'*US Postal Service* aurait régulièrement crû, passant de 32 % en 1998 à 47 % en 1999 et 77 % en 2000. Toutefois, l'*US Postal Inspection Service* « a [également] pu constater que l'utilisation accrue de l'Internet par les pédocriminels s'est traduite parallèlement par une progression de leur recours aux services postaux<sup>30</sup>. » Ce constat suggère que, après avoir connu un pic dans les années 1970, puis reculé sous la pression de la généralisation de la régulation de ces contenus en Europe et aux États-Unis entre les années 1970 et 1990<sup>31</sup>, la distribution de pédo-pornographie pourrait connaître un regain à l'âge des médias électroniques.

---

29. Catherine Chambon, audition du 27 avril 2004.

30. *L'impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains aux fins d'exploitation sexuelle. Rapport final du groupe de spécialistes EG-S-NT.* Conseil de l'Europe, Direction générale des droits de l'homme, Division égalité entre les femmes et les hommes. Strasbourg, septembre 2003, pp. 14-15.

31. Margaret A Healy, *Child pornography: an international perspective*, Computer Crime Research Center, août 1996.

Les interprétations des chiffres de la diffusion de pornographie enfantine sur l'internet divergent toutefois. À l'idée que l'internet rend possible la massification et la banalisation de l'échange d'images pédo-pornographiques à l'échelle planétaire, répond la thèse selon laquelle la diffusion d'images pédo-pornographiques sur l'internet ne fait que rendre plus visible un phénomène largement préexistant au réseau et à ses applications.

La réalité participe sans doute des deux lectures du phénomène, et il convient de porter ici quelques observations :

- la perception de la diffusion de pédo-pornographie sur l'internet et le nombre d'affaires judiciaires liées à ce phénomène vont croissants ;
- la diffusion d'images pédo-pornographiques sur l'internet reste toutefois sans commune mesure avec celle de pornographie adulte, qui s'est constituée en l'un des secteurs d'activité les plus florissants du réseau<sup>32</sup> ;
- certaines images pédo-pornographiques ne circulant plus seulement sous plis scellés, mais étant librement accessibles sur le réseau sous une apparence d'anonymat renforcée, il paraît probable que certaines personnes qui n'auraient pas fait la démarche de rechercher puis d'acquérir des contenus pédo-pornographiques auprès de revendeurs « traditionnels » ont pu y accéder, souvent gratuitement, sur l'internet<sup>33</sup> ;
- la terminologie propre à la pédo-pornographie paraît avoir largement « contaminé » sur l'internet la pornographie adulte : les sites diffusant de la pornographie adulte prétendant diffuser des images de « *preteens* » (« pré-adolescentes ») sont aujourd'hui innombrables, banalisant les codes de la pédo-pornographie, sinon ses représentations.

On ne peut guère établir, au vu des éléments recueillis, que la diffusion d'images pédo-pornographiques sur l'internet concourt à la « banalisation » de tels contenus. Seule la veille systématique de l'exploitation de l'internet aux fins de diffusion de pédo-pornographie pourrait indiquer si l'internet a créé, en facilitant l'accès à ces contenus, les conditions d'un renouvellement du marché de la pédo-pornographie.

État des moyens en vue de combattre la diffusion  
et le recel de pornographie enfantine sur l'internet,  
et des limites de ces moyens

### **Analyse des dispositifs pénaux réprimant le recel et la diffusion de pornographie enfantine**

En engageant les États signataires à prendre les dispositions appropriées pour empêcher que « *des enfants ne soient exploités aux fins de la production de spectacles ou de matériel de caractère pornographique* », la Convention internationale relative aux Droits de l'enfant du 20 novembre 1989 (art. 34) identifie la pédo-pornographie comme une violation des droits des enfants. Les dispositions en condamnant la production, la diffusion et la détention restent pourtant diversement intégrées dans les droits internes.

---

32. Voir Le Forum des droits sur l'internet, *op. cit.*

33. Voir Roger Darlington, « Sex on the Net », 2 août 2004.



## En France, un dispositif pénal complet

L'article 227-23 du Code pénal punit de 45 000 euros d'amende et de trois ans de prison le fait de fixer, d'enregistrer, de transmettre, de diffuser, d'importer ou d'exporter l'image ou la représentation à caractère pornographique d'un mineur de moins de 18 ans ou d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de 18 ans au jour de la fixation ou de l'enregistrement de son image. Depuis la loi pour la confiance dans l'économie numérique du 21 juin 2004 est punie de la même peine la tentative de fixation, d'enregistrement ou de transmission d'une telle image ou représentation en vue de sa diffusion. Les peines sont portées à cinq ans d'emprisonnement et à 75 000 euros d'amende lorsqu'un réseau de télécommunications (ou communications électroniques) a été utilisé pour diffuser l'image ou la représentation du mineur à destination d'un public non déterminé. Depuis la loi du 4 mars 2002 relative à l'autorité parentale, enfin, le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30 000 euros d'amende.

Une spécificité de l'article 227-23 doit être soulignée: il protège les mineurs victimes, mais également, depuis la loi du 17 juin 1998, l'image des mineurs, en punissant la représentation pornographique d'un mineur, même virtuelle (montage, dessin...) <sup>34</sup>, ce qui fait du Code pénal français un dispositif particulièrement protecteur.

Le recel d'images pédo-pornographiques, soit «*le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit*» et «*le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit*», est puni de cinq ans de prison et de 375 000 euros d'amende (art. 321-1 et suivants du Code pénal) <sup>35</sup>. Cette incrimination a souvent servi, avant l'adoption de la loi du 4 mars 2002, à punir la simple détention d'images pédo-pornographiques.

De l'avis de M. Yvon Tallec, chef du parquet des mineurs du TGI de Paris, l'article 227-23 pose, en pratique, des difficultés d'appréciation du caractère pornographique des images. En effet, de nombreuses images en circulation sur le réseau sont d'une nature ambiguë. Elles présentent par exemple parfois les protagonistes majeurs de scènes pornographiques comme mineurs, ou représentent des personnes mineures dans des scènes de nu aux limites de la pornographie. Des enquêteurs notent que l'appréciation de la nature «pornographique» d'une représentation ou de la minorité d'âge présumée d'une personne varie selon les juridictions. La minorité des personnes représentées ne peut toutefois être mise en doute dans la plupart des affaires dont se saisissent les services d'enquête <sup>36</sup>.

---

34. Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des enfants, art. 17.

35. Un exemple de décision rendu sur le fondement du recel d'images pédo-pornographiques: Tribunal de grande instance du Mans, jugement correctionnel, 16 février 1998, Monsieur le Procureur de la République c/ Ph. H.

36. Yvon Tallec, audition du 8 juin 2004.

Des enquêteurs de la brigade parisienne de protection des mineurs (BPM) notent qu'en moyenne, la détention d'images est punie dans leur juridiction de peines de 2 à 3 mois de prison avec sursis, et la diffusion de ces contenus d'une peine de 6 à 8 mois de prison avec sursis, souvent assortie d'un contrôle socio-judiciaire<sup>37</sup>. Ces indications sont à rapprocher des statistiques du casier judiciaire, qui indiquent que l'infraction de recel de biens provenant de la diffusion de l'image d'un mineur à caractère pornographique a été punie en moyenne, entre 2000 et 2002, de peines d'emprisonnement avec sursis dans près de condamnations prononcées sur 10 et, plus rarement, de 5,5 à 14 mois d'emprisonnement ferme. Les informations disponibles ne permettent toutefois pas de savoir combien de ces condamnations sont liées à l'utilisation de l'internet, ni si les contrevenants ont retiré un profit du recel de ces images.

Figure 2

**Recel de bien provenant de la diffusion d'image d'un mineur à caractère pornographique**

Année	2000	2001	2002	Moyenne
<b>Condamnations</b> (portant sur cette infraction à titre principal)	64	22	88	58,00
<b>Emprisonnement</b>	64	20	83	55,67
soit en pourcentage des condamnations prononcées	100 %	90,91 %	94,32 %	95,08 %
<b>... dont emprisonnement ferme</b>	2	2	23	9,00
soit en pourcentage des condamnations prononcées	3,13 %	9,09 %	26,14 %	12,78 %
<b>Quantum ferme de l'emprisonnement ferme (mois)</b>	7,5	5,5	14,8	9,27
<b>Amendes</b>	0	1	4	1,67
soit en pourcentage des condamnations prononcées	0,00 %	4,55 %	4,55 %	3,03 %
<b>Montant moyen de l'amende ferme</b>	0,00 €	1 219,60 €	1 000,00 €	1 109,80 €

Source: Casier judiciaire.

Le nombre de condamnations pour détention de l'image d'un mineur présentant un caractère pornographique est encore faible en 2002, année de création de l'infraction, en comparaison du nombre de condamnations pour recel, mais enregistre une nette augmentation en 2003. L'évolution de cette tendance reste à confirmer.

37. Marie Lajus, Fabrice Gauthier, audition du 11 mai 2004.

Figure 3

**Détention de l'image d'un mineur présentant un caractère pornographique.**

Année	2002	2003
<b>Condamnations</b> (ensemble des condamnations portant cette infraction, à titre principal ou secondaire)	6	39
<b>Emprisonnement</b> (condamnations portant cette infraction à titre principal exclusivement)	2	9
<b>... dont emprisonnement ferme</b>	1	1
<b>Quantum ferme de l'emprisonnement ferme (mois)</b>	2	2
<b>Amendes</b>	3	3
<b>Montant moyen de l'amende ferme</b>	1 000,00€	1 167€

Source: Casier judiciaire.

Les condamnations prononcées à l'encontre des auteurs de faits de diffusion d'images pédo-pornographiques « en utilisant un réseau de télécommunication » sont également majoritairement punies de peines d'emprisonnement avec sursis et, plus rarement, de 3 à 8 mois d'emprisonnement ferme.

Figure 4

**Diffusion de l'image d'un mineur présentant un caractère pornographique en utilisant un réseau de télécommunications**

Année	2000	2001	2002	2003	Moyenne
<b>Condamnations</b> (ensemble des condamnations portant cette infraction, à titre principal ou secondaire)	7	21	24	52	26
<b>Emprisonnement</b> (condamnations portant cette infraction à titre principal exclusivement)	0	10	7	19	12
<b>... dont emprisonnement ferme</b>	-	1	1	7	2,25
<b>Quantum ferme de l'emprisonnement ferme (mois)</b>	-	4	8	6,4	4,6
<b>Amendes</b>	-	1	1	-	0,5
<b>Montant moyen de l'amende ferme</b>	-	3000 F	750€		603€

Source: Casier judiciaire.

Le nombre de condamnations prononcées, relativement faible, doit être considéré en tenant compte du fait que les procédures entreprises en masse à la suite de récentes enquêtes d'envergure nationale et internationale sont aujourd'hui encore en cours d'instruction: la durée moyenne de l'instruction des délits s'élevait en 2002 à 17,7 mois<sup>38</sup>.

38. Ministère de la Justice, « Les chiffres clés de la justice – Justice pénale » – <http://www.justice.gouv.fr/chiffres/penale03.htm>.

Si le code pénal réprime sévèrement la détention, la diffusion, l'enregistrement, la fixation et la production de représentation à caractère pornographique, il n'incrimine pas les incitations à commettre des viols ou agressions sexuelles qui ne seraient pas suivies d'effets. Un amendement sénatorial visant directement la diffusion de tels messages sur l'internet, avait ainsi été rejeté au cours de la discussion du projet de loi relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des enfants au motif, selon les mots du rapporteur du texte, qu'«aux termes de l'article 23 de la loi de 1881 sur la presse, sont considérés comme complices ceux qui incitent directement à commettre un crime ou un délit, à condition que la provocation ait été suivie des faits, voire d'une tentative de crime<sup>39</sup>.» On note que cette provocation est notamment punissable lorsqu'elle est commise par «tout moyen de communication au public par voie électronique», en vertu de l'article 2 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

### **Unanimité et nuances des législations pénales européennes**

L'ensemble des pays d'Europe met en œuvre une législation permettant de lutter contre la pédo-pornographie, c'est-à-dire d'empêcher la production, la diffusion, et même, souvent, la détention de telles représentations. Ces infractions sont diversement sanctionnées. Certaines de ces dispositions, comme celles punissant la détention de pornographie infantine, sont d'adoption récente, même dans les pays réprimant de longue date la production et la diffusion de tels matériels comme la France<sup>40</sup>.

L'Union européenne s'est également saisie de ces questions. Le Conseil a adopté le 24 février 1997 une «action commune relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants». Par elle, les États membres acceptaient d'ériger en infractions pénales certains comportements comme «l'exploitation sexuelle des enfants aux fins de la production [...] de matériel à caractère pornographique, y compris la production, la vente et la distribution ou d'autres formes de trafic de matériel de ce type, et la détention de ce type de matériel<sup>41</sup>.»

La décision du Conseil du 29 mai 2000 «relative à la lutte contre la pédo-pornographie sur Internet<sup>42</sup>» a renforcé les mesures de prévention et de lutte contre la production, la diffusion et la détention d'images pédo-pornographiques. Elle a fixé des objectifs de répression effective de ces comportements, de coopération des points de contact spécialisés assurant une veille permanente du phénomène, et de coopération des acteurs étatiques et industriels au niveau national dans le «but d'empêcher et de combattre l'exploitation sexuelle des enfants et, en particulier, la production, le traitement, la diffusion et la détention de matériel pédo-pornographique sur internet.»

---

39. Charles Jolibois, Rapporteur du projet de loi devant le Sénat, Sénat, séance du 30 octobre 1997 – [http://www.senat.fr/seances/s199710/s19971030/s19971030\\_mono.html](http://www.senat.fr/seances/s199710/s19971030/s19971030_mono.html).

40. «La lutte contre la pornographie infantine». *Les documents de travail du Sénat. Série Législation comparée*. N° LC 90. Sénat. Service des Affaires européennes. Paris. 18 mai 2001.

41. Action commune 97/154/JAI du 24 février 1997 adoptée par le Conseil relative à la lutte contre la traite des êtres humains et l'exploitation sexuelle des enfants.

42. Décision 2000/375/JAI du Conseil du 29 mai 2000 relative à la lutte contre la pédopornographie sur l'internet. *JOUE* n° L 138 du 09/06/2000. pp. 1-4.

Ces principes constituent les principales orientations du Plan d'action pour un internet plus sûr (*Safer Internet Action Plan*) de la Commission européenne. Ce plan d'action pluriannuel comporte par exemple, depuis sa mise en place en 1998, une ligne d'action tendant à « créer un réseau européen de lignes directes » de signalement des contenus illicites. 5,88 millions d'euros étaient consacrés par le programme de travail 1999-2002 au développement de ces lignes directes; 3,3 millions d'euros y ont été alloués dans le programme de travail 2002-2004<sup>43</sup>. De 2005 à 2008, la Commission européenne investira encore 45 millions d'euros dans ce plan d'action<sup>44</sup>.

Abrogeant l'action commune de 1997, la décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie, unifie les législations pénales des États membres. Elle prend spécifiquement en compte les risques liés à la diffusion de tels matériels sur les réseaux en précisant que « la pédopornographie [...] prend de l'ampleur et se propage par le biais de l'utilisation des nouvelles technologies et de l'internet<sup>45</sup>. » La décision-cadre définit la pédopornographie comme la représentation visuelle « d'un enfant réel », « une personne réelle qui paraît être un enfant », ou « des images réalistes d'un enfant qui n'existe pas » « participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne ». Alors que les législations nationales fixaient l'âge à partir duquel peut être faite la représentation pornographique d'une personne entre 14 et 18 ans, le texte impose l'âge de 18 ans, sans toutefois modifier l'âge de la majorité sexuelle dans les États membres. La décision-cadre a enfin pour objet d'uniformiser les législations européennes en requérant que des peines privatives de liberté maximales de un à trois ans soient prévues à l'encontre des personnes qui produisent, distribuent, diffusent, transmettent, acquièrent et détiennent du matériel pédopornographique.

## **Une illustration de l'hétérogénéité des dispositifs pénaux dans le monde**

### **États-Unis**

Souvent dénoncés comme le territoire hébergeant le plus grand nombre de serveurs d'images pédopornographiques, les États-Unis disposent pourtant d'un dispositif pénal complet en matière de lutte contre la production, la diffusion et la détention de ce type de contenus, qui a inspiré pour partie la décision-cadre européenne.

Une succession de textes adoptés depuis 1977 a défini un cadre prohibant la détention, la production et la diffusion de représentations pornographiques de mineurs de moins de 18 ans. L'article 2251 du Code fédéral condamne ainsi la production d'images d'un enfant de moins de 18 ans « se livrant à un comportement sexuellement

---

43. Les programmes de travail du Plan d'Action pour un Internet plus sûr (*Internet Action Plan*) peuvent être consultés à l'adresse : [http://europa.eu.int/information\\_society/programmes/iap/programmes/workprogramme/text\\_en.htm](http://europa.eu.int/information_society/programmes/iap/programmes/workprogramme/text_en.htm).

44. Voir : [http://europa.eu.int/information\\_society/activities/sip/news\\_events/saferinternet\\_plus/index\\_en.htm](http://europa.eu.int/information_society/activities/sip/news_events/saferinternet_plus/index_en.htm). La proposition de décision instituant le plan « *Safer Internet Plus* » a été agréée par le Conseil le 2 décembre 2004.

45. Décision-cadre 2004/68/JAI du Conseil du 22 décembre 2003 relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie. *JOUE* n° L 13 du 20/01/2004. pp.44-48.

*explicite*», ce dernier étant défini comme les relations sexuelles, quelle que soit leur nature, la zoophilie, la masturbation, les violences sado-masochistes et l'exhibition lascive des parties génitales ou de la région pubienne. L'article 2252 du Code fédéral punit la diffusion et la possession d'images représentant une telle scène réalisée ou simulée avec la participation effective d'un mineur. Le Code fédéral ajoute une circonstance aggravante à l'infraction lorsque les images possédées ou diffusées ont franchi une frontière.

Le *Child Pornography Prevention Act* (CPPA), qui avait pour objectif de criminaliser les représentations pédo-pornographiques virtuelles, rendues possibles par les nouvelles techniques de traitement de l'image, a été jugé inconstitutionnel par la Cour suprême le 16 avril 2002 en vertu des dispositions du Premier amendement à la Constitution, la prohibition de la représentation d'images d'enfants fictifs paraissant susceptible d'entraver la création artistique<sup>46</sup>.

En conclusion, ce n'est pas dans d'éventuelles carences de la législation qu'il convient de rechercher les causes de la récurrence des signalements de serveurs d'images pédo-pornographiques hébergés sur le territoire des États-Unis. D'autres explications peuvent être avancées, comme par exemple le grand nombre de services d'hébergement de sites *web* gratuits ou à bas prix situés sur le territoire des États-Unis<sup>47</sup>, ou le fait que les autorités américaines semblent plutôt concentrer une grande partie de leurs efforts sur la lutte contre les contacts entre de potentiels agresseurs sexuels et des enfants sur l'internet.

### **Japon**

Longtemps désigné comme une source importante de pornographie enfantine, le Japon a mis en place, en 1999, une législation pénale adaptée. La loi «punissant les actes liés à la prostitution enfantine et à la pédo-pornographie» rend illégaux la production, la diffusion et la vente de pédo-pornographie. La diffusion de pornographie enfantine sur l'internet peut ainsi être punie de trois ans d'emprisonnement.

### **Fédération de Russie**

La Fédération de Russie est fréquemment désignée, au côté des États-Unis, comme l'un des pays hébergeant le plus grand nombre de serveurs pédo-pornographiques, et comme un territoire où la production de tels contenus reste active.

Le Code pénal russe punit la production non autorisée de contenus pornographiques à des fins de diffusion, quel que soit le support, mais ne prévoit pas de dispositions particulières en matière de pédo-pornographie, ni ne réprime spécifiquement la diffusion, l'acquisition ou la détention de pornographie. La production de contenus pédo-pornographiques est toutefois susceptible d'être poursuivie comme une infraction sexuelle commise sur un mineur.

---

46. Agathe Lepage, *Libertés et droits fondamentaux à l'épreuve de l'internet*, éditions du Juris-Classeur, Paris, 2002, pp.176-177

47. Pour l'association Le Bouclier, «Plus de la moitié des sites pédophiles sont hébergés sur des machines se situant physiquement sur le territoire des États-Unis et du Canada. Les sites "russes" sont pour la plupart installés sur des serveurs américains et font partie de ceux qui produisent le plus de richesses en offrant à la vente des vidéos (...)». Le Bouclier, *op. cit.*

Malgré le « non alignement » de son droit pénal, la Russie participe au groupe de lutte contre la pédo-pornographie qui se réunit au sein du G8, et a pris part à quelques initiatives ponctuelles en matière de coopération judiciaire, comme l'opération « Blue Orchid », qui a abouti en 2001 au démantèlement d'un réseau de production de pédo-pornographie par les douanes américaines et la police de Moscou.

### **Les apports de la Convention sur la cybercriminalité**

La Convention sur la cybercriminalité du Conseil de l'Europe, adoptée à Budapest par le Comité des ministres le 8 novembre 2001, est le premier traité international portant en particulier sur les infractions liées à la criminalité informatique et, notamment, à la pornographie enfantine sur l'internet. Son principal objectif, énoncé dans le préambule, est de poursuivre « *une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale* »<sup>48</sup>.

L'article 9 de la Convention fait ainsi de la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique, de l'offre ou de la mise à disposition, du fait de se procurer ou de procurer à autrui, ou encore de la possession de pornographie enfantine dans ou par un système informatique, une infraction destinée à être traduite dans le droit interne de l'ensemble des pays signataires. « Pornographie enfantine » est ici entendu comme la représentation visuelle d'« *un mineur se livrant à un comportement sexuellement explicite* », d'« *une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite* », ou « *des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.* » Le terme « mineur » désigne dans la Convention toute personne âgée de moins de 18 ans ; un État-partie peut toutefois fixer une limite d'âge inférieure, qui doit être au minimum de 16 ans.

Signé au 30 septembre 2004 par trente-huit des quarante-cinq États représentés au Conseil de l'Europe, dont les États-Unis, et ratifié par huit d'entre eux seulement, au nombre desquels ne figure par la France<sup>49</sup>, le traité est entré en vigueur le 1<sup>er</sup> juillet 2004. La Russie n'a pas signé ce traité.

Il ressort de cette brève analyse de quelques-uns des régimes applicables à la diffusion de pédo-pornographie sur l'internet que les carences en matière pénale ne peuvent expliquer à elles seules la persistance et l'accroissement de la diffusion de pédo-pornographie sur l'internet.

### **Organisation et moyens des services d'enquête en France**

La poursuite des actes de production, de diffusion et de détention d'images pédo-pornographiques liés à l'internet fait intervenir, en France, différents services de police et de gendarmerie, spécialisés ou non.

---

48. Conseil de l'Europe, Convention STE n° 185 sur la Cybercriminalité, 8 novembre 2001.

49. Albanie, Croatie, Estonie, Hongrie, Lituanie, Macédoine, Roumanie, Slovaquie.

## Services de police

La Division nationale de répression des atteintes aux biens et personnes (DNRAPB) anime depuis 1997 un groupe de six enquêteurs formés et dédiés aux enquêtes sur l'internet. Ce service observe une croissance exponentielle des signalements qui lui sont adressés, qui sont passés de 300 à 400 signalements au cours des dernières années à plus de 3000 signalements en 2004, tandis que le nombre de personnels que la division consacre à ces affaires est demeuré inchangé. La DNRAPB traite en propre près de 10 % des affaires qui lui sont signalées, et transmet le solde aux juridictions dont relèvent les suspects identifiés. La plupart des signalements transmis à la DNRAPB font suite à la saisie d'adresses IP et de coordonnées de cartes bancaires françaises par des autorités étrangères, qui les transmettent en masse aux autorités nationales par les canaux de coopération judiciaire internationaux<sup>50</sup>.

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est constitué depuis mai 2000 en centre de compétences et de coordination où doivent se rencontrer « *le ministère de la Défense (Direction générale de la gendarmerie nationale) et le ministère de l'Économie, des Finances et de l'Industrie (Direction générale des douanes et droits indirects et direction générale de la concurrence, de la consommation et de la répression des fraudes).* » L'Office doit notamment « *animer et [...] coordonner, au niveau national, la mise en œuvre opérationnelle de la lutte contre les auteurs et complices d'infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication* », « *procéder, à la demande de l'autorité judiciaire, à tous actes d'enquête et de travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ou liée à l'utilisation des technologies de l'information et de la communication*<sup>51</sup>. » L'OCLCTIC apporte ainsi l'expertise de ses personnels en soutien à d'autres services en matière d'interprétation de données de connexion, d'analyse de disques durs saisis et perquisitionnés, etc.

L'OCLCTIC procède également au traitement des signalements de contenus pédopornographiques adressés par les internautes sur le site officiel [www.internet-mineurs.gouv.fr](http://www.internet-mineurs.gouv.fr). La création de ce site a été décidée par le Gouvernement lors du Conseil de Sécurité intérieure du 13 novembre 2001, qui avait pour objectif de dégager les moyens d'une plus grande protection des enfants et d'une répression accrue des infractions à caractère sexuel dont ces derniers sont victimes. Une base de données regroupe l'ensemble des informations relatives aux sites signalés afin de disposer de toutes les informations nécessaires à l'engagement des poursuites et de rapprocher les informations issues de signalements ultérieurs. L'OCLCTIC peut demander à un prestataire ou à un juge de bloquer, ou informer un magistrat en vue de faire bloquer l'accès à des contenus hébergés en France. Il signale ces contenus au parquet de Paris ou informe les services d'Interpol lorsque les signalements concernent des matériels hébergés hors de France.

---

50. Marcel Faure, audition du 27 avril 2004.

51. Décret n° 2000-405 du 15 mai 2000 portant création d'un office central de lutte contre la criminalité liée aux technologies de l'information et de la communication.



Les services territoriaux de la police judiciaire, placés auprès des Directions régionales de la police judiciaire (DRPJ) peuvent également intervenir, sur saisine d'un parquet ou de leur propre initiative. Ainsi la Brigade de protection des mineurs (BPM) de la Direction régionale de la police judiciaire (DRPJ) de Paris, dont la compétence territoriale couvre la région la plus « connectée » de France, qui est aussi la zone d'implantation des principaux fournisseurs d'accès à l'internet, a constitué un groupe de trois (2003), puis de six (2004) enquêteurs dont l'activité se concentre sur la recherche et la poursuite d'infractions impliquant l'utilisation des technologies de l'information. Au cours de sa première année d'existence, en 2003, ce groupe « Internet » a traité 96 affaires ayant trait dans leur grande majorité à la diffusion et à la détention de pédopornographie sur l'internet. À la date de leur audition, en mai 2004, les enquêteurs de la BPM prévoyaient de traiter plus de 300 dossiers en 2004<sup>52</sup>.

Avec le soutien de 50 enquêteurs spécialisés en criminalité informatique (ESCI) spécifiquement formés à la recherche d'infractions liées aux nouvelles technologies, les services de police locaux sont enfin également fondés à intervenir, d'autorité ou sur saisine du parquet, dans les affaires relevant de leur compétence territoriale.

### **Services de gendarmerie**

La Gendarmerie nationale intervient également dans la lutte contre la diffusion et la détention d'images pédopornographiques sur l'internet.

De compétence nationale, le département Internet du Service technique de recherches judiciaires et de documentation (STRJD) procède depuis 1998, d'initiative ou sur information des unités de la gendarmerie nationale ou de tiers ayant déposé un signalement sur l'adresse [sitepj@gendarmerie.defense.gouv.fr](mailto:sitepj@gendarmerie.defense.gouv.fr), à la surveillance et à la recherche d'infractions sur les principaux protocoles de l'internet. C'est auprès de ce service qu'a été placé le Centre national d'analyse des images pédopornographiques (CNAIP), qui collecte depuis octobre 2003 l'ensemble des images recueillies par les différents services d'enquête français, en sorte d'opérer analyses et rapprochements permettant d'apporter une aide concrète aux enquêteurs de police et de gendarmerie. Ce service a récemment fait l'acquisition du logiciel Image Seeker, conçu par la société française LTU Technologies, qui facilite ces rapprochements.

Depuis 1992, le département informatique-électronique (INL) de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) apporte un soutien technique (expertises, surveillance, interceptions) aux différents services de gendarmerie. Les examens scientifiques et les expertises conduites par l'IRCGN pour les enquêteurs et les magistrats ont porté, en 2003, sur plus de 2,4 téra-octets de données, dont plus de 80 % étaient relatives à des affaires de pédophilie et de pédopornographie.

Avec le soutien de 80 personnels « NTECH » spécifiquement formés aux techniques d'enquête propres aux infractions liées aux nouvelles technologies, les différents services régionaux comme départementaux de gendarmerie sont également fondés à intervenir sur saisine et d'initiative. Comme on le notait plus haut, M. Philippe Jarlov, enquêteur de la section des Recherches de Bordeaux, détecte par exemple

---

52. Marie Lajus, Fabrice Gauthier, audition du 11 mai 2004.

les serveurs de diffuseurs de contenus pédo-pornographiques basés dans toute la France à l'aide d'outils logiciels permettant l'automatisation de cette opération.

### **Freins à la poursuite et à la répression de la diffusion des contenus pédo-pornographiques**

Les services de police et de gendarmerie nationaux et, de plus en plus fréquemment, régionaux, regroupent de précieuses compétences. Le dispositif d'ensemble de répression de la diffusion de contenus pédo-pornographiques sur l'internet n'en paraît pas moins souffrir d'une grande complexité et du manque de moyens en personnels, en équipement et en capacités d'intervention.

#### ***La nécessaire évolution des moyens humains et matériels***

Les effectifs des services et groupes d'enquête spécialisés dans la répression des infractions commises par le vecteur des technologies de l'information n'ont pas évolué dans les mêmes proportions que le volume des dossiers relatifs à des cas de diffusion et de recel d'images pédo-pornographiques sur l'internet. Selon certains enquêteurs, le manque de moyens en personnels compétents, mais aussi en matériel et logiciels appropriés, fait aujourd'hui courir le risque que certains services d'enquête se trouvent contraints de privilégier la poursuite de certaines infractions plutôt que d'autres, ou ne soient pas en mesure d'atteindre certains objectifs, comme la recherche des mineurs victimes.

Le 7 septembre 2004, le ministre de l'Intérieur Dominique de Villepin, qui a fait de la lutte contre la cybercriminalité l'une de ses priorités, a annoncé un effort de formation d'enquêteurs de police et de gendarmerie spécialisés, dont l'effectif doit passer, à l'horizon 2007, à 300, puis 600. Au niveau national, les effectifs de l'OCLCTIC seraient amenés à passer de 38 à 75, et ceux de l'IRCGN de 30 à 50 gendarmes.

#### ***La relative dispersion des structures d'enquête***

L'analyse de l'organisation des services d'enquête permet de constater l'éclatement des unités de police et de gendarmerie, dont les actions à l'encontre des diffuseurs ou acquéreurs d'images pédo-pornographiques sur l'internet ne font l'objet d'aucune coordination systématique. Plusieurs services d'enquête, spécialisés ou non, locaux ou nationaux, de gendarmerie ou de police peuvent ainsi mener des enquêtes sur des faits identiques ou connexes, sans pour autant recouper et partager leurs informations et conclusions. Dans un domaine d'étendue et de compétence nationale, voire internationale, on conçoit pourtant l'utilité d'un organisme central rassemblant tous les services concernés (police et gendarmerie, notamment) ayant mission de collecter toutes les informations relatives aux enquêtes en cours et d'assurer efficacement la coordination des unités spécialisées ou régionales en matière de lutte contre la pédo-pornographie sur l'internet.

Le ministre de l'Intérieur a annoncé son intention de procéder à la réorganisation des services de lutte contre les infractions liées aux technologies de l'information, le pôle de la gendarmerie étant dédié à la veille des contenus pédo-pornographiques et des activités pédophiles, et le pôle de la police nationale plus particulièrement aux faits

de racisme, d'antisémitisme et de haine raciale, de terrorisme et de piratage informatique<sup>53</sup>. Les modalités précises de cette réorganisation restent à préciser.

#### ***L'organisation territoriale des juridictions***

Chaque juridiction étant territorialement compétente, les affaires de diffusion ou de recel de matériels pédo-pornographiques sont susceptibles d'être traitées sans réelle coordination par une multitude de magistrats diversement formés. Certains magistrats et enquêteurs suggèrent ainsi que les compétences spécifiques à la répression de la cybercriminalité pourraient être utilement renforcées, voire mutualisées, dans certaines juridictions<sup>54</sup>.

Le parquet général près la Cour d'appel de Paris compte aujourd'hui de fait un magistrat spécialisé pour les affaires ayant trait aux technologies de l'information, auquel il y a lieu d'ajouter les neuf « magistrats référents » des parquets du ressort. Le parquet général près la Cour d'appel de Versailles a mis en place le même dispositif.

#### ***Les limites de la procédure pénale***

Examinant une affaire criminelle où un particulier, « navigant sur internet, a été choqué des découvertes qu'il a faites sur un site pédophile, et a voulu démasquer en se faisant passer pour un adolescent de 14 ans, les utilisateurs de ce site », la chambre criminelle de la Cour de cassation a considéré, dans un arrêt du 1<sup>er</sup> octobre 2003, qu'« il ne peut être reproché un manque de loyauté à une personne physique qui veut, par un stratagème, empêcher de nuire les délinquants sexuels utilisant un site constitué sur des crimes commis à l'égard de jeunes enfants », admettant ainsi que l'on puisse recourir à une identité d'emprunt pour démasquer une infraction, pour autant qu'il n'y ait pas provocation à agir<sup>55</sup>.

Il n'est toutefois pas certain que les enquêteurs soient pour autant légitimés à agir selon ces méthodes lorsqu'ils recherchent proactivement des diffuseurs de pédo-pornographie sur l'internet. Les enquêteurs ne peuvent de plus agir, aux fins de l'enquête, en « *coauteurs, complices ou receleurs* » des infractions ou de leurs produits, ni proposer une ou plusieurs images pédo-pornographiques aux animateurs de serveurs spécialisés, qui les exigent souvent avant d'autoriser l'accès d'internautes aux contenus illicites qu'ils distribuent. En l'absence de cadre légal spécifique, les enquêteurs recourant à une identité d'emprunt restent de plus susceptibles d'usurper l'identité d'un autre utilisateur de l'internet ou d'un service donné<sup>56</sup>.

---

53. Allocution de Dominique de Villepin sur la lutte contre la cybercriminalité, 7 septembre 2004 – [http://www.interieur.gouv.fr/rubriques/c/c1\\_le\\_ministre/c13\\_discours/2004\\_09\\_08\\_cybercriminalite](http://www.interieur.gouv.fr/rubriques/c/c1_le_ministre/c13_discours/2004_09_08_cybercriminalite).

54. Yvon Tallec, audition du 8 juin 2004.

55. Cass. crim., 1<sup>er</sup> octobre 2003, n° 03-84142.

56. L'usurpation d'identité devient un délit pénal dès l'instant où « *le fait de prendre le nom d'un tiers, [a été opéré] dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales* » (art. 434-23 du Code pénal). La condition, pour que le délit soit constitué, tient à ce qu'ait été pris « *le nom d'un tiers* ». A ce jour, il n'existe pas de jurisprudence qui puisse affirmer qu'emprunter un pseudonyme, une adresse IP ou une adresse de courrier électronique puisse être assimilable au « *nom* » évoqué dans l'article 434-23.

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité définit dans le Code de procédure pénale la notion d'infiltration et la procédure qui l'encadre : « *l'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans des conditions fixées par décret et agissant sous la responsabilité d'un officier de police judiciaire chargé de coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer, auprès de ces personnes, comme un de leurs coauteurs, complices ou receleurs*<sup>57</sup>. » À cette fin, l'agent infiltré peut recourir à une identité d'emprunt et, si nécessaire, acquérir, détenir, transporter, livrer ou délivrer des substances, biens, produits, documents ou informations tirés de la commission des infractions ou servant à leur commission, sans être tenu responsable de ces actes. Une telle procédure est aujourd'hui limitée aux enquêtes portant sur certains délits commis « en bande organisée », dont la liste limitative est définie à l'article 706-73 du Code de procédure pénale, et n'inclut pas la diffusion ou la détention d'images pédo-pornographiques. Certains enquêteurs souhaitent que ce procédé soit étendu à la recherche des contenus pédo-pornographiques et de leurs diffuseurs, afin de pouvoir démanteler plus facilement les réseaux d'échange de ces contenus.

Bon nombre d'enquêteurs soulignent enfin leur incapacité à constater la diffusion d'images pédo-pornographiques sur les sites dont l'accès est conditionné au paiement d'un droit d'accès par carte bancaire. Ils suggèrent que leurs moyens procéduraux et financiers soient étendus en sorte de pouvoir procéder, aux fins de l'enquête, à de telles opérations de paiement.

Introduit par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, l'article 706-95 du Code de procédure pénale prévoit que « *si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 [crimes et délits commis en bande organisée, dont sont exclues les atteintes aux mineurs et les infractions relatives à la pédo-pornographie] l'exigent, le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention.* » Certains enquêteurs souhaitent que cette procédure spécifique puisse être étendue à la recherche d'infractions liées à l'échange d'images pédo-pornographiques et permette l'accès aux comptes de courrier électronique de suspects, ainsi qu'aux espaces de stockage de documents qui y sont fréquemment associés.

Ces propositions d'extension des moyens procéduraux des autorités policières, si elles permettaient sans doute de renforcer les capacités d'action des enquêteurs, n'en comporteraient pas moins des risques, notamment en matière de libertés publiques. Certains opposants à la loi du 9 mars 2004 craignent ainsi que les dispositions de ce texte ne soient appliquées abusivement, hors du cadre strict qui leur est

---

57. Loi n° 2004-204 du 9 mars 2004, art. 1. Code de procédure pénale, art. 706-81 et suivants.

imposé ou sans égard pour la gravité des faits suspectés ou poursuivis, et que le fait de rendre applicables les dispositions spéciales de la loi à l'enquête préliminaire en matière de recel de pornographie infantine n'ouvrent la voie à certains excès comme, par exemple, l'interception des communications électroniques et l'accès aux espaces de stockage en ligne de tous les correspondants identifiés d'un receleur avéré... Les bénéfices attendus de telles dispositions doivent ainsi être considérés au regard de la gravité du phénomène et de tels risques. Enfin, on peut se demander s'il est utile de procéder à l'extension des moyens de rechercher des infractions sans que soient étendus dans le même temps les moyens consacrés au traitement de ces dernières.

## **Moyens et limites de la coopération policière et judiciaire internationale**<sup>58</sup>

Les législations dont se sont dotés un grand nombre d'États dans les années 1990 ne suffisent pas en elles-mêmes à remédier aux difficultés liées à l'accessibilité universelle des contenus sur l'internet. Les États doivent également se doter d'instruments de coopération policière et judiciaire adaptés à la poursuite d'infractions dans l'environnement ouvert qu'est l'internet.

Cette coopération peut contribuer à remplir certains objectifs intermédiaires ou finaux de l'action judiciaire que les autorités nationales ne peuvent atteindre seules : faire procéder au retrait de contenus illicites hébergés sur le territoire d'un autre État au vu d'une décision judiciaire française exécutoire, identifier le propriétaire, l'animateur ou un utilisateur d'un service en ligne, interpellé un suspect...

### **Les outils d'investigation à l'étranger et les instruments de la coopération policière**

La coopération policière internationale est régie par l'accès à des centres de ressources qui apportent une aide aux enquêteurs. Ces centres ont notamment pour finalité de coordonner l'action des services répressifs de plusieurs États et de leur apporter l'assistance utile en terme de rapprochement, de recherches et d'échanges d'informations. Ils sont notamment compétents en matière de traite des êtres humains, de pédo-pornographie et d'atteintes à la dignité humaine. Les centres ressources facilitent la lutte contre le crime et la délinquance en offrant leurs expertises aux services d'enquêtes. Des améliorations et des aménagements de leurs modes de fonctionnement paraissent toutefois encore nécessaires.

#### ***Interpol***

Le rôle de l'Organisation internationale de police criminelle (OIPC) Interpol consiste à coordonner l'action des polices des États membres, qui interviennent à la fois comme fournisseurs et demandeurs d'informations et de services. Interpol facilite également l'échange d'expérience et la définition de principes d'action communs, l'organisation

---

58. Myriam Quemener, sous-directrice de la justice pénale générale, et Joël Ferry, officier de liaison à la Direction des affaires criminelles et des grâces, ont largement contribué à la rédaction de cette partie. Qu'ils en soient remerciés.

de sessions de formation ou encore l'élaboration de guides des meilleures pratiques destinés aux services d'enquêtes.

La coopération s'applique à tous les types d'activité criminelle ou délictuelle qui présentent un caractère ou un élément international. Elle s'exerce spécialement dans les domaines de la criminalité de violence contre les personnes et la criminalité contre les biens. Interpol participe ainsi activement à la lutte contre l'exploitation sexuelle des enfants y compris sur l'internet.

Afin d'apporter un soutien immédiat aux enquêteurs chargés de mener des investigations sur une ou plusieurs infractions perpétrées sur ou au moyen de l'internet, et sous l'impulsion du G8, Interpol a décidé la mise en œuvre de points de contact fonctionnant 24 heures sur 24 et 7 jours sur 7 dans les services de police des États associés. En France, c'est l'OCLCTIC qui remplit cette fonction. Interpol développe également des instruments nouveaux, comme une base de données centrale d'images pédo-pornographiques alimentée par tous les États membres et susceptible d'être interrogée à la demande de leurs autorités. Un tel outil permettra de rapprocher des informations et de participer plus efficacement à la lutte contre les crimes mettant en scène des mineurs. La France dispose au Centre national d'analyse des images pédo-pornographiques (CNAIP) d'un instrument de ce type, qui doit à présent monter en puissance.

En dépit de certains succès d'importance, comme le concours apporté par Interpol dans le cadre de l'opération « Cathédrale », au cours de laquelle 108 personnes ont été interpellées dans 13 États différents, dont la France, cette organisation comporte des limites : les enquêteurs font observer que les signalements et les informations transmis d'État à État par l'intermédiaire du secrétariat général d'Interpol transitent trop lentement et ne sont pas toujours suivis d'interventions des services de police destinataires des signalements. Ces signalements font surtout rarement l'objet d'une réponse : la « voie de retour » prévue par Interpol est peu exploitée.

### ***Europol***

L'office européen de police – Europol, dont l'organisation et les missions sont prévues par la convention du 26 juillet 1995, est chargé du traitement des renseignements relatifs aux activités criminelles au sein de l'Union européenne (UE). Il constitue un point central de coordination et de coopération, chargé de soutenir les services enquêteurs afin de rationaliser leurs efforts et compléter leurs moyens en ce qui concerne la prévention et la lutte contre les formes graves de criminalité internationale organisée<sup>59</sup>.

Europol peut ainsi faciliter les enquêtes relatives à des faits de diffusion et de recel de contenus pédo-pornographiques sur l'internet entre États européens. Il intervient en facilitant l'échange d'informations, en fournissant des analyses opérationnelles et stratégiques, en apportant son expertise et son assistance techniques aux enquêtes. Pour cela, il dispose d'un système d'informations qui n'a toutefois pas encore atteint

---

59. Voir Alex Türk, *Quand les policiers succèdent aux diplomates*, Rapport d'information 523 (97-98), Paris, Sénat (Commission des lois), 1998.

sa pleine maturité. Cependant, les échanges directs et rapides de données peuvent également intervenir entre les officiers de liaison des États membres.

Les fichiers d'analyse enrichis des informations communiquées par les services d'enquête des États membres de l'Union européenne constituent aujourd'hui, d'après les enquêteurs, une plus-value au travail des enquêteurs pour combattre les réseaux criminels, examiner leur complexité et les diverses formes de leur manifestation. Un fichier d'analyse concernant la pédophilie sur Internet a été créé pour approfondir cette question. Un séminaire a été organisé sur ce thème en juin 2001 à La Haye. Enfin, en relation avec les services répressifs allemands, quatre séminaires de formation d'enquêteurs ont été organisés sur le thème de « la lutte contre l'exploitation sexuelle des enfants ».

Pour traiter les dossiers, les services répressifs des États membres de l'Union européenne pourront constituer des équipes conjointes et mener des actions spécifiques d'enquête y compris des actions opérationnelles conjointes, comprenant en appui des représentants d'Europol.

### **Schengen**

Le 14 juin 1985, a été conclu à Schengen, un accord international visant, dans le cadre défini par l'acte unique européen, la création de l'espace communautaire sans frontière dénommé Schengen. Une convention signée le 19 juin 1990, complète cet accord et en précise les modalités d'application<sup>60</sup>.

La coopération entre les États de l'Union européenne s'appuie aussi sur ce dispositif, qui définit le cadre de l'assistance mutuelle aux fins de la prévention et de la recherche de faits punissables, et permet l'intensification de la coopération policière dans les régions frontalières (article 39 de la convention)<sup>61</sup>. Le système d'information Schengen permet l'échange d'informations entre les États signataires et la consultation automatisée de données sur les personnes. Ces outils sont susceptibles d'être employés au profit de la répression de la diffusion et du recel d'images pédo-pornographiques entre États frontaliers signataires.

Les différents canaux de coopération policière au sein de l'Union européenne (Europol, Schengen) ne communiquent pas encore entre eux. Des discussions sont toutefois engagées pour permettre aux instances d'Europol d'accéder aux données contenues dans le système d'information Schengen<sup>62</sup>. La combinaison de ces outils dessine un cadre de coopération pertinent et semble pouvoir constituer un levier effi-

---

60. La convention de Schengen concernera à terme tous les États de l'Union européenne. Pour l'heure, l'Islande a rejoint les États Schengen. En revanche le Royaume-Uni et l'Irlande qui avaient refusé jusqu'à présent d'adhérer à l'accord préparent leur intégration pour septembre 2004.

61. À cela, il convient d'ajouter la possibilité pour les enquêteurs d'exercer un droit de suite (art 40 de la CASS) et d'observation (art 41 de la CASS)

62. Le parlement européen ne semble pas opposé à cette mesure. La commission des libertés, en a cependant fixé les limites : « le droit pour Europol d'utiliser le système de recherche du SIS devra être soumis au respect de certaines conditions de protection des données ». Par ailleurs Europol ne pourra consulter que « les données qui se rapportent à l'objet pour lequel celles-ci ont été fournies et qui sont nécessaires à l'accomplissement de ses missions ». La commission ajoute qu'« Europol ne doit pas pouvoir transmettre les données auxquelles il a accès à des États ou des organismes tiers ».

cace dans la lutte contre la diffusion et le recel de contenus pédo-pornographiques sur le territoire de l'Union européenne, dont tous les membres punissent désormais ces comportements.

#### ***Au sein du G8: le groupe de Lyon***

Le sous-groupe « haute technologie » du groupe de Lyon du G8 constitue enfin un lieu informel de réflexion et d'orientation des politiques de sécurité des États, dont l'influence n'est pas négligeable au sein des instances internationales. Il est à l'initiative de la base de données centrale d'images pédo-pornographiques mise en place par Interpol. La coopération renforcée des polices de Grande-Bretagne, des États-Unis, du Canada et d'Australie, y a ainsi été lancée en décembre 2003 sous la forme d'une *International Virtual Global Task Force* coordonnant les activités de certains services nationaux.

Il ressort de l'examen de la mise en œuvre des instruments existants que, si la coopération policière paraît se développer de manière satisfaisante aux niveaux global et européen en matière de lutte contre les contenus pédo-pornographiques sur l'internet, cette dernière n'est pas encore pleinement exploitée, et paraît encore largement entravée par le formalisme des procédures qui l'encadrent. Ainsi, de nombreux échanges d'informations entre enquêteurs ont encore lieu, en marge des procédures officielles, sur des bases informelles.

#### **L'entraide judiciaire**

L'entraide judiciaire en matière pénale concerne la coopération entre les magistrats. Elle peut mener à l'extradition d'un ressortissant.

#### ***L'entraide judiciaire en matière pénale***

Il existe une multiplicité de sources juridiques de l'entraide judiciaire en matière pénale. Celle-ci peut être réglée par des conventions bilatérales à l'exemple de la convention d'assistance juridique conclue entre la France et les États unis, des conventions multilatérales comme la convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 ou des conventions multilatérales spéciales comme la convention sur la cybercriminalité du Conseil de l'Europe.

Lorsqu'il n'existe pas de convention, à la différence de certains États, la France présente les demandes des magistrats français à des autorités judiciaires étrangères en proposant, à titre de réciprocité, une offre identique dans des affaires comparables.

L'entraide judiciaire en matière pénale est par exemple réglée avec les États-Unis par un traité signé à Paris le 10 décembre 1998. Il est entré en vigueur le premier décembre 2001. C'est un instrument qui traite entre les deux pays de l'ensemble des questions liées à l'entraide judiciaire. Il n'est pas nécessaire que l'infraction poursuivie par l'un des deux États constitue également une infraction dans l'autre État pour mettre en œuvre les mesures d'entraide. Les dispositions de cet instrument s'appliquent à la cybercriminalité en général et à la lutte contre la pédo-pornographie en particulier en permettant notamment de recueillir sur le territoire de l'autre État toute image ou donnée relative à ce type d'infractions. L'instrument prévoit que l'entraide concerne tous les actes « non prohibés par la législation de l'État requis ». Les



mécanismes particuliers d'entraide sont d'ailleurs visés dans le texte notamment les perquisitions, saisies et même les confiscations. Il arrive que dans le domaine de la pédo-pornographie, lorsque les serveurs sont implantés à l'étranger, certains États ne répondent pas à une demande d'entraide.

Il convient dès lors de rechercher au cas par cas l'existence de conventions liant la France avec d'autres États, et vérifier la nature de l'entraide qui y est visée.

En Europe, l'entraide judiciaire est régie par une convention du Conseil de l'Europe du 20 avril 1959. Elle est matérialisée par un acte signé d'une autorité de justice qui demande à un homologue d'un autre pays de procéder à des mesures d'enquête pour l'affaire qu'elle instruit lorsque des investigations à l'étranger apparaissent nécessaires.

La Convention d'entraide de l'Union européenne signée le 29 mai 2000 vise à remédier aux principales difficultés de l'entraide judiciaire en assouplissant la gestion des dossiers et en introduisant un dialogue entre les parties afin d'éviter le blocage des demandes. Ainsi, les demandes d'entraide pourront être adressées directement de magistrat à magistrat sans passer par les administrations centrales, en utilisant éventuellement le courrier électronique. Les demandes d'entraide pourront être exécutées conformément aux procédures et aux formalités définies par l'État requérant. Il est prévu la possibilité de mettre en place des équipes communes d'enquête composées d'agents de services appartenant à plusieurs États. Le magistrat français pourra également procéder par vidéoconférence à l'audition d'un témoin, d'un expert ou de la personne poursuivie.

Mais cette convention, adoptée et signée par les quinze pays de l'Union européenne, doit encore être ratifiée par chacun des États de l'Union afin d'en inclure les principes dans le droit national des États et la rendre applicable. La ratification du texte par la France devrait intervenir très prochainement. La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité prend déjà en compte certains principes de la convention dans un chapitre consacré aux dispositions concernant la lutte contre la délinquance et la criminalité internationale. Un chapitre intitulé «de l'entraide judiciaire internationale» vise à améliorer les échanges entre les États. Un chapitre particulier de la loi est enfin consacré à l'Union européenne et aux pouvoirs reconnus aux agents étrangers détachés auprès d'une équipe commune d'enquête.

Au-delà de cette convention, d'autres dispositions, insufflées notamment par la convention d'application des accords de Schengen du 19 juin 1990, ont été adoptées en vue de favoriser l'entraide judiciaire. Il s'agit notamment de la simplification de la transmission des notifications d'actes de procédure et de certaines dénonciations d'infractions aux fins de poursuites entre les États parties, ainsi que de la transmission directe des demandes d'entraide judiciaire comme voie normale des échanges entre les autorités (article 53 de la convention). On ajoutera que l'article 31 du traité d'Amsterdam dispose que l'action en commun dans le domaine de la coopération judiciaire en matière pénale vise entre autres à faciliter l'extradition entre les États membres.

Enfin, la France a procédé avec d'autres États à l'échange de magistrats de liaison<sup>63</sup>. La réussite de cette expérience, qui a déjà porté ses fruits en matière de recueil de certaines preuves dans le cadre notamment d'enquêtes sur l'exploitation sexuelle de mineurs, a conduit l'Union européenne à imaginer un réseau couvrant l'ensemble des États de l'Union et fonctionnant vingt-quatre heures sur vingt-quatre. Ce réseau a pour finalité de faciliter l'exécution des demandes d'entraide judiciaire relatives aux formes graves de criminalité, de coordonner les demandes d'enquêtes judiciaires et de fournir toutes les informations nécessaires aux magistrats de l'Union européenne sur les systèmes juridiques, les textes en vigueur et les règles de procédure.

Cependant, malgré ces outils et avancées, certaines demandes d'entraide ne sont pas traitées avec célérité, ou pas du tout. De telles situations peuvent résulter de difficultés administratives, mais également de l'impact politique du contenu des demandes.

### ***Le régime de l'extradition***

La loi pénale française est applicable aux infractions commises sur le territoire de la République (art. 113-1 du code pénal). L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ces faits constitutifs a eu lieu sur le territoire (art. 113-2 du code pénal). En outre, la loi pénale française est applicable aux crimes et délits punis d'une peine d'emprisonnement commis hors du territoire de la République par un français ou par un étranger lorsque la victime est française.

L'extradition est le moyen juridique pour un État requérant de réclamer d'un État requis la mise à disposition d'une personne afin de procéder à sa traduction devant une juridiction de jugement ou à l'exécution de sa peine. La France a ratifié la Convention européenne d'extradition du 13 décembre 1957. En l'absence de texte international applicable, le droit d'extradition français est réglé par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, qui a introduit dans le code de procédure pénale un principe de réciprocité avec l'État concerné<sup>64</sup>.

Parmi les principes majeurs applicables, pour qu'une extradition obtienne une réponse favorable, il est nécessaire que les faits reprochés soient considérés comme un crime dans la législation de l'État demandeur et dans la législation française, selon le principe de la double incrimination, ou répondent à un seuil minimum de gravité. L'extradition pourra ne pas être prononcée par un État à l'égard d'un de ses ressortissants. En outre, conformément aux bonnes pratiques adoptées par les États du G8, un pays refusant l'extradition pour des motifs de nationalité s'engage à soumettre l'affaire à ses autorités judiciaires nationales en vue d'engager des poursuites contre la personne mise en cause.

Le mandat d'arrêt européen se substitue, au sein de l'Union européenne, au processus de l'extradition.

---

63. Tel est le cas avec les Pays Bas, l'Italie, l'Allemagne, l'Espagne, le Royaume Uni, et en dehors de l'Union européenne avec la République Tchèque et les États-Unis.

64. Articles 696 à 696-24 et 696-34 à 696-41 du Code de procédure pénale.

### **Le mandat d'arrêt européen**

Sur le plan de l'Union européenne, la décision-cadre<sup>65</sup> relative au mandat d'arrêt européen et aux procédures de remises entre États membres fait notamment référence à l'exploitation sexuelle des enfants, à la pédo-pornographie, et à la cybercriminalité. Dès lors que l'infraction est punie d'une peine de prison d'un maximum d'au moins trois ans, il n'est pas requis la double incrimination pour mettre à exécution ce mandat d'arrêt.

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité prévoit l'application en France du mandat d'arrêt européen et la levée de la double incrimination dans les affaires d'exploitation sexuelle des enfants et de pornographie infantile punies d'au moins trois ans d'emprisonnement :

*« Art. 695-23. – L'exécution d'un mandat d'arrêt européen est également refusée si le fait faisant l'objet dudit mandat d'arrêt ne constitue pas une infraction au regard de la loi française.*

*« Par dérogation au premier alinéa, un mandat d'arrêt européen est exécuté sans contrôle de la double incrimination des faits reprochés lorsque les agissements considérés sont, aux termes de la loi de l'État membre d'émission, punis d'une peine privative de liberté d'une durée égale ou supérieure à trois ans d'emprisonnement ou d'une mesure de sûreté privative de liberté d'une durée similaire et entrent dans l'une des catégories d'infractions suivantes :*

*[...]*

*« – exploitation sexuelle des enfants et pornographie infantile [...]. »*

### **Eurojust**

Intégré au traité de l'Union européenne par le conseil européen de Nice en décembre 2000, Eurojust est envisagé comme une unité de coopération opérationnelle de lutte contre la criminalité. Organe de l'Union européenne, il sera chargé de promouvoir et d'améliorer la coordination et la coopération entre les autorités judiciaires compétentes des États membres de l'Union européenne. Il pourra demander aux procureurs nationaux de faire procéder à une enquête ou d'engager des poursuites, de dénoncer des infractions aux autorités compétentes d'un autre État membre, de participer à la mise en place d'équipes communes d'enquête.

### **L'entraide judiciaire dans la Convention sur la cybercriminalité**

La Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001, est un instrument juridique majeur et inédit. Elle définit notamment des moyens et des axes de coopération internationale permettant de lutter plus efficacement contre la cybercriminalité.

---

65. Décision-cadre 2002/584/JAI du Conseil, du 13 juin 2002, relative au mandat d'arrêt européen et aux procédures de remise entre États membres. Le 6<sup>e</sup> considérant indique qu'il s'agit de la première concrétisation du principe de reconnaissance mutuelle que le Conseil européen a qualifié de pierre angulaire de la coopération judiciaire. Le mandat d'arrêt européen s'applique entre les États de l'Union européenne qui ont transposé cette décision. Sur les vingt-cinq États de l'Union européenne, seule l'Italie n'a pas encore transposé ce dispositif.

La Convention établit des principes de base en matière de procédure afin de trouver et recueillir les preuves électroniques nécessaires à découvrir et poursuivre les auteurs d'infractions perpétrées au moyen des réseaux numériques. Ces mesures portent sur la conservation de données, la perquisition et la saisie informatique, la collecte de données de connexion et l'interception des communications.

Selon les termes de la Convention, les services d'enquêtes des États doivent s'unir et s'entendre pour effectuer des actes d'enquête en lieu et place des services demandeurs et leur communiquer d'urgence les résultats obtenus. Aussi, en plus des formes traditionnelles d'entraide et d'extradition, la Convention propose de nouveaux moyens de procédure constituant une nouvelle forme d'entraide judiciaire. Par exemple, il pourra être procédé à une perquisition et saisie pour le compte d'un autre État, et toutes les informations utiles à l'enquête de l'État requérant devront être communiquées, notamment lorsque celles-ci ont transité par un État intermédiaire.

En matière d'extradition, la Convention dispose que si celle-ci est refusée sur la base de la nationalité de la personne recherchée ou parce que la partie requise s'estime compétente pour cette infraction, l'État requérant peut demander à l'État requis de soumettre l'affaire à ses propres autorités aux fins de poursuites et de lui rendre compte de l'issue de l'affaire.

Cet instrument juridique pourrait être considéré comme une norme de référence incontournable. Pourtant, force est de constater que depuis la signature de la Convention par trente-trois pays européens, auxquels il faut ajouter les États-Unis, le Japon, le Canada et l'Afrique du sud, huit États seulement ont ratifié le texte.

Il ressort en conclusion qu'il existe une grande diversité de vecteurs d'entraide judiciaire en matière pénale, qui complexifie le choix de l'instrument le plus pertinent. Tout en reconnaissant le principe de la souveraineté des États, les conventions facilitent les demandes d'entraide, élargissent de proche en proche le périmètre de leur application et ainsi limitent les refus d'application de leurs dispositions. Ces vecteurs peuvent être mobilisés aux fins de la lutte contre la pornographie enfantine sur l'internet. Toutefois, les délais inhérents au traitement de ces procédures internationales sont souvent dénoncés par les enquêteurs comme n'étant pas approprié au traitement d'affaires de pornographie enfantine sur l'internet, où les contenus sont extrêmement mobiles, et les auteurs des infractions localisés dans une multitude de pays : il n'est pas rare, en dépit des différents canaux de coopération existants, qu'une commission rogatoire internationale transmise en vue d'obtenir l'identité du titulaire d'une adresse IP d'un FAI étranger nécessite de trois à quatre mois pour aboutir. Les réponses fournies sont parfois imprécises, ou peu exploitables. Il arrive également que des réponses ne parviennent jamais. Les délais nécessaires à la mise en œuvre des nouveaux canaux de coopération et le fait que certains États ne participent pas à cet effort semblent indiquer que les collaborations informelles continueront de se développer, en marge des procédures et des instances établies par les accords internationaux.

## Analyse des responsabilités, obligations et initiatives des fournisseurs d'accès et de services en ligne

### Quelle responsabilité pour les acteurs de l'internet ?

L'article 9 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit, en transposition de la directive relative au commerce électronique du 8 juin 2000<sup>66</sup>, que « *les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* » soit, en premier lieu, les fournisseurs d'accès à l'internet (FAI), ne peuvent voir leur responsabilité civile ou pénale engagée que dans les cas où :

- ils sont à l'origine de la demande de transmission litigieuse ;
- ou ils sélectionnent ou modifient les contenus faisant l'objet de la transmission.

Le législateur affirme également que les prestataires techniques ne sont soumis à aucune obligation générale de surveillance des informations qu'ils transmettent ou qu'ils stockent, mais que le juge conserve la possibilité d'imposer une telle mesure de surveillance, ciblée et temporaire (art. 6-I-7°).

Selon les termes de l'article 6 de la loi, les prestataires assurant le stockage de données sur l'internet, soit les prestataires d'hébergement et les acteurs associés à leur statut, « *ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible* ».

Dans sa décision n° 2004-496 DC du 10 juin 2004, le Conseil constitutionnel a émis sur ce point une réserve d'interprétation estimant que : « *ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge* ». Selon une explication de la réserve d'interprétation livrée en conférence de presse, le caractère manifestement illicite d'un contenu désigne avant tout les messages incitant à la haine raciale et les images pédo-pornographiques<sup>67</sup>. Faisant écho aux dispositions prévues par les articles 808 et 809 du Nouveau Code de procédure civile, la loi rappelle enfin (art. 6-I-8°) que le juge peut prescrire aux hébergeurs ou, à défaut, aux fournisseurs d'accès, en référé ou sur requête, toute mesure propre à prévenir un dommage ou à faire cesser un dommage occasionné par un contenu en ligne, soit par exemple le retrait d'un contenu, ou le fait d'en rendre l'accès impossible.

En outre, la loi du 21 juin 2004 oblige les prestataires français d'hébergement, d'une part, à « *informer promptement les autorités publiques compétentes de toutes les*

---

66. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.

67. Estelle Dumout, Jérôme Thorel, « LCEN : le Conseil constitutionnel censure l'amendement Devedjian' », Paris, *ZDNet France*, 15 juin 2004.

*activités illicites mentionnées à l'alinéa précédent [ayant trait, notamment, à la pédopornographie] qui leur seraient signalées et qu'exerceraient les destinataires de leurs services» et, d'autre part, à «rendre publics les moyens qu'[ils] consacrent à la lutte contre ces activités illicites» (loi du 21 juin 2004, art. 6-I-7). Ces dispositions ont légalisé des pratiques largement répandues auprès des principaux prestataires d'hébergement français, qui informent les autorités et procèdent, lorsque les besoins de l'enquête le permettent, au retrait des contenus illicites.*

Enfin, les fournisseurs d'accès et d'hébergement «grand public» membres de l'AFA ont élaboré et souscrit ensemble le 14 juin 2004, sous l'égide du ministre délégué à l'Industrie, une charte clarifiant les modalités par lesquelles elles se conformeront aux objectifs assignés par la loi. Les fournisseurs grand public d'hébergement et de services internet «fixe» se sont par exemple engagés à faciliter le signalement de contenus illicites aux entreprises qui les hébergeraient, aux services de police (Internet-mineurs.gouv.fr) ou au point de signalement opéré par l'AFA (Pointdecontact.net) «*sur tous les espaces communautaires, objets de leurs services d'hébergement – tels que les forums de discussion, «chats», salons –, sur les pages d'accueil de leurs services, et le cas échéant, sur les pages de listes de réponses des moteurs de recherche intégrés à leurs portails, de manière à ce que ces usagers puissent effectuer ce signalement d'un seul 'clic', (art. 2) à «porter promptement à l'information des autorités de police compétentes [...] l'existence d'un contenu en ligne visé à l'article 1<sup>er</sup> [de nature pédopornographique ou raciste] [...], signalé par les internautes» et à «agir promptement pour retirer ces contenus ou pour en rendre l'accès impossible conformément aux dispositions légales en vigueur» (art. 3)<sup>68</sup>. Ce dernier engagement est de plus prévu par les clauses des conditions générales d'utilisation de la plupart des prestataires français d'hébergement qui, lorsqu'ils ne sont pas membres de l'AFA, ne se conforment toutefois pas tous aux engagements liés à la charte.*

### **L'exception à l'obligation d'effacement des données de connexion**

L'article L. 34-1 du Code des postes et des communications électroniques prévoit une obligation générale d'effacement des données de connexion et de trafic générées et stockées par les prestataires de services de communication en ligne. Il mentionne trois dérogations à cette obligation d'effacement pour les besoins de la facturation des prestations des opérateurs, pour les besoins de la sécurité de leurs réseaux, et pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

L'article L. 39-3 du Code des postes et des communications électroniques punit ainsi d'un an d'emprisonnement et de 75 000 euros d'amende et de peines d'interdictions d'exercer le fait, pour un opérateur ou l'un de ses agents, «*1° De ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications [...]» et «2° De ne pas procéder à la conservation des données techniques dans les conditions où cette conservation est exigée par la loi».*

---

68. «Charte des prestataires de services d'hébergement en ligne et d'accès à Internet en matière de lutte contre certains contenus spécifiques», 14 juin 2004 – [http://www.afa-france.com/actions/charte\\_internet.htm](http://www.afa-france.com/actions/charte_internet.htm).

L'article 6-II de la loi pour la confiance dans l'économie numérique du 21 juin 2004 renforce les moyens d'identifier les créateurs de tous types de contenus en disposant que les fournisseurs d'accès à des services de communication en ligne et les fournisseurs d'hébergement «*détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires*».

Les décrets d'application de ces dispositions, qui n'ont pas encore été adoptés mais ont fait l'objet de diverses consultations, doivent compléter le dispositif de conservation des données de connexion, essentiel à la recherche des auteurs d'infractions commises par le moyen des réseaux, et aujourd'hui diversement appliqué. La loi prévoit que ces décrets doivent fixer la durée de conservation des données de connexion et d'identification, ainsi que le spectre des données à conserver. Les modes de réquisition de ces données, les tarifs facturés par les opérateurs aux tribunaux pour chaque réquisition uniformisés et le mode de versement pourraient également être organisés par la voie réglementaire. Des groupes de travail communs à l'AFA et à la Direction générale de la police judiciaire ont été créés pour améliorer les procédures. Les enquêteurs espèrent beaucoup de la régularisation de ce dispositif, qui pourrait selon eux permettre un traitement plus rapide de leurs réquisitions auprès des intermédiaires techniques.

### **Certains prestataires de services prennent une part active à la lutte contre la pédo-pornographie sur l'internet**

Comme on l'a vu, la Commission européenne a favorisé le développement dans chaque État membre de *hotlines* de signalement de contenus illicites. Ces points de signalement sont opérés par les professionnels du secteur et par des associations de défense des droits de l'enfant. Depuis 1998, le réseau *InHope* a fédéré seize *hotlines* européennes, et quatre sites d'assistance associés basés en Australie, aux États-Unis, en Corée du Sud et à Taiwan<sup>69</sup>. Ce réseau facilite l'échange rapide d'informations entre les hotlines des pays où ont été signalés les contenus illicites, et les points de signalements des pays où ils sont localisés.

Sous réserve des particularités et de la législation locale de chaque hotline, lorsqu'un contenu en apparence pédo-pornographique est signalé à un point de contact du réseau *InHope*, et que ce dernier est compétent sur le territoire où est hébergé le contenu, le point de contact transfère le signalement au prestataire d'hébergement concerné ainsi qu'aux autorités nationales. Si le contenu est hébergé dans un pays représenté par un membre du réseau *InHope*, le point de contact le transmet à son homologue local. En France, l'Association des fournisseurs d'accès et de services internet (AFA) opère depuis 1997, à l'adresse [Pointdecontact.net](http://Pointdecontact.net), un site de signalement à l'usage des internautes français.

Outre la mise en place de points de contact, d'autres réalisations peuvent être observées à l'étranger, comme l'initiative du fournisseur d'accès *British Telecom* intitulée «*Cleanfeed*». En concertation avec certaines associations de protection de l'enfance

---

69. La liste des membres du réseau *InHope* est accessible à l'adresse : <http://www.inhope.org/english/about/members.htm>.

et le *Home Office*, le premier fournisseur d'accès à haut débit de Grande-Bretagne bloque depuis le 21 juin 2004 l'accès de ses abonnés à une liste de sites pédo-porno-graphiques compilée par l'association *Internet Watch Foundation*, par ailleurs point de signalement de contenus pédo-porno-graphiques membre du réseau *InHope*<sup>70</sup>. Plutôt que d'empêcher la diffusion et l'échange de matériel pédo-porno-graphique, cette mesure a manifestement pour objectif de prévenir l'exposition, accidentelle ou non, aux plus accessibles de ces contenus. Soutenue par le Premier ministre britannique, elle doit faire l'objet, à partir de septembre 2004, d'une série de consultations au cours duquel sera discuté le principe de l'extension d'une telle initiative à d'autres fournisseurs d'accès<sup>71</sup>. *British Telecom* a annoncé, trois semaines après la mise en place de son système, avoir bloqué plus de 230 000 tentatives d'accès aux sites proscrits, et jusqu'à 20 000 requêtes par jour. Contestés par l'association des fournisseurs d'accès britanniques (ISPA UK), ces chiffres comprennent les tentatives d'accès multiples à certains contenus par un même utilisateur et les tentatives d'accès involontaires aux contenus proscrits.

Un débat sur la pertinence et l'utilité de cette initiative a pris corps en Grande-Bretagne. La légitimité d'un organisme privé comme l'*Internet Watch Foundation* à établir des «listes noires» de sites a été mise en cause. Le blocage des sites risque de surcroît, selon ses détracteurs, de provoquer le blocage de ressources licites stockées par d'autres entités sur de mêmes serveurs mutualisés.

Semblable débat s'est tenu aux États-Unis, où une loi de l'État de Pennsylvanie (*Statute 7330*) obligeait depuis 2002 les fournisseurs d'accès à l'internet à bloquer l'accès aux sites pédo-porno-graphiques qui leur étaient notifiés par le procureur de l'État. La loi a été jugée contraire au Premier amendement de la Constitution des États-Unis le 10 septembre 2004 par un tribunal fédéral, au motif que le blocage de l'accès à 400 sites pédo-porno-graphique occasionnait le blocage collatéral de plus d'un million de sites licites<sup>72</sup>.

Enfin, la plupart des fournisseurs d'accès français, européens, et même américains, ne relaient pas sur leurs serveurs l'ensemble des groupes de discussion sur Usenet (*newsgroups*) existants, certains d'entre eux étant notoirement spécifiquement dédiés à l'échange de matériels pédo-porno-graphiques. Cette mesure technique, si elle empêche l'accès du plus grand nombre aux *newsgroups* dédiés à l'échange de contenus illicites, ne permet toutefois pas d'éradiquer ces derniers, et un véritable marché de l'accès à ces *newsgroups* a vu le jour sur certains serveurs qui les répliquent sciemment, sans plus de considérations légales ni éthiques.

---

70. Martin Bright, «BT puts block on child porn sites», *The Observer*, Manchester, 6 juin 2004.

71. Robert Jacques, «Blair backs BT child porn prevention filter», VNUNet.com, 22 juillet 2004.

72. Center for Democracy and Technology, American Civil Liberties Union, *Platagenet, Inc. vs. Gerald J. Pappert*. United States District Court for the Eastern District of Pennsylvania, 10 septembre 2004.



## **L'utilisation de l'internet aux fins de préparer une atteinte sexuelle sur un mineur**

Une majorité de jeunes Français ont aujourd'hui accès à l'internet, depuis leur domicile ou à l'école, notamment. Et à mesure que se développent leurs usages du réseau, il apparaît de plus en plus nettement que les usages *interactifs* de l'internet sont ceux qu'ils prisent le plus. L'internet ouvre ainsi des perspectives nouvelles et sans précédent de communication et de libre expression pour les millions de jeunes utilisateurs du réseau.

Tandis que se développent et se banalisent les pratiques sociales des jeunes sur l'internet (retrouver ses copains sur messagerie instantanée après l'école, s'en faire de nouveaux dans un salon de discussion généraliste ou thématique, s'inventer un personnage sur ces espaces publics ou dans un jeu en réseau...), des personnes mal intentionnées ont pu étendre ou déplacer sur le réseau leur recherche de faveurs sexuelles auprès d'enfants, et utiliser l'internet pour préparer une atteinte ou une agression sexuelle, ou encore un viol sur un mineur.

L'internet n'est évidemment pas à l'origine de tels comportements. Il n'est pas non plus démontré qu'évoluer dans ce nouvel espace social soit plus périlleux que dans d'autres environnements. Certaines particularités de l'internet et de ses usages, toutefois, sont susceptibles d'être exploitées par des personnes déterminées à abuser sexuellement d'enfants : les espaces publics de l'internet spécifiquement destinés aux jeunes peuvent par exemple servir de moyen de contacter ces derniers directement et immédiatement, un internaute peut aisément maquiller son identité réelle sur ces espaces publics, certaines informations personnelles imprudemment diffusées sur le réseau sont également susceptibles d'être employées aux fins d'approcher un enfant.

### Perception et réalités des risques associés à certains usages de l'internet

#### **Un objet d'inquiétude mal connu**

Plusieurs faits divers récents, en France et à l'étranger, témoignent des risques d'atteintes et agressions sexuelles ou de viols que peuvent encourir les mineurs à la suite de contacts établis sur l'internet. À défaut de veille systématique du phénomène, la mesure de ce dernier reste malaisée.

Dans ce domaine plus encore que dans celui de la diffusion de contenus pédo-pornographiques sur l'internet, on ne saurait produire d'éléments statistiques satisfaisants pour établir le panorama de l'utilisation de l'internet aux fins de commettre les faits d'atteinte ou d'agression sexuelle ou de viol sur mineurs. Rares sont les décisions de justice se rapportant à un viol ou une agression sexuelle sur un mineur résultant d'une mise en contact sur l'internet. Les statistiques du casier judiciaire font état, pour les années 1998 à 2002, d'une condamnation prononcée en 2000 sur le fondement du délit d'atteinte sexuelle sur un mineur de 15 ans par un majeur mis en contact avec la victime par un réseau de télécommunications. Les faits de corruption de mineur par une personne mise en contact avec la victime par un réseau de télécommunications ont donné lieu à deux condamnations en 2000 et 2001.

Le 23 novembre 2004, le tribunal de grande instance de Brest a condamné un homme de 47 ans à trois ans d'emprisonnement dont 18 mois de sursis avec mise à l'épreuve assorti de suivi médico-psychologique pour avoir commis une atteinte sexuelle sur une mineure de 13 ans rencontrée sur l'internet. D'après l'avocate de la famille, l'auteur de l'atteinte « menaçait de révéler à sa mère ce qu'elle faisait sur Internet. Elle s'est soumise à son agresseur, sans révolte, mais sans consentement<sup>73</sup>. » D'autres affaires seraient encore en cours d'instruction, et la presse se fait régulièrement l'écho de mises en examen de suspects d'agressions sexuelles, de viols ou encore de proxénétisme sur des mineurs rencontrés sur les espaces publics de l'internet. Selon M. Éric Freyssinet, le département INL de l'IRCGN a contribué au cours des 12 mois précédents à l'expertise de matériels informatiques liés à deux affaires de ce type<sup>74</sup>. D'autres affaires de cette nature étaient déjà connues et ont été jugées suite à l'utilisation du Minitel par l'agresseur. En 2001, par exemple, le tribunal correctionnel de Villefranche-sur-Saône condamnait un homme à quatre ans de prison ferme pour corruption de mineur et atteinte sexuelle avec circonstance aggravante pour avoir eu des relations sexuelles avec un adolescent de 13 ans, qui avait répondu à une annonce sur un réseau Minitel de rencontres.

En Grande-Bretagne, où ces questions font l'objet d'une attention particulière de la presse et des pouvoirs publics, la première affaire connue de cette nature remonte à 2000. Patrick G., un homme de 33 ans, a établi un contact avec une jeune fille de 12 ans, et entretenu avec elle des échanges réguliers durant deux mois, avant de lui faire subir des atteintes sexuelles. L'homme a été condamné en octobre 2000 à cinq ans de réclusion pour atteinte sexuelle sur mineur et possession de pédo-pornographie. À plusieurs reprises, la presse britannique s'est également fait l'écho d'affaires dans lesquelles un suspect appréhendé sur les lieux du rendez-vous qu'il avait fixé à un enfant après des contacts suivis sur l'internet n'avait pu aboutir, faute d'incrimination spécifique<sup>75</sup>. Le fait divers qui a vu, en 2003, une écolière britannique de 12 ans, Shevaun P., fuguer en compagnie d'un ancien soldat âgé de 31 ans rencontré sur l'internet, a fait le tour du monde.

En décembre 2003, le consultant de l'organisation NCH John Carr avait recensé dans la presse britannique 27 cas d'enfants ou de jeunes gens ayant rencontré un adulte suite à un contact en ligne, et ayant été victime d'un viol ou d'une atteinte sexuelle grave lors de cette rencontre. Les victimes identifiées étaient en majorité des filles âgées de 12 à 15 ans. L'étude de NCH affirme que, au-delà de ces cas connus, un grand nombre d'affaires ont pu n'être pas signalées aux autorités ou aux médias<sup>76</sup>.

Ces éléments épars ne reflètent pas toute la réalité du phénomène, et ne sauraient à eux seuls exprimer une tendance. Seule une étude des comportements de certains pédophiles et du détail des affaires en cours d'instruction et des condamnations

---

73. Frédéric Barille, « Le pédophile chassait sur Internet ». Brest, *Ouest-France*, mercredi 24 novembre 2004.

74. Éric Freyssinet, entretiens des 14 et 18 octobre 2004.

75. Will Gardner, *The Sexual Offences Bill: Progress and the Future*. Tackling Sexual Grooming conference, Londres, 29 septembre 2003.

76. John Carr, *Child abuse, child pornography and the Internet*, Londres, NCH, 2004. p.3.

prononcées permettrait d'élaborer enfin un constat précis de la réalité de ces risques. Il serait nécessaire, pour que de tels outils servent à guider l'action publique, que le rôle de l'internet dans la préparation des infractions soit systématiquement consigné par les enquêteurs et les tribunaux, même lorsque l'utilisation du réseau n'intervient qu'à titre accessoire ou n'entre pas directement dans la commission de l'infraction condamnée.

La mise en place d'un Observatoire national de l'enfance en danger (ONED) par la loi du 2 janvier 2004 relative à l'accueil et la protection de l'enfance est porteuse de promesses. L'Observatoire a pour missions l'amélioration de la connaissance du phénomène de maltraitance, le recueil et l'analyse des données chiffrées, l'identification des partenaires produisant des statistiques, la mise en cohérence des concepts et définitions, l'identification des secteurs non couverts par les producteurs de statistiques, des études et recherches concernant l'enfance maltraitée et la mise en cohérence des différentes informations. Il doit participer au réseau des Observatoires européens.

## **Les usages sociaux de l'internet et leurs risques**

On observe en France une forme de retard dans la connaissance des usages des jeunes utilisateurs de l'internet. L'agrégation d'éléments d'information rassemblés dans d'autres pays d'Europe permet toutefois de se forger une idée des pratiques des jeunes, et de leur exposition à des sollicitations de nature sexuelle sur l'internet susceptibles d'entrer dans la préparation d'atteintes sexuelles.

### **L'internet comme terrain d'expérimentation sociale**

Selon l'enquête du CREDOC sur «la diffusion des technologies de l'information dans la société française», publiée en novembre 2003, 72 % des 12-17 ans disposaient en juin 2003 d'un accès à l'internet sur leurs lieux d'étude ou de travail, tandis que 40 % étaient équipés à domicile d'une connexion à l'internet, dont 16 % à haut débit.

55 % des 12-17 ans usagers de l'internet considèrent que le réseau est «un bon outil pour se faire des amis et entretenir des relations». Ainsi la messagerie instantanée (48 % des 12-17 ans connectés), l'échange de fichiers sur les réseaux *peer-to-peer* (P2P) (31 %) et les jeux en réseau (35 %, 15 % des 12-17 ans n'ayant encore jamais joué en réseau ayant l'intention de le faire dans l'année) figurent-ils parmi les principaux usages de l'internet par les jeunes<sup>77</sup>.

Les chercheurs du Réseau Éducation-Médias canadien considèrent également que la communication par courrier électronique, chat, messagerie instantanée fait partie des usages favoris des jeunes sur l'internet, et s'intègre désormais à la vie sociale de nombreux jeunes internautes. Ils apportent des précisions intéressantes sur ces pratiques, issues de séries d'entretiens avec de jeunes utilisateurs: au quotidien, et entre amis, la messagerie instantanée semble avoir la préférence des jeunes internautes; le courrier électronique, plus formel, sert plus volontiers à communiquer avec un

---

77. Régis Bigot, «La diffusion des technologies de l'information dans la société française», Enquête *Conditions de vie et Aspirations des Français*, CREDOC, Paris, juin 2003.

enseignant ou un parent éloigné; le chat, enfin, constitue un véritable terrain d'expérimentation et d'exploration sociale. Les chercheurs nous enseignent que de nombreux jeunes Canadiens explorent ainsi les interactions sociales en testant, sous le couvert de plusieurs avatars, différents comportements, attitudes et pratiques<sup>78</sup>.

En ligne comme hors ligne, les relations sociales comportent des « situations limites » et des risques inhérents aux intentions d'autres acteurs, qu'ils soient eux-mêmes mineurs ou bien adultes.

### **Sollicitations en ligne et rencontres physiques**

Une enquête réalisée dans le cadre du programme SAFT (*Safety, Awareness, Facts and Tools*), financée par l'Union européenne et portant sur un large échantillon d'internautes âgés de 9 à 16 ans du Danemark, de Suède, d'Islande, de Norvège et d'Irlande, indiquait en mai 2003 qu'entre 19 % (Irlande) et 39 % (Norvège, Danemark) des enfants fréquentant les chats s'étaient vu proposer une rencontre physique. Entre 12 % (Irlande) et 26 % (Suède) du même échantillon ont rencontré une personne avec laquelle ils avaient établi un premier contact sur l'internet.

31 % des 1511 jeunes internautes Britanniques âgés de 9 à 19 ans interrogés dans le cadre de l'enquête *UK Children Go Online*, coordonnée par l'*Economic & Social Research Council (ESRC)*<sup>79</sup>, ont reçu en ligne des sollicitations sexuelles non désirées dans le courant de l'année. L'enquête met en évidence le fait que 8 % des jeunes se connectant au moins une fois par semaine ont rencontré « hors ligne » une personne connue sur l'internet. Parmi ces derniers, 5 % n'avaient averti personne de leur intention de rencontrer leur correspondant. L'étude rapporte enfin que 48 % des jeunes Britanniques interrogés craignent d'être « *contactés par des personnes dangereuses* ».

Une vaste enquête entreprise aux États-Unis en 2000 par le *National Center for Missing and Exploited Kids (NCMEC)* indiquait que 19 % des membres d'un panel de 1501 utilisateurs de l'internet âgés de 10 à 17 ans avaient reçu des « sollicitations sexuelles » non désirées dans le courant de l'année, ces « sollicitations sexuelles » recouvrant un ensemble très large de réalités, soit des situations où quelqu'un tente de convaincre l'enfant de parler de sexe alors qu'il ne le souhaite pas, ou pose des questions intimes auxquelles l'enfant ne souhaite pas répondre, des situations où des personnes demandent à l'enfant de se livrer à des activités sexuelles auxquelles il ne souhaite pas s'adonner, des situations où des amitiés liées sur l'internet avec des adultes ont comporté des « ouvertures » sexuelles, et des invitations à s'enfuir émanant de correspondants sur l'internet. 3 % des enfants interrogés avaient

---

78. Réseau Education-médias, *Young Canadians in a Wired World – Phase II*. Focus Groups. Réseau Education-Médias, Ottawa, février 2004.

79. Sonia Livingstone, Magdalena Bober, *UK Children Go Online. Surveying the experiences of young people and their parents*. Economic & Social Research Council, Londres, Juillet 2004.

fait l'objet d'une sollicitation «agressive», impliquant une tentative de contact en personne, par téléphone, ou par courrier traditionnel<sup>80</sup>.

Les sollicitations de nature sexuelle reçues en ligne par ces enfants n'émanent naturellement pas toutes d'adultes conscients de solliciter un mineur, mais fréquemment d'autres jeunes utilisateurs, qui accèdent de plus en plus précocement à des registres de langage et de relations fortement sexualisés. Les enfants employant de plus en plus souvent, et plus volontiers encore sous couvert de pseudonymat, certains codes que l'on croyait réservés aux adultes, les risques propres aux mises en contact sur l'internet sont rendus difficiles à apprécier, dans la mesure il est parfois très difficile de distinguer le langage et les intentions d'un autre jeune usager de celles d'un adulte mal intentionné. Dans 48 % des cas de «sollicitations sexuelles» rapportées dans l'enquête du NCMEC, l'initiateur de la sollicitation paraissait être âgé de moins de 18 ans. Il semblait être un adulte, le plus souvent âgé de 18 à 25 ans, dans 24 % des cas. Les enfants interrogés ne pouvaient déterminer l'âge de leur correspondant dans 27 % des cas<sup>81</sup>. Comme le note la sociologue Céline Metton, «*Internet est [...] devenu un accompagnateur privilégié des premiers émois amoureux*», où «*les «accroches» souvent très crues des garçons effraient les filles*»<sup>82</sup>.» De même, le professeur Philippe Jeammet, psychiatre, note que «*le pseudonymat permet aux jeunes de s'approcher de comportements et de matériels qui leur sont défendus, avec le risque de se faire piéger en oubliant leurs prévenances. C'est ainsi que certains jeunes, garçons avant tout, n'hésitent pas à représenter leur nudité devant leur webcam*»<sup>83</sup>.

Malgré l'apparence fort «libérée» des échanges en direct entre jeunes sur l'internet, ces derniers font toutefois le plus souvent preuve d'une prudente réserve. Céline Metton précise que «*lorsque le contact est bon, les dialogues sur le chat font office de prénégociation à une rencontre de visu. Les deux interlocuteurs s'échangent leurs coordonnées téléphoniques, et se fixent ensuite par téléphone un rendez-vous dans un lieu public. Le téléphone portable est le prolongement naturel du chat: il occupe une place centrale dans le processus de rencontre. Il permet d'abord une certaine protection et maintient la relation hors du contrôle parental*»<sup>84</sup>.

En France, le protocole d'accord signé le 4 février 2004 entre l'institution du Défenseur des enfants et le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche, qui s'intègre dans la démarche de sécurisation des usages de l'internet entreprise par le ministère, crée la possibilité que le Défenseur «*soit chargé, en relation étroite avec les académies, de faire une typologie des agressions le plus*

---

80. David Finkelhor, Kimberly Mitchell, Janis Wolak, *Online Victimization: A Report on the Nation's Youth*, Washington DC, National Center for Missing & Exploited Children (NCMEC), juin 2000. David Finkelhor, Kimberly Mitchell, Janis Wolak, «*Hightlights of the Youth Internet Safety Survey*», *OJJDP Fact Sheet*, Washington DC, U.S. Department of Justice, Office of Justice Programs, n° 4, mars 2001.

81. David Finkelhor, Kimberly Mitchell, Janis Wolak, *Online Victimization: A Report on the Nation's Youth*, op. cit.

82. Céline Metton, «*Ils s'aiment par Internet*», in *Informations sociales*, n° 111, novembre 2003. Paris, Caisse nationale des allocations familiales. pp.32-41.

83. Philippe Jeammet, audition du 6 juillet 2004.

84. *Ibid.*

fréquemment répertoriées» au cours de l'utilisation du réseau à l'école. De cette veille pourraient émerger de nouveaux indicateurs des risques ressentis par les jeunes utilisateurs de l'internet à l'école.

### **Profil de victimes et méthodes de « prédateurs »**

Psychiatres, enquêteurs, sociologues, ainsi que l'ensemble des observateurs des pratiques sociales des jeunes sur l'internet, notent que les adolescents constituent, parmi les mineurs, le groupe le plus exposé aux sollicitations de nature sexuelle de la part d'agresseurs potentiels sur le réseau. Les garçons, «*sexuellement curieux et inexpérimentés et un peu rebelles*», sont d'après l'auteur d'un rapport du *National Center for Missing and Exploited Children* (NCMEC) et du ministère de la Justice américain, les plus susceptibles d'être les cibles d'adultes cherchant à obtenir les faveurs sexuelles d'enfants. Ce même auteur considère que les «*enfants de familles dysfonctionnelles et de familles où l'on communique peu encourrent des risques significatifs de séduction*<sup>85</sup>.» Le Professeur Jeammet confirme que les enfants les plus vulnérables sont, sur l'internet comme hors ligne, les plus menacés: si les enfants éprouvant des carences affectives importantes sont la plupart du temps très méfiants à l'encontre des adultes, ils font également preuve d'une grande candeur à l'égard des personnes qui gagnent leur confiance<sup>86</sup>.

L'internet offre aux agresseurs potentiels de nouveaux moyens d'identifier une future victime, puis de tisser avec elle des liens et une intimité qui pourront résister, le cas échéant, à la révélation de l'âge véritable de l'adulte. John Carr décrit, pour l'organisation NCH, le mode opératoire typique d'un «*prédateur*» sur l'internet comme un processus méticuleux au cours duquel un pédophile va aborder un mineur dans un espace public de discussion en se présentant comme de quelques années plus jeunes que son correspondant, isoler l'enfant dans un salon de discussion particulier, puis gagner sa confiance au cours d'une relation dont il insistera pour qu'elle reste secrète, et qui pourra s'établir suivant plusieurs modes de communication: courriers électroniques, messagerie instantanée puis, parfois, téléphone et téléphone mobile<sup>87</sup>. De la même façon, l'auteur du rapport du NCMEC décrit un processus s'inscrivant dans la durée. Il précise que les agresseurs sexuels déterminés à établir des relations sexuelles avec des enfants développent fréquemment des aptitudes particulières à identifier les enfants les plus vulnérables et à s'identifier à leurs victimes: ils connaissent le plus souvent les derniers jeux vidéo, jouets, films, musiques ou sites *web* susceptibles d'intéresser les jeunes dont ils cherchent à gagner la confiance; ils savent également séduire un enfant en dispensant à ce dernier attention, affection et cadeaux<sup>88</sup>.

---

85. Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis*. Washington DC, National Center for Missing & Exploited Children, Office of Juvenile Justice and Delinquency Prevention – U.S. Department of Justice, septembre 2001.

86. Philippe Jeammet, audition du 6 juillet 2004.

87. John Carr, *Child abuse, child pornography and the Internet*, op. cit.

88. Kenneth V. Lanning, *Child Molesters: A Behavioral Analysis*, op. cit.

## La question de la diffusion de données personnelles d'enfants

Si le risque de contacts en ligne entre des enfants et des agresseurs potentiels s'exprime de manière particulièrement sensible sur les espaces interactifs (*chats*, notamment) car les protagonistes sont mis instantanément en contact, la publication sur le *web* de certaines informations personnelles peut, à l'évidence, être un facteur de risque en facilitant le rapprochement d'adultes et de mineurs.

Des associations de défense des droits de l'enfant expriment ainsi leurs inquiétudes au sujet de la diffusion de telles données personnelles sur des sites associatifs ou scolaires, par exemple, ou encore de services dédiés à faciliter les rencontres entre jeunes personnes. M. Alain Boulay, président de l'Association d'aide aux parents d'enfants victimes (APEV) recommande une plus grande prudence des organismes publiant les photographies, et parfois certaines informations nominatives précises sur les enfants (écoles, clubs sportifs), et appelle de ses vœux la diffusion d'une circulaire ministérielle sur le sujet<sup>89</sup>. Le rappel des dispositions légales punissant la fixation, l'enregistrement et la transmission de l'image d'une personne sans son consentement ou celui de ses parents si elle est mineure, pourrait conduire de nombreux sites à régulariser les informations qu'ils rendent accessibles.

En Grande-Bretagne, le retrait des données nominatives relatives aux mineurs sur les sites *web* des écoles fait partie des recommandations aux établissements dans le cadre du plan d'équipement *National grid for learning (NGFL)* du secrétariat à l'Éducation<sup>90</sup>. Et selon la *task force* «Protection des mineurs sur l'internet» du *Home office* britannique, «*les profils et les annuaires d'utilisateurs [de services de chat] peuvent permettre à une personne déterminée à abuser d'un mineur d'accéder à des informations très utiles, ainsi que d'établir un premier contact*<sup>91</sup>.» Diverses recommandations relatives à la préservation de l'anonymat des jeunes utilisateurs de l'internet ont été formulées parmi les «modèles de bonnes pratiques» élaborées en janvier 2003 par la *task force* «Protection des mineurs sur l'internet» du *Home office* britannique, qui comprend des représentants des pouvoirs publics, des acteurs économiques et des associations. Le ministère de l'Intérieur britannique recommande par exemple que «*les sites web procèdent avec prudence lorsqu'ils incluent des photographies, des coordonnées ou d'autres détails pouvant servir à identifier ou à contacter des enfants.*» Le *Home office* recommande également que les enfants soient encouragés à ne pas déclarer leurs adresse et numéro de téléphone lorsqu'ils remplissent leur «profil public» d'utilisateur d'un service en ligne, et qu'il leur soit possible de masquer un maximum d'informations<sup>92</sup>.

---

89. Alain Boulay, audition du 1<sup>er</sup> juin 2004.

90. Voir: <http://safety.ngfl.gov.uk/>

91. Home Office task force on child protection on the internet, *Good practice models and guidance for the internet industry on: chat services, instant messaging (IM), web based services*. Londres, Home Office Communication Directorate, janvier 2003.

92. Voir: <http://www.homeoffice.gov.uk/crime/internetcrime/taskforce.html>. Le sous-groupe responsable de l'élaboration de ces recommandations compte des représentants des principales sociétés et associations professionnelles (AOL, BBC Online, ICSTIS, ISPA, LINX, Microsoft, Yahoo!, Surf Control...) et associations de protection des enfants (Childline, NCH, Childnet International...).

## La relative ignorance des parents

Différents indicateurs suggèrent qu'une minorité de parents sont aujourd'hui bien informés sur les risques qui peuvent être associés à certains usages de l'internet et aux moyens de les prévenir.

Un sondage «Eurobaromètre» de mars 2004, réalisé en novembre-décembre 2003 auprès de 16000 citoyens de 15 États membres de l'Union, indique que 55 % des parents français de jeunes utilisateurs de l'internet souhaitent plus d'informations sur les moyens de sécuriser l'utilisation de l'internet par leurs enfants. 49 % interdisent aux enfants de transmettre sur l'internet des informations personnelles les concernant. De même, 38 % des parents utilisant régulièrement l'internet demandaient à leurs enfants de les informer de toute découverte déplaisante qu'ils pourraient faire en ligne. Et tandis que 39 % interdisent à leurs enfants de rencontrer quiconque dont ils auraient fait la connaissance sur l'internet, 32 % interdisent même à leurs enfants de fréquenter les *chat rooms* ou d'y communiquer avec des étrangers<sup>93</sup>.

D'autres études mettent en évidence le fait que les parents n'ont pas encore pris, dans leur majorité, la mesure des risques pouvant être associés à certains usages de l'internet. Les résultats de la toute récente étude conduite sous l'égide de l'*Economic & Social Research Council* en Grande-Bretagne<sup>94</sup> indiquent ainsi que si 31 % des jeunes utilisateurs de l'internet 9 à 19 ans interrogés reconnaissent avoir reçu des commentaires non désirés de nature sexuelle, 7 % seulement des parents pensent qu'un tel événement s'est produit. De même, alors que 5 % seulement des parents interrogés pensent que leurs enfants ont transmis des informations personnelles sur l'internet, près de la moitié (46 %) des jeunes interrogés déclarent avoir déjà transmis à un correspondant rencontré en ligne leur nom complet, leur âge, leur adresse électronique, leur numéro de téléphone, ou les coordonnées de leur école.

## L'action des parties concernées et ses limites

Méconnu, difficile à quantifier, le phénomène de l'utilisation de l'internet par des personnes mal intentionnées aux fins de commettre des atteintes sexuelles sur des mineurs fait également l'objet d'assez peu de mesures spécifiques de la part des acteurs engagés dans la protection de l'enfance sur le réseau.

## Le cadre juridique et procédural en France et à l'étranger

### **Le droit français n'incrimine pas spécifiquement le fait de rechercher les faveurs sexuelles d'un mineur**

Il n'existe pas, en droit français, d'infraction décrivant spécifiquement le fait de rechercher les faveurs sexuelles de mineurs, en ligne ou hors ligne, ou encore d'aller

---

93. European Union Opinion Research Group (EEIG), *Illegal and harmful content on the Internet*, Special Eurobarometer 203/Wave 60.2, Bruxelles, Commission Européenne, mars 2004.

94. Sonia Livingstone, Magdalena Bober, *UK Children Go Online*, op. cit.



à la rencontre d'un mineur dans l'intention de commettre sur lui une atteinte ou agression sexuelle ou un viol.

Seuls sont susceptibles d'être poursuivies l'agression sexuelle ou la tentative d'agression sexuelle (art. 222-27 à 222-31 du Code pénal), le viol ou la tentative de viol (art. 222-23 et 222-24 du Code pénal) sur mineurs, ainsi que l'atteinte sexuelle « sans contrainte, menace ni surprise » sur mineur de 15 ans (art. 227-25 et 227-26 du Code pénal) et les faits de proxénétisme (art. 225-7 et 225-7-1 du Code pénal). Le fait que le mineur victime ait été mis en contact avec l'auteur des faits ou que l'infraction ait été réalisée grâce à l'utilisation d'un réseau de télécommunications aggrave depuis la loi n° 98-468 du 17 juin 1998 les peines associées à ces crimes et délits (art. 222-24 al. 8, 222-28 al. 6, 225-7 al. 10 et 227-26 al. 4 du Code pénal). Les incriminations existantes supposent donc que l'acte délictueux soit consommé ou que soit constaté un commencement d'exécution, soit « *des actes devant avoir pour conséquence directe et immédiate de consommer le crime, celui-ci étant ainsi entré dans la période d'exécution*<sup>95</sup>. »

L'article 227-22 du Code pénal punit le fait de « *favoriser ou de tenter de favoriser la corruption d'un mineur* » soit, comme l'écrivait l'ancien Code pénal, d'exciter un mineur à la débauche. C'est pour lutter contre l'utilisation par certaines personnes des « *moyens modernes de communication, qui constituent d'indéniables progrès techniques, pour prendre dans leurs filets leurs futures victimes*<sup>96</sup> », que la loi du 17 juin 1998 a porté les peines punissant ce délit à un maximum de sept ans d'emprisonnement et 100 000 euros d'amende « *lorsque le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunications* ».

La jurisprudence pose toutefois quelques limites qui rendent délicat le recours à cet article pour punir la recherche de faveurs sexuelles auprès d'un enfant. La Cour de cassation a ainsi jugé que « *l'excitation de mineurs à la débauche n'est pénalement punissable que si l'auteur des faits a eu en vue la perversion de la jeunesse, et non pas seulement la satisfaction de ses propres passions*<sup>97</sup> ». La Chambre criminelle a toutefois également considéré que « *l'envoi de correspondances érotiques et de dessins pornographiques à un mineur*<sup>98</sup> » et le fait de pousser un mineur « *à un ou plusieurs actes d'immoralité par des conseils persistants et précis ou par des provocations réitérées*<sup>99</sup> » sont susceptibles d'être incriminés au titre de l'article 227-22 du Code pénal. Dans certaines circonstances, l'article 227-22 du Code pénal semble ainsi pouvoir fonder des enquêteurs informés de contacts répétés entre un mineur et un adulte à appréhender ce dernier avant qu'il ne commette l'une des atteintes décrites plus haut.

---

95. Cass. crim. 25 oct. 1962 : *Bull. crim.* n° 292 (Lacour) et n° 292 (Benamar et Schieb).

96. Elizabeth Guigou, garde des Sceaux, ministre de la Justice, discussion du projet de loi au Sénat le 28 octobre 1997 – [http://www.senat.fr/seances/s199710/s19971028/s19971028\\_mono.html](http://www.senat.fr/seances/s199710/s19971028/s19971028_mono.html).

97. Cass. crim. 14 nov. 1990 : *Dr. Pénal* 1991 105.

98. Cass. crim. 25 janv. 1983 : *Bull. crim.* N° 29 ; *RS crim.* 1983. 668, obs. Levasseur.

99. CA Dijon, 15 janv. 1954 : *Gaz. Pal.* 1954. 1. 224.

En Grande-Bretagne, le *Sexual Offence Act* de 2003<sup>100</sup> punit spécifiquement d'un maximum de dix ans d'emprisonnement le fait, pour un adulte, de rencontrer ou d'aller à la rencontre d'un enfant de moins de 16 ans dans l'intention d'entretenir avec lui des relations sexuelles, et après avoir communiqué avec lui par quelque moyen que ce soit à au moins deux reprises. À l'évidence, l'intention des personnes susceptibles d'être poursuivies sur ce fondement sera difficile à établir. Il semble toutefois que la volonté du législateur britannique ait été de créer avant tout un outil de dissuasion à l'encontre d'agresseurs potentiels. On note que, soucieux de ne pas incriminer une simple intention, le législateur britannique a choisi de retenir pour élément matériel de l'infraction le fait de rencontrer ou d'aller à la rencontre du mineur.

La législation fédérale américaine rend également possible le fait d'appréhender et de poursuivre une personne avant qu'elle ne commette une infraction sexuelle sur un mineur. Ainsi quiconque convainc ou essaye de convaincre, de persuader ou de contraindre, par courrier ou tout autre moyen, un mineur de moins de 18 ans à participer à une activité sexuelle s'expose à une amende et jusqu'à quinze années de réclusion<sup>101</sup>. Certaines juridictions locales américaines prévoient spécifiquement l'utilisation d'un ordinateur pour solliciter un mineur. Cette disposition est à rapprocher de la conduite d'opérations de police «sous couverture» dans les *chat rooms*, où des enquêteurs disposent des moyens légaux de se faire passer pour mineurs et de constater des infractions. D'après une étude américaine, le constat de telles sollicitations de mineurs par des enquêteurs «sous couverture» a donné lieu, entre juillet 2001 et juillet 2002, à 644 arrestations<sup>102</sup>.

Les coopérations qui se sont développées entre pays anglo-saxons en matière de lutte contre la cybercriminalité doivent aboutir à la création prochaine d'équipes de surveillance issues des équipes spécialisées des autorités britanniques, américaines, canadiennes et australiennes, qui parcourront les salons de discussion du monde entier et établiront une présence visible des autorités sur ces espaces<sup>103</sup>.

### **Procédés et limites de l'action des services d'enquête en France**

La nouveauté des situations auxquelles sont confrontés les enquêteurs et l'absence d'infraction décrivant spécifiquement le fait de rechercher les faveurs sexuelles de mineurs en ligne ou hors ligne amènent les services d'enquête à explorer des méthodes nouvelles de surveillance des espaces de discussion en ligne, et à souhaiter que le cadre de certaines procédures soit élargi. La création de nouvelles

---

100. *Sexual Offence Act* 2003, Section 15.

101. «*b) Whoever, using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title, imprisoned not more than 15 years, or both*» -18 U.S.C. 2422: Cœrcion and Enticement.

102. Janis Wolak, Kimberly Mitchell, David Finkelhor, *Internet Sex Crimes Against Minors: The Response of Law Enforcement*, Washington DC, National Center for Missing & Exploited Children (NCMEC), novembre 2003.

103. «Cyber-cops to patrol Internet chatrooms», *CNN.com*, 9 juin 2004.

infractions et l'extension de procédures particulières constituent des actions de très large portée dont les bénéfices attendus doivent toutefois être mesurés et confrontés à la réalité des phénomènes qu'elles entendent combattre et aux risques qu'elles feraient peser sur les libertés publiques.

Certains services d'enquête français entreprennent de surveiller les espaces de discussion de l'internet où des enquêteurs, sous des identités fictives, sont à même d'observer le comportement d'adultes présumés en quête de faveurs sexuelles auprès de mineurs. On pourra opposer que cette méthode s'apparente à un procédé de provocation dès lors que l'enquêteur interagit directement avec un suspect.

Une enquête préliminaire peut être diligentée sous le contrôle du parquet sur le fondement des articles 227-24 (diffusion d'un message à caractère pornographique lorsque ce message est susceptible d'être perçu par un mineur) ou 227-22 (corruption de mineurs) du Code pénal, lorsqu'un mineur victime de telles sollicitations est connu. Les protagonistes pourront être identifiés par voie de réquisitions au cours de cette enquête préliminaire. L'infraction pourra être requalifiée au besoin si l'enquête apporte des éléments tendant à indiquer qu'une atteinte, une agression ou un viol a été commis sur une personne mineure.

Désireux d'intervenir en amont des faits, et convaincus que l'internet peut servir de vecteur de rencontres et de contacts entre des mineurs et des adultes déterminés à recueillir de ces derniers des faveurs sexuelles, certains enquêteurs souhaitent que puisse être incriminé spécifiquement le fait, pour un majeur, d'émettre une proposition de nature sexuelle à destination d'une personne connue comme mineure, l'utilisation de l'internet pouvant constituer une circonstance aggravante de la sanction prévue.

Certains enquêteurs souhaitent également que la procédure particulière en matière d'interceptions prévue par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, puisse être étendue à la recherche d'infractions sexuelles à l'encontre de mineurs, et permette l'accès, au cours de l'enquête préliminaire, aux comptes de courrier électronique et la surveillance de l'activité dans les salons de discussion privés de personnes sur lesquelles reposent de fortes présomptions. L'article 706-95 du Code de procédure pénale prévoit que *« si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application de l'article 706-73 l'exigent [crimes et délits commis en bande organisée, notamment relatifs à la traite des êtres humains, ne comprenant pas spécifiquement les atteintes aux mineurs et les infractions relatives à la pédo-pornographie], le juge des libertés et de la détention du tribunal de grande instance peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications selon les modalités prévues par les articles 100, deuxième alinéa, 100-1 et 100-3 à 100-7, pour une durée maximum de quinze jours, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention »*.

## Rappel des responsabilités et initiatives des fournisseurs de services

### Le régime juridique applicable aux intermédiaires techniques et aux exploitants de services interactifs

Le 14 octobre 2003, la direction du portail MSN décidait de fermer tous ses espaces de discussion gratuits dans le monde, sauf en Amérique du Nord et au Japon, où ces services sont devenus payants. Malgré la surveillance opérée par des employés et des bénévoles sur les *chats* du portail, les *chats* comportaient, selon Grégory Salinger, directeur de MSN France, «*des risques très importants liés à la pédophilie*»<sup>104</sup>, entre autres abus. Cet événement invite à aborder l'examen du régime légal de responsabilité et des initiatives protectrices des éditeurs de services en ligne et des opérateurs de communications électroniques.

Comme on l'a rappelé plus haut<sup>105</sup>, la loi du 21 juin 2004 pour la confiance dans l'économie numérique prévoit un principe général d'exonération de la responsabilité civile et pénale à raison des contenus accessibles sur les réseaux pour les «*personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne*». Le législateur a également affirmé que les prestataires techniques ne sont soumis à aucune obligation générale de surveillance des informations qu'ils transmettent ou qu'ils stockent.

Les prestataires assurant le stockage de données sur l'internet «*ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible*».

### L'obligation de conservation des données d'identification

Comme il a été exposé plus tôt, les fournisseurs d'accès et les fournisseurs d'hébergement sont tenus de conserver certaines données permettant l'identification des utilisateurs de leurs services dans le cadre d'une enquête judiciaire<sup>106</sup>.

Le statut des fournisseurs de services de communication synchrone (*chats*) et asynchrone (*forums*) mérite d'être précisé. En tant que fournisseurs de services de la société de l'information permettant à des tiers de communiquer entre eux, ils sont susceptibles de relever de la définition de l'article 6-I/-2 de la loi du 21 juin 2004 sur la confiance dans l'économie numérique, et d'être ainsi contraints de détenir et de conserver les données d'identification visées par l'article 6-II.

---

104. Arnaud Devillard, «MSN ferme ses salons pour cause de dérive pornographique», *01Net*, 24 septembre 2003.

105. Voir «Responsabilité, obligations et initiatives des fournisseurs d'accès et de services en ligne.»

106. Voir «Analyse des responsabilités, obligations et initiatives des fournisseurs d'accès et de services en ligne.»

## **Les bonnes pratiques des fournisseurs de services**

Certains exploitants d'espaces publics de discussion synchrones (*chats*) ou asynchrones (forums, par exemple) affichent, dans ces espaces, des messages destinés à mettre en garde leurs jeunes utilisateurs contre les intentions de certains adultes ou encore un bouton permettant d'alerter les animateurs du service d'un comportement ou d'un contenu déplacés. D'autres entretiennent des équipes de modération ou de surveillance de ces espaces, où des surveillants le plus souvent bénévoles ont pour mission d'assister les utilisateurs et de surveiller les espaces de discussion en semonçant ou « bannissant » au besoin certains usagers peu respectueux de la loi ou des chartes d'utilisation associées aux services.

Les fournisseurs d'accès et d'hébergement « grand public » membres de l'Association des fournisseurs d'accès et de services internet (AFA) se sont engagés par une charte, le 14 juin 2004, à établir des liens vers « *un formulaire de signalement d'abus* » permettant aux utilisateurs « *de signaler directement au prestataire du service d'hébergement concerné, ou au Point de contact de la profession accessible à l'adresse [www.pointdecontact.net](http://www.pointdecontact.net), ou aux autorités publiques dûment habilitées, tout contenu en ligne visé par [ladite] Charte* ». Ces liens ont vocation à être placés « *sur tous les espaces communautaires, objets de leurs services d'hébergement – tels que les forums de discussion, « chats », salons –, sur les pages d'accueil de leurs services, et le cas échéant, sur les pages de listes de réponses des moteurs de recherche intégrés à leurs portails, de manière à ce que ces usagers puissent effectuer ce signalement d'un seul « clic »* » (art. 2). Le principe d'une uniformisation des moyens de signalements, identifiés au besoin sur tous les espaces publics de discussion par une signalétique particulière et accompagnés d'explications visant à sensibiliser les enfants aux spécificités et aux règles des usages de l'internet, paraît une initiative prometteuse. Elle s'ajoute au dispositif d'information spécifique à la protection de l'enfance adopté par l'AFA, tendant à généraliser un lien « Protection de l'enfance » sur les pages d'accueil des sites de ses membres.

De nombreux espaces interactifs de l'internet font l'objet d'une veille par des modérateurs chargés, le plus souvent, de rappeler les règles de courtoisie aux utilisateurs de l'espace (*chat* ou forum). Des applications fort populaires de l'internet, toutefois, ne peuvent être modérées ou surveillées. Ainsi, la grande majorité des *chats* comportent une partie publique, parfois surveillée, mais autorisent aussi une forme de communication de personne à personne échappant à la surveillance des modérateurs et des autorités. De même les dialogues échangés par l'intermédiaire des outils de messagerie instantanée ne sont pas susceptibles de surveillance hors du cadre des interceptions de correspondances.

## **Initiatives publiques et privées de sensibilisation des jeunes utilisateurs de l'internet, des éducateurs et des familles**

Diverses initiatives d'origines publiques ou privées entreprennent de sensibiliser les jeunes utilisateurs de l'internet aux risques qui peuvent être associés à certaines pratiques.

### **Les attentes des utilisateurs**

Le sondage « Eurobaromètre » de mars 2004 consacré aux contenus illégaux et préjudiciables sur l'internet nous renseigne sur les attentes des parents de jeunes utilisateurs de l'internet en matière de sensibilisation au bon usage de l'internet. 48 % des parents interrogés dans les quinze pays membres de l'Union européenne entre novembre et décembre 2003 et dont les enfants utilisent l'internet souhaitent plus d'information sur les moyens de protéger leurs enfants des contenus illégaux et préjudiciables sur le réseau. En France, 55 % des parents de jeunes utilisateurs de l'internet souhaitent plus d'informations.

Pour 47 % des parents dont les enfants utilisent l'internet, l'école est la première source dont ils attendent que vienne l'information sur les moyens de sécuriser les usages de l'internet, avant les médias (32 % : télévision, radio, journaux), puis les fournisseurs de services d'accès à l'internet et de télécommunications (28 %) et le gouvernement ou les autorités locales (20 %).

Il semble également que les parents interrogés préféreraient recevoir cette information par les canaux traditionnels plutôt que devoir la rechercher : à la télévision (43 %), par courrier (43 %) et, dans une moindre mesure, par les journaux (31 %). Moins de 15 % des parents souhaitant disposer de plus d'information sur les moyens de sécuriser les usages de l'internet préféreraient trouver cette information sur un site *web*<sup>107</sup>.

### **La diversité des initiatives de sensibilisation en Europe et dans le monde**

On note, parmi les actions de sensibilisation et d'éducation à l'internet et à ses dangers potentiels, deux principaux types d'approches :

– l'énoncé de recommandations établies par des experts, destinées à sensibiliser les adultes ou les jeunes, et à leur indiquer les comportements jugés adéquats face à des situations potentiellement dangereuses sur l'internet ;

– des démarches d'éducation aux médias, souvent reprises en Europe sous le terme « *Internet literacy* », à visée plutôt préventive, destinées à faire mieux connaître Internet aux adultes et aux jeunes (ses caractéristiques, ses fonctionnements, ses richesses, ses limites) de manière à les rendre autonomes et responsables dans leurs choix face à l'internet. Cette approche, plus exigeante et agissant sur le plus long terme, part des connaissances et des comportements réels des adultes et des jeunes et permet notamment de prendre en compte les évolutions rapides des technologies.

### **Incitations et financements européens**

Le rapport d'évaluation concernant l'application de la Recommandation du Conseil de l'Europe du 24 septembre 1998 sur la protection des mineurs et de la dignité humaine notait, en 2001, que « *des campagnes en vue d'une utilisation plus sûre*

---

107. European Union Opinion Research Group (EEIG), *Illegal and harmful content on the Internet*, *op. cit.*

d'Internet ont eu lieu dans la plupart des États membres<sup>108</sup>. Plusieurs États membres ont souligné l'importance que revêtent les écoles en tant que lieu approprié pour des mesures pédagogiques<sup>109</sup>. » Depuis, les initiatives se sont multipliées, le plus souvent venant de la société civile, associations et acteurs économiques, parfois soutenus par la Commission européenne et les États. Récemment reconduit pour les années 2004-2008<sup>110</sup>, le « Programme d'action pour un internet plus sûr » (*Safer Internet Action Plan*) de la Commission européenne distribue 11,7 millions d'euros suivant huit lignes de projets réparties au gré des trois objectifs principaux du programme, parmi lesquels la mise en place de campagnes nationales de sensibilisation<sup>111</sup>. Douze projets de sensibilisation aux risques liés aux usages de l'internet ont été financés dans ce cadre<sup>112</sup>. La Commission prépare un projet de proposition d'extension du Plan d'action pour un internet plus sûr aux années 2005-2008.

### Exemples d'initiatives gouvernementales

Certains États ont choisi de développer des campagnes d'ampleur nationale. La *task force* dédiée à la protection des enfants sur l'internet du *Home Office* britannique est à l'origine, depuis 2002, de plusieurs initiatives de communication nationales, comme le site *thinkuknow.co.uk*, ou « comment rester en sécurité tout en s'amusant sur l'internet<sup>113</sup> », conçu à l'attention des enfants et de leurs parents. Début 2003, le gouvernement britannique a investi plus de 1,5 million d'euros dans une campagne pluri-médias (une campagne télévisée a été diffusée en juillet 2003) alertant enfants et parents sur les mesures de prudence élémentaires à adopter sur l'internet en général, et sur les *chats* en particulier<sup>114</sup>. Le *Home Office* a annoncé le 4 octobre 2004 l'extension jusqu'en janvier 2005 de cette campagne, qui fait l'objet de nouvelles annonces radiophoniques et de publicités en ligne. Plus de 450 000 euros seront investis par le Gouvernement britannique dans cette nouvelle phase<sup>115</sup>.

---

108. Autriche, Belgique, Allemagne, Grèce, Espagne, Irlande, Pays-Bas, Luxembourg, Suède, Finlande, Royaume-Uni. La France, avec le programme Educaunet, s'est également engagée dans cette voie en coopération avec une institution belge.

109. Commission européenne, Rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant l'application de la recommandation du Conseil du 24 septembre 1998 sur la protection des mineurs et de la dignité humaine, *op. cit.*, p. 9.

110. Décision n° 2003/1151/CE du Parlement européen et du Conseil.

111. « Appel à propositions pour des actions indirectes au titre du plan d'action communautaire pluriannuel sur la promotion d'une utilisation plus sûre d'internet et des nouvelles technologies en ligne (2003 à 2004) », *JOUE*, C 209/30, 4 septembre 2003.

112. Tous ces projets peuvent être consultés sur le site du programme à l'adresse : [http://europa.eu.int/information\\_society/programmes/iap/projects/index\\_en.htm](http://europa.eu.int/information_society/programmes/iap/projects/index_en.htm) et <http://www.saferinternet.org/projects/>.

113. Voir : <http://www.thinkuknow.co.uk/>.

114. « Online child safety drive launched », *BBC News – World Edition*, 6 janvier 2003.

115. Home Office, « Protecting children online when they are most at risk – new radio & online advertising », Communiqué de presse. Reference: 310/2004. 4 octobre 2004 – [http://www.homeoffice.gov.uk/n\\_story.asp?item\\_id=1092](http://www.homeoffice.gov.uk/n_story.asp?item_id=1092).

### **Exemples d'initiatives de la société civile**

Différentes organisations à but non lucratif ont également entrepris de communiquer des conseils de prudence auprès des parents et des enfants, le plus souvent sur le *web*, qui constitue naturellement l'un des canaux de communication les plus économiques, même s'il n'est pas toujours le plus efficace. Pionnier de l'éducation aux médias, le Réseau Éducation-Médias canadien a par exemple créé le site *WebAverti*, qui multiplie les conseils de sécurité à l'attention des enfants de cinq tranches d'âges différentes, et met en valeur les moyens de « tirer le meilleur d'internet » autant que les dangers du réseau<sup>116</sup>. Aux États-Unis, l'*Internet Education Foundation (IEF)* a fédéré dès 1999 les principaux acteurs économiques de l'internet (constructeurs de matériel, opérateurs de réseaux, éditeurs de logiciels, éditeurs de services, sites marchands...) autour du site *GetNetWise*, qui constitue l'une des sources les plus complètes et les plus fréquentées en matière de sensibilisation à des usages raisonnés de l'internet<sup>117</sup>.

Certains acteurs économiques se sont également impliqués exclusivement dans la réalisation de sites et de documents attirant l'attention des plus jeunes et de leurs parents sur le bon usage de l'internet. La société Microsoft est ainsi à l'initiative, en Grande-Bretagne, du site *WebSafeCrackerz*, qui entreprend de sensibiliser sur un ton ludique les jeunes internautes à certains usages à risques de l'internet<sup>118</sup>.

### **Un autre «retard français» en matière d'éducation aux usages de l'internet?**

Les précédents travaux du Forum des droits sur l'internet portant sur la protection de l'enfance sur l'internet recensaient certains des projets paraissant les plus aboutis en ce domaine<sup>119</sup>.

### **La lente maturation des programmes de sensibilisation aux usages de l'internet à l'école**

On y notait la faiblesse des programmes de sensibilisation aux usages de l'internet à l'école en France, où le ministère de la Jeunesse, de l'Éducation nationale et de la Recherche s'est pourtant fixé pour objectif de développer la sécurité des jeunes utilisateurs sur les réseaux. Le ministre délégué à l'Enseignement scolaire a ainsi écrit aux recteurs d'académie au début de l'année 2004 qu'il souhaitait que des « *mesures de sensibilisation, de formation et de responsabilisation des utilisateurs* » accompagnent le renforcement des contrôles sur les contenus accessibles en ligne depuis les établissements scolaires: « *des actions d'information et de sensibilisation à destination des équipes éducatives et des élèves sont à prévoir en s'appuyant sur les ressources éducatives les plus concernées* »<sup>120</sup>. Instauré en 2000, le Brevet informatique et internet (B2i), qui atteste le niveau acquis par les élèves des écoles, du collège, et prochainement

---

116. Voir: <http://www.webaverti.ca/>

117. Voir: <http://www.getnetwise.org/>

118. Voir: <http://www.websafecrackerz.co.uk/>

119. Le Forum des droits sur l'internet, *op. cit.*

120. Lettre de Xavier Darcos, ministre délégué à l'Enseignement scolaire, aux rectrices et recteurs d'académie. 26 janvier 2004 – <http://www.educnet.education.fr/chrgt/courrierRecteurs04.pdf>.



du lycée dans la maîtrise des outils multimédias et de l'internet, reste largement centré sur la validation de compétences techniques plutôt qu'il n'éveille les jeunes internautes aux précautions qui doivent assortir certains usages du réseau. Le B2i n'est pas encore mis en œuvre dans tous les établissements scolaires concernés. Le Centre de liaison de l'enseignement et des médias d'information (CLEMI), un organisme de l'Éducation nationale, et l'Université belge de Louvain ont développé, avec le soutien de l'Union européenne, un *kit* de sensibilisation et d'éducation critique aux usages de l'internet à destination des éducateurs et des parents de qualité<sup>121</sup>. Cette initiative, toutefois, n'a pas encore été déployée à une large échelle auprès des établissements scolaires français.

De nombreuses expérimentations se sont développées, souvent isolément, au sein de certaines classes. Ces travaux sont suivis par différentes instances éducatives, en particulier les cellules TICE dépendant des recteurs d'académie et les centres régionaux et départementaux de documentation pédagogique. Des formations sont dispensées dans les académies et les départements aux enseignants du primaire et du secondaire, en formation continue comme dans les instituts universitaires de formation des maîtres (IUFM). Ces diverses expérimentations et initiatives pédagogiques sur les aspects civiques et éthiques de l'internet ne semblent toutefois faire l'objet que de d'une faible coordination.

Développée en partenariat avec plusieurs acteurs publics et privés, une récente initiative du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche s'est donnée pour objectif de « *sensibiliser et informer les enfants, les parents et les enseignants des enjeux et des risques liés à l'utilisation de l'internet à l'école comme à la maison* » au cours de journées d'informations organisées dans toute la France à la demande d'établissements volontaires. Une première campagne de ce « Tour de France des collèves » doit être entreprise de décembre 2004 à juin 2005<sup>122</sup>.

### **Les initiatives existantes sont le plus souvent isolées**

Diverses initiatives de sensibilisation plus ponctuelles ont vu le jour en France, à l'initiative d'acteurs institutionnels ou privés. Un guide *Internet et familles*, élaboré en 1999 par l'Association des fournisseurs d'accès et de services internet (AFA), l'Union nationale des associations familiales (UNAF) et la Délégation interministérielle à la famille (DIF), constitue sans doute le premier véritable outil de sensibilisation et de responsabilisation des jeunes sur l'internet. En mai 2004, en application des recommandations émises en février 2004, le Forum des droits sur l'internet a pris l'initiative de la publication, en partenariat avec Bayard Presse, les ministères délégués à la Recherche et à la Famille, le fournisseur d'accès à l'internet Wanadoo et l'Union nationale des associations familiales (UNAF), de 400 000 exemplaires de deux guides pratiques illustrés à destination des adolescents et de leurs parents, suggérant notamment quelques conseils de prudence élémentaires. Ces guides sont également diffusés en libre téléchargement sur les sites des partenaires<sup>123</sup>, et seront prochainement réédités. Le site DroitDuNet.fr, également édité par le Forum des

---

121. Voir : <http://www.educaunet.org/>.

122. Voir : <http://www.unclieclieclie.net/>.

123. Voir par exemple : <http://www.droitdunet.fr/guide/>.

droits sur l'internet, informe spécifiquement parents et enfants de leurs droits, mais aussi des règles de prudence qu'il leur est recommandé d'observer dans leurs usages du réseau<sup>124</sup>. Le fournisseur d'accès à l'internet AOL a lancé en septembre 2003 un « programme ludo-éducatif pour sensibiliser les plus jeunes à la sécurité sur Internet » intitulé « Code du Web ». Cette initiative s'appuie sur un mini-site comprenant des conseils<sup>125</sup>, un quiz et un dessin animé à vocation pédagogique, et sur l'organisation d'interventions dans des magasins d'une sélection de villes. Le site Mineurs.fr, édité par la Délégation aux usages de l'internet (DUI), recense ces initiatives et s'efforce de leur donner quelque visibilité.

Atypique, enfin, est l'initiative d'un groupe de programmeurs bordelais qui a rendu publique, en 2004, la première version d'un logiciel capable de bloquer la communication par un jeune utilisateur de services de *chat* de données personnelles que ses parents ont préalablement définies. Sans prétendre empêcher de manière absolue le jeune utilisateur ne communique des informations personnelles sur l'internet, les variations possibles de la composition de chaque mot étant infiniment nombreuses, les concepteurs du logiciel semblent considérer ce dernier comme un outil utile à attirer l'attention d'un jeune enfant sur les risques qu'il peut encourir en communiquant ces données à un inconnu. *LogProtect* est distribué gratuitement sous licence de logiciel libre, et pourrait être intégré à des solutions logicielles de contrôle parental<sup>126</sup>.

De même qu'ils n'abordent pas spécifiquement ces problématiques sur le support internet, les pouvoirs publics n'ont pas encore entrepris de campagne grand public sur ces thèmes, comme on a pu l'observer, par exemple, à l'initiative du *Home Office* en Grande-Bretagne. La contribution de l'État à la sécurisation de la navigation des jeunes usagers de l'internet et à l'information des adultes sur les utilisations du réseau paraît ainsi comporter encore une large marge de progression.

## La contribution des logiciels de contrôle parental

En plus de bloquer l'affichage de certains contenus inappropriés aux enfants, certains logiciels de contrôle parental permettent aux parents d'interdire aux jeunes utilisateurs de communiquer avec des personnes inconnues sur l'internet. Certains outils permettent ainsi aux parents de bloquer l'accès à certains protocoles de communication, interdisant ainsi l'usage de certains logiciels (logiciel de courrier électronique, de communication instantanée...), ou encore les communications directes avec des correspondants non agréés en premier lieu par les parents.

Le logiciel *LogProtect*, dont la vocation paraît en premier lieu pédagogique, se présente comme un complément à de tels outils.

Les outils de contrôle parental, pour utile que puisse être leur contribution, ne peuvent toutefois palier l'insuffisance de l'information des adultes et les carences de l'effort de sensibilisation destiné aux enfants.

---

124. Voir notamment : <http://www.droitdunet.fr/juniors/> et <http://www.droitdunet.fr/parents/>.

125. Voir : [http://www.aol.fr/declic\\_securite/](http://www.aol.fr/declic_securite/).

126. Voir : <http://www.logprotect.net/>.

## Recommandations

L'internet est porteur de formidables opportunités pour les jeunes. Ces derniers comptent parmi les utilisateurs les plus actifs et les plus curieux du réseau. Cependant, des activités et des contenus susceptibles de constituer une menace, directe ou indirecte, pour eux prospèrent aussi dans cet environnement.

Les présentes recommandations ont pour objectif de contribuer à renforcer les moyens de lutter contre la diffusion et le recel de contenus pédo-pornographiques sur l'internet, et de prévenir les risques que des contacts établis sur l'internet puissent préparer une atteinte sexuelle, une agression sexuelle ou une tentative d'agression sexuelle, un viol ou une tentative de viol sur un mineur.

**L'examen des données disponibles établit incontestablement que le réseau est employé au profit de l'échange d'un volume important d'images pédo-pornographiques. Il confirme également que des adultes sont susceptibles d'identifier, de contacter et de « piéger » des enfants en tirant avantage des possibilités de mise en contact offertes par les applications les plus populaires de l'internet. L'ampleur de la menace, toutefois, reste difficile à évaluer.**

Le préalable à toute action efficace contre ces atteintes et risques d'atteintes graves à l'encontre de mineurs consiste à prendre la mesure précise de ces phénomènes. Beaucoup de travail reste à entreprendre dans ce domaine pour obtenir une image nette, susceptible de guider précisément l'action publique et d'inspirer de nouvelles initiatives aux acteurs de l'internet.

Il se dégage depuis plusieurs années, parmi les États comme parmi l'ensemble des acteurs de l'internet, un véritable consensus à agir contre ces phénomènes : pouvoirs publics, acteurs économiques, associations. Ces derniers confirment, dans ces recommandations, leur volonté de participer, chacun à la mesure de ses capacités d'action et de ses responsabilités.

Aucune solution n'est, à elle seule, de nature à faire cesser ces activités. On ne saurait en particulier s'en remettre simplement au renforcement des dispositifs pénaux et à l'action des seuls pouvoirs publics pour atteindre ces objectifs. Les recommandations proposent par conséquent à l'ensemble des acteurs de l'internet (pouvoirs publics, acteurs économiques, associations, parents) la mise en place d'une diversité d'actions visant à lutter contre ces délits ou à prévenir les actes qui les préparent sur l'internet.

### Mieux connaître les usages et les risques

#### **1) Étudier les comportements des jeunes utilisateurs de l'internet et la diversité des risques auxquels ils peuvent être exposés sur le réseau.**

Les usages de l'internet par les jeunes Français ne sont pas précisément connus. Les premiers travaux consacrés par le Forum des droits sur l'internet à la protection des mineurs sur l'internet dressaient le constat du « défaut ou [de] l'obsolescence d'études du mode d'accès des jeunes à l'internet en France, de leurs pratiques sur le réseau et des circonstances de leur exposition à des contenus préjudiciables ». Le Forum recommandait alors que « soit entreprise, à l'initiative des pouvoirs publics, une veille nationale des usages de l'internet par les jeunes et de leur exposition en ligne à

*des contenus tenus pour préjudiciables par la loi*»<sup>127</sup>. Cette lacune paraissait en effet constituer un frein à l'appréciation des éventuels risques des usages de l'internet par les jeunes, et à la définition de politiques et d'outils adaptés.

Ce constat et ces recommandations concernant l'exposition des mineurs à des contenus préjudiciables sur l'internet restent d'actualité. Il importe de souligner que le rôle de l'internet dans la préparation d'atteintes ou d'agressions sexuelles ou de viols sur des mineurs est également méconnu en France.

### **Étudier les usages et les comportements des mineurs sur l'internet**

**Le Forum des droits sur l'internet recommande que les pouvoirs publics constituent un pôle de veille des usages de l'internet par les jeunes.** Ce pôle pourrait avoir mandat de recenser les études existantes dans ce domaine auprès des centres de recherche et des acteurs économiques, d'impulser de nouvelles études quantitatives (accès au réseau, fréquence d'utilisation, principaux sites et services, par exemple) et qualitatives (études comportementales) auprès de partenaires publics et privés, et de prendre l'initiative de sondages réguliers. Il serait ainsi à même de contribuer à identifier l'opportunité d'action et les champs d'action prioritaires de la puissance publique, tout comme les canaux de communication à privilégier pour sensibiliser les mineurs à des usages maîtrisés de l'internet. **Le Forum recommande que cette veille se concentre tout particulièrement sur les nouveaux supports d'accès et les applications émergentes du réseau, comme les différents services interactifs accessibles depuis les téléphones mobiles.**

Les missions de la Délégation aux usages de l'internet (DUI) «*de proposer les mesures propres à généraliser l'accès à l'internet ainsi que la formation des familles, des enfants et du grand public aux usages des nouvelles technologies*» et de «*[répondre] aux demandes de conseil et d'expertise qui lui sont adressées par les administrations centrales, les services déconcentrés de l'État, les collectivités territoriales et les autres acteurs du développement de l'accès du grand public à la micro-informatique, à l'internet et au multi-média*»<sup>128</sup> paraissent prédisposer cette administration à piloter une telle mission.

### **Identifier et étudier les risques auxquels les jeunes utilisateurs de l'internet sont susceptibles d'être exposés sur les espaces publics du réseau**

**Le Forum des droits sur l'internet recommande que les pouvoirs publics entreprennent une veille de l'exposition des mineurs sur l'internet à des actes participant à la préparation d'atteintes, d'agressions sexuelles ou de viols,** que ces actes fassent ou non l'objet d'une incrimination pénale : harcèlement, propositions de nature sexuelle non sollicitées sur les espaces de discussion, tentatives de rencontres non sollicitées et agressions suite à des contacts noués sur l'internet...

Plusieurs organismes et services, comme par exemple l'Observatoire national de l'enfance en danger (ONED) ou l'institution du Défenseur des Enfants, paraissent suscep-

---

127. Le Forum des droits sur l'internet, *op. cit.*

128. Décret n° 2003-1168 du 8 décembre 2003 portant création d'une délégation aux usages de l'internet, *JORF*, n° 284 du 9 décembre 2003.

tibles d'entreprendre une telle veille<sup>129</sup>. Le Forum des droits sur l'internet recommande que le ministère en charge des affaires familiales et de l'enfance détermine quelle institution est le mieux à même de porter cette mission.

## **2) Recueillir et exploiter les statistiques policières et judiciaires pour mieux connaître les phénomènes.**

Un indicateur statistique comptabilisant, sur des bases unifiées, l'activité des services de police et de gendarmerie et des tribunaux en matière d'usages de l'internet aux fins d'échanger des contenus pédo-pornographiques ou de préparer des atteintes, agressions sexuelles et viols sur mineurs pourrait contribuer à alimenter et à orienter utilement l'action répressive et les initiatives de prévention dans ces domaines. Un tel indicateur n'existe pas.

Il conviendrait que chaque service d'enquête rapporte effectivement l'ensemble de ses activités dans le domaine de la protection des mineurs sur l'internet à une structure de référence chargée de coordonner les actions des services de police et de gendarmerie dans ce domaine spécifique de la cybercriminalité. La création d'indicateurs de référence communs aux services de police, de gendarmerie et de la justice serait utile à la collecte de ces informations.

Enfin, certaines infractions spécifiques décrivant l'échange des contenus pédo-pornographiques ou les atteintes et agressions sexuelles ou viols sur mineurs au moyen d'un réseau de communications électroniques n'interviennent souvent qu'à titre secondaire dans les procédures où elles sont mentionnées, et échappent à toute comptabilité. Il apparaît souhaitable qu'elles soient consignées anonymement et alimentent les statistiques judiciaires.

**Le Forum des droits sur l'internet recommande que les ministères de la Justice, de l'Intérieur et de la Défense mettent en place une base de données statistiques recensant les faits de détention et de diffusion de contenus pédo-pornographiques sur l'internet et d'agression de mineurs suite à des contacts établis sur l'internet.**

Cette base de données devra être constituée dans le respect des règles qui gouvernent la protection de la vie privée et des données personnelles relatives aux auteurs et aux victimes d'infractions, des outils communs permettant le partage de l'information.

**Le Forum des droits sur l'internet recommande que le ministère en charge des affaires familiales et de l'enfance soit rendu destinataire des données statistiques** décrivant l'activité des services judiciaires en matière d'usages de l'internet aux fins d'échanger des contenus pédo-pornographiques ou de préparer des atteintes, agressions sexuelles et viols sur mineurs.

---

129. L'Observatoire national de l'enfance en danger (ONED) doit «[contribuer] au recueil et à l'analyse des données et des études concernant la maltraitance envers les mineurs, en provenance de l'État, des collectivités territoriales, des établissements publics, des fondations et des associations» (loi n° 2004-1 relative à l'accueil et à la protection de l'enfance, art. 9). L'institution du Défenseur des Enfants est «chargé [e] de défendre et de promouvoir les droits de l'enfant consacrés par la loi ou par un engagement international régulièrement ratifié ou approuvé» (loi n° 2000-196 du 6 mars 2000 instituant un Défenseur des enfants, art. 1).

### **3) Organiser un rendez-vous annuel des acteurs de la protection des mineurs sur l'internet.**

La diversité des parties engagées en faveur de la protection des mineurs sur l'internet, l'évolution rapide des usages du réseau par les jeunes et celle des moyens de sécuriser ces usages justifient que s'intensifie le dialogue entre ces différents acteurs, qui le plus souvent ignorent l'étendue des compétences et des initiatives des autres parties.

**Le Forum des droits sur l'internet recommande l'organisation d'un rendez-vous annuel au cours duquel les pouvoirs publics, le réseau des associations et les acteurs économiques seraient amenés à échanger leurs connaissances et à rapprocher leurs actions en matière de protection des mineurs sur l'internet.** Des acteurs étrangers, en particulier européens, pourraient être invités à rendre compte de leurs actions et à témoigner de leur expérience dans ce cadre. Un tel rendez-vous permettrait enfin de rendre compte de la mobilisation des différentes parties en faveur du renforcement de la protection des mineurs sur l'internet en France.

Cette réunion régulière pourrait être organisée à l'initiative du ministère en charge des affaires familiales et de l'enfance.

## Sensibiliser les jeunes internautes et les adultes

### **4) Mettre en œuvre une vaste campagne de sensibilisation du grand public.**

Depuis plusieurs années, tant au niveau national qu'europpéen, la protection de l'enfance et la prévention des risques associés aux usages de l'internet font l'objet de rapports et recommandations qui tous soulignent la nécessité des politiques de sensibilisation et d'information du grand public. De nombreuses actions de communication ont été menées par une diversité d'acteurs institutionnels et associatifs sans cependant parvenir à un niveau satisfaisant d'information des enfants et des parents.

D'après un sondage Eurobaromètre réalisé fin 2003, une majorité (55 %) de parents de jeunes utilisateurs de l'internet déclaraient souhaiter être mieux informés sur les moyens de sécuriser les usages de l'internet, de préférence *via* les canaux traditionnels : à la télévision (43 %), par courrier (43 %) et, dans une moindre mesure, par les journaux (31 %) <sup>130</sup>.

On comprend à la lecture de ces statistiques que, s'ils ont été accueillis favorablement par les internautes qui en ont bénéficié, les efforts de sensibilisation à des usages maîtrisés de l'internet qui ont déjà vu le jour en France n'ont toutefois pas atteint l'objectif légitime de sensibilisation du très grand public.

**Le Forum des droits sur l'internet recommande que les pouvoirs publics prennent l'initiative d'une large campagne pluri-médias de sensibilisation aux usages**

---

130. European Union Opinion Research Group (EEIG), *Illegal and harmful content on the Internet*, Special Eurobarometer 203/Wave 60.2, Bruxelles, Commission Européenne, mars 2004 – Sondage réalisé interrogés en France entre novembre et décembre 2003.

**maîtrisés de l'internet, à l'adresse des parents et des jeunes utilisateurs de l'internet.**

Une telle campagne de type publicitaire (spots télévisés, radiophoniques, affichage, presse) pourrait avoir pour objectifs de faciliter la compréhension des usages des technologies de l'information par les parents, de souligner leur responsabilité et de valoriser leur rôle dans l'accompagnement de ces usages auprès des jeunes utilisateurs de l'internet. Elle viserait également à doter les jeunes utilisateurs des réflexes leur permettant des usages maîtrisés de l'internet.

**5) Mobiliser tous les canaux publics au profit d'une information complète des jeunes internautes et de leurs parents.**

**Le Forum recommande que cette campagne publicitaire soit associée à la création de supports d'information spécifiques au service des jeunes utilisateurs de l'internet et de leurs parents (émissions télévisées ou radiophoniques, numéro vert, site web...).**

Aucun site *web* d'information sur la maîtrise des usages de l'internet ne touche encore le très grand public. **Le Forum des droits sur l'internet recommande qu'un site *web de référence* soit constitué en « guichet unique » de l'information des jeunes utilisateurs de l'internet et des adultes sur l'ensemble des précautions à observer pour un usage maîtrisé de l'internet. Ce guichet devra de surcroît orienter ses visiteurs vers toutes les ressources utiles et autres initiatives de formation et d'information en ce domaine.** Pour remporter l'adhésion du très grand public, et atteindre des objectifs d'audience élevés, ce site devrait s'adresser spécifiquement à chaque cible (jeunes enfants, pré-adolescents, adolescents, parents, éducateurs...) en tenant compte de son niveau d'expertise, mobiliser des personnalités susceptibles de porter efficacement les principaux messages auprès de chacune de ces cibles, et proposer une diversité d'activités pédagogiques.

Les parents attendent de la télévision qu'elle les informe sur les moyens de sécuriser les usages de l'internet de leurs enfants. Ce canal de communication n'a pourtant encore jamais servi de support pour des informations de ce type. Il apparaît important, au regard des enjeux de la protection de l'enfance et de l'éducation sur l'internet, que soit réaffirmée la vocation éducative du secteur public de l'audiovisuel.

**Le Forum des droits sur l'internet recommande l'organisation d'une table ronde réunissant les responsables du secteur public de l'audiovisuel sous l'égide du Conseil supérieur de l'audiovisuel, afin d'envisager les modalités de production et de diffusion d'émissions récurrentes consacrées à l'éducation aux médias et incluant notamment des informations sur la prévention de certains risques des usages de l'internet par les plus jeunes et sur les moyens d'y parer.**

**Le Forum recommande que les acteurs économiques et les associations représentant les utilisateurs du réseau comme les familles participent de manière concertée à l'élaboration de cette campagne de sensibilisation et d'information, et qu'ils soient sollicités pour en assurer le relais auprès du grand public et des familles.** Il paraît particulièrement important que l'ensemble des acteurs soit partie prenante de la conception du site de référence, « guichet unique » de l'information des jeunes utilisateurs de l'internet et des adultes.

**Le Forum des droits sur l'internet recommande qu'une action d'information spécifique soit entreprise à destination des associations incluant la protection de l'enfance dans leurs missions**, qui leur rappellent notamment la marche à suivre et le cadre juridique à observer pour signaler aux autorités compétentes les contenus ou les comportements illicites qui leur sont parfois rapportés.

#### **6) Pour une éducation à des usages maîtrisés de l'internet à l'école.**

Renouvelant ses premières recommandations de mars 2004, **le Forum des droits sur l'internet recommande que les pouvoirs publics favorisent le développement auprès des établissements scolaires du premier et du second degré d'une véritable éducation à la civilité de l'internet à destination des élèves**, notamment les plus jeunes, et renforcent les objectifs et les moyens des établissements scolaires en matière d'information et de sensibilisation à des usages maîtrisés de l'internet, en sorte que chaque élève soit informé *a minima* des règles de prudence à adopter à l'égard de ses correspondants en ligne. Le Brevet informatique et internet (B2i) devrait être effectivement déployé dans tous les établissements scolaires, conformément à l'objectif formulé par le ministre de l'Éducation nationale dès 2000. Le B2i pourrait être étendu en sorte de valider la maîtrise des règles de prudence et d'éthique élémentaires qui doivent gouverner la découverte de l'internet par les mineurs.

Cette démarche de formation scolaire à des usages maîtrisés de l'internet devra prendre en compte et, le cas échéant, se combiner aux autres initiatives de sensibilisation, d'information et de formation à destination des enfants et des familles entreprises à l'initiative de l'État et de la société civile.

#### **7) Mobiliser les parents avec le soutien des associations familiales.**

Il est essentiel que les parents de jeunes usagers de l'internet exercent pleinement leur responsabilité d'adultes au cours des premières années d'utilisation du réseau par leurs enfants.

Il paraît par exemple essentiel que les parents des jeunes internautes accompagnent ceux-ci dans leur découverte du réseau, qu'ils placent l'ordinateur familial dans une pièce commune plutôt que dans la chambre de l'enfant, et ne permettent l'utilisation de certains outils comme la *webcam* par leurs plus jeunes enfants qu'en leur présence. Il apparaît souhaitable que les parents entretiennent un dialogue suivi avec leurs enfants au sujet de leurs perceptions et de leurs expériences de l'internet.

Les parents de jeunes enfants pourront également choisir d'adopter un outil de contrôle parental permettant notamment de limiter les communications de leurs enfants les plus jeunes à une liste prédéterminée de correspondants. L'usage de tels outils ne saurait toutefois intervenir qu'en complément de la vigilance des parents. Aucun outil de contrôle parental n'est en effet infaillible, ni ne saurait suppléer le rôle éducatif des parents.

**Le Forum des droits sur l'internet recommande que les associations familiales et de parents d'élèves prennent, en partenariat avec les pouvoirs publics, une part active à la sensibilisation des parents aux enjeux de la maîtrise des usages**



**de l'internet** et les assistent dans l'exercice de leur pleine responsabilité d'adultes sur l'internet. De telles initiatives pourront prolonger utilement d'autres campagnes de sensibilisation, d'information et de formation tournées vers les jeunes utilisateurs de l'internet.

**8) Encourager fournisseurs d'accès et exploitants de services à adopter un standard élevé d'information des usagers de leurs services.**

À en croire l'Eurobaromètre publié en mars 2004, les fournisseurs d'accès à l'internet et de services de télécommunication figurent en bonne place parmi les sources dont les parents de jeunes internautes attendent qu'ils les informent sur la maîtrise des usages de l'internet<sup>131</sup>.

De nombreux fournisseurs d'accès à l'internet (FAI) ont déjà entrepris, suite aux premiers travaux du Forum des droits sur l'internet relatifs à la protection de l'enfance, d'établir sur la page d'accueil de leurs sites un lien «Protection de l'enfance» menant vers une page d'information dédiée de leurs sites ou du site Pointdecontact.net, opéré par l'Association des fournisseurs d'accès et de services internet (AFA). Les fournisseurs d'hébergement et d'accès internet «grand public» membres de l'AFA se sont aussi engagés, dans la «Charte des prestataires de services d'hébergement en ligne et d'accès à Internet en matière de lutte contre certains contenus spécifiques» de juin 2004 «à rendre facilement accessibles depuis leurs portails, des informations [...] destinées à aider les parents à protéger leurs enfants sur Internet.»

**Le Forum des droits sur l'internet encourage l'ensemble de la profession à mettre en place un dispositif comparable à celui détaillé dans la charte des prestataires membres de l'AFA et à adopter un standard élevé d'information de leurs abonnés en matière de contrôle parental.** Le Forum encourage notamment l'ensemble des prestataires de services à réserver sur leurs sites une bonne visibilité à un lien «Protection de l'enfance» renvoyant vers des contenus destinés à aider les parents à protéger leurs enfants sur l'internet.

## Développer les outils favorisant la maîtrise des usages de l'internet

**9) Renforcer les outils à la disposition des jeunes utilisateurs d'espaces interactifs et de logiciels de messagerie instantanée.**

Les services interactifs et les applications de messagerie instantanée connaissent un succès grandissant parmi les jeunes utilisateurs de l'internet. Par leurs choix, les exploitants de ces services peuvent contribuer à limiter les risques que ces outils soient détournés de leur finalité par des adultes mal intentionnés à l'encontre de mineurs.

Par une charte signée le 14 juin 2004, les fournisseurs d'accès et d'hébergement «grand public membres de l'Association des fournisseurs d'accès et de services

---

131. 28% des parents de jeunes internautes indiquent attendre des informations sur les moyens de sécuriser les usages de l'internet des «fournisseurs d'accès à l'internet et de télécommunications» – European Union Opinion Research Group (EEIG), *op. cit.*

internet (AFA) se sont engagés à établir des liens vers «un formulaire de signalement d'abus» permettant aux utilisateurs «de signaler directement au prestataire du service d'hébergement concerné, ou au Point de contact de la profession accessible à l'adresse [www.pointdecontact.net](http://www.pointdecontact.net), ou aux autorités publiques dûment habilitées, tout contenu en ligne visé par [ladite] charte», «sur tous les espaces communautaires, objets de leurs services d'hébergement – tels que les forums de discussion, «chats», salons –, sur les pages d'accueil de leurs services, et le cas échéant, sur les pages de listes de réponses des moteurs de recherche intégrés à leurs portails, de manière à ce que ces usagers puissent effectuer ce signalement d'un seul «clic»» (art. 2). **Le Forum des droits sur l'internet recommande que l'ensemble de la profession, exploitants d'espaces communautaires ouverts au public (forums de discussion, chats, services de rencontres et communautaires ouverts aux adolescents) en particulier, se conforment aux bonnes pratiques que décrit cette charte.**

**Certains exploitants de services interactifs et éditeurs de logiciels de messagerie instantanée mettent en garde les jeunes internautes contre l'usage préjudiciable pouvant être fait du réseau par des personnes mal intentionnées, et leur adressent des conseils de prudence élémentaires. Le Forum des droits sur l'internet recommande que l'ensemble des exploitants de services et éditeurs de logiciels interactifs publient de telles mises en garde.** Ces messages pourraient par exemple être mis en évidence dans les espaces interactifs dédiés aux mineurs ou portant sur des thématiques les concernant au premier chef lors, le cas échéant, du téléchargement de l'application, de l'ouverture d'un compte d'utilisateur ou d'un profil public accessible à tous les utilisateurs du service, voire à l'ouverture de chaque session, sous réserve de faisabilité technique. Ces exemples pourront être adaptés en fonction du service, dans le souci de permettre la réception optimale de l'information par le jeune public. L'étude spécifique des usages de ces applications et services par les jeunes utilisateurs de l'internet et la mesure régulière de l'efficacité de ces messages pourront contribuer à renforcer l'impact de ces initiatives.

**Le Forum des droits sur l'internet recommande aux exploitants de services interactifs et aux éditeurs de logiciels de messagerie instantanée que les utilisateurs de leurs services bénéficient de fonctionnalités leur permettant de ne plus recevoir de messages d'un utilisateur en particulier et de bloquer la réception des messages d'utilisateurs ne figurant pas dans la liste de leurs contacts habituels, lorsque le service s'y prête.**

**Le Forum des droits sur l'internet recommande que soient explicitement affichées à l'entrée de tout espace interactif public son thème, le cas échéant la tranche d'âge à laquelle il s'adresse et la présence ou non de modérateurs.**

**Le Forum des droits sur l'internet recommande qu'il soit possible aux usagers de salons de discussion dédiés aux mineurs – ou portant sur des thématiques les concernant au premier chef – de contacter à tout moment un adulte référent, clairement identifié comme tel, compétent pour leur venir en aide et pour signaler, le cas échéant, un comportement préjudiciable aux mineurs aux autorités de police.**

## **10) Renforcer la maîtrise de la diffusion de données personnelles relatives à des mineurs sur l'internet.**

Les données personnelles de mineurs peuvent, lorsqu'elles sont rendues publiques, permettre à un adulte mal intentionné d'identifier de potentielles victimes, et parfois de les contacter directement et personnellement. Il paraît important, alors que les mineurs utilisent de plus en plus massivement l'internet et ses applications interactives, de renforcer la protection de leurs données personnelles.

### **Dans le cadre des services et applications interactifs de l'internet**

Les services interactifs et plates-formes de discussion en ligne comme les *chats* ou les logiciels de messagerie instantanée exercent un fort attrait sur les jeunes utilisateurs de l'internet, qui peuvent y être contactés par d'autres utilisateurs mal intentionnés. De tels cas de figure peuvent également se présenter sur certains sites de rencontres et de services communautaires s'adressant spécifiquement aux mineurs.

Certains exploitants de services et éditeurs de ces logiciels conseillent à leurs jeunes utilisateurs, lors du choix de leur pseudonyme ou lorsqu'il leur est proposé de déclarer des informations nominatives (nom, prénom, âge ou date de naissance, ville, adresse, numéro de téléphone, adresse de courrier électronique, par exemple), de ne pas rendre publiques d'informations les identifiant. **Le Forum des droits sur l'internet recommande que l'ensemble des exploitants de services interactifs et éditeurs de logiciels de messagerie instantanée adoptent cet usage** lorsque la nature et la finalité du service s'y prêtent.

**Le Forum des droits sur l'internet recommande de plus que tout utilisateur puisse avoir le choix de ne pas publier d'informations nominatives non nécessaires au fonctionnement du ou des services.** Un enfant devrait par exemple pouvoir rejoindre un salon de discussion ouvert au public sans toutefois devoir communiquer aux autres utilisateurs du *chat* de données personnelles comme son âge et sa ville de résidence.

### **Sur le web, en particulier dans le cadre des activités associatives ou scolaires**

L'article 9 du Code civil dispose que « *chacun a droit au respect de sa vie privée* », et donne à toute personne un droit exclusif sur son image et sur l'utilisation qui en est faite, sauf intérêt légitime de tiers. L'autorisation de la personne représentée ou du titulaire de l'autorité parentale lorsque la personne est mineure et non émancipée, les mineurs ne disposant pas de leurs droits, est par conséquent indispensable.

Les articles 226-16 et suivants du Code pénal et la loi n° 78-17 du 6 janvier 1978 sur l'informatique et les libertés interdisent tout traitement informatisé de données personnelles lorsqu'il ne satisfaisait pas à certaines conditions. Il convient notamment par principe que la personne dont les données doivent faire l'objet d'une publication sur un réseau informatique comme l'internet consente à ce traitement. L'autorisation ne peut être délivrée que par le titulaire de l'autorité parentale si la personne est mineure et non émancipée.

**Le Forum des droits sur l'internet rappelle les dispositions de la loi française aux éditeurs de sites personnels et associatifs (associations sportives, associations**

de parents d'élèves...), et leur recommande de ne pas publier sur leurs pages *web* la photographie ou les données personnelles d'un mineur sans l'accord explicite des titulaires de l'autorité parentale.

Le Forum des droits sur l'internet recommande que les établissements scolaires veillent tout particulièrement à respecter les termes de la loi en matière de diffusion de l'image ou des données personnelles de personnes mineures, et qu'ils évitent en règle générale de rendre publiques de telles informations sur leurs sites *web*.

#### **11) Donner aux parents les moyens de choisir les meilleurs outils permettant de renforcer la sécurité des jeunes utilisateurs.**

Les pouvoirs publics ont contribué au renouvellement, en mai 2004, de l'étude comparative des outils de contrôle parental réalisée par l'Institut National de la Consommation (INC). Compte tenu de l'évolution rapide des techniques de contrôle parental et de l'information encore lacunaire dont disposent les parents sur ces outils, le Forum des droits sur l'internet encourage les pouvoirs publics à conclure avec l'INC un accord pluriannuel permettant la mise à jour régulière de cette étude.

Le Forum recommande également que les prochaines éditions de cette étude mettent spécifiquement en valeur les outils permettant de renforcer la sécurité des jeunes utilisateurs des applications interactives de l'internet (courrier électronique, messagerie instantanée, P2P...).

Engager une réflexion spécifique sur le droit et l'organisation du dispositif répressif

#### **12) Approfondir la réflexion sur d'éventuelles évolutions du droit.**

##### **Mesurer les opportunités d'évolution du droit pénal**

Le droit pénal français incrimine plusieurs comportements dont peut être victime un mineur : l'atteinte sexuelle « *sans contrainte, menace, ni surprise* », l'agression sexuelle ou le viol et leurs tentatives, qui supposent que l'acte délictueux soit consommé ou que soit constaté un commencement d'exécution. La chambre criminelle de la Cour de cassation adopte une conception constante du commencement d'exécution qui doit associer une intention irrévocable et un lien de causalité suffisamment étroit et direct entre le comportement et l'infraction consommée (« *des actes qui tendent directement au crime avec intention de la commettre* », « *des actes qui tendent directement et immédiatement à la réalisation du délit* », ou encore « *des actes devant avoir pour conséquence directe et immédiate de consommer le crime, celui-ci étant ainsi entré dans la période d'exécution* »). L'internet peut servir à préparer ces infractions, la mise en relation d'adultes déterminés à commettre une atteinte ou une agression sexuelle à l'encontre de mineurs étant notamment possible sur les espaces interactifs de communication électronique comme en d'autres lieux.

*Il n'existe pas, en droit français, d'infraction décrivant spécifiquement le fait, pour un adulte, de rechercher les faveurs sexuelles de mineurs, en ligne ou hors ligne, ou le*

*fait de rencontrer un mineur dans l'intention de commettre une atteinte ou une agression sexuelle ou un viol.* Certains membres des forces de police et associations de protection des droits des enfants déplorent cette situation, et souhaitent la création d'une infraction pénale spécifique au fait, pour un adulte, de rechercher sur l'internet les faveurs sexuelles d'un mineur. Ces acteurs considèrent qu'une telle incrimination nouvelle serait seule capable de permettre la répression de certaines prises de contact avant que ne soit effective une agression physique, et de renforcer les moyens de dissuader des adultes mal intentionnés d'entreprendre de telles démarches. Si l'on conçoit aisément l'intérêt d'un tel dispositif en termes, notamment, de dissuasion, ce dernier n'en paraît pas moins contraire aux principes de droit pénal qui excluent que l'on puisse incriminer une simple intention.

**Le Forum des droits sur l'internet recommande aux ministères de la Justice et de l'Intérieur d'examiner et de provoquer un débat sur l'opportunité de créer ou non une nouvelle incrimination pénale punissant le fait, pour un adulte, d'émettre des propositions à caractère sexuel à destination de mineurs, ou de chercher à rencontrer un mineur auquel il aurait adressé des propositions à caractère sexuel.**

#### **Envisager l'évolution des moyens de la procédure pénale**

Les faits de détention, de recel ou de diffusion de pédo-pornographie ne figurent pas au nombre des infractions citées par l'article 706-73 du Code de procédure pénale, qui établit la liste des incriminations auxquelles sont applicables les procédures spéciales décrites par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité. Ces procédures particulières, relatives notamment à l'infiltration (art. 706-81 du CPP), aux perquisitions (art. 706-89 et suivants du CPP) et à l'interception de correspondances émises par la voie des communications (art. 706-96 du CPP), ne sont donc pas applicables aux enquêtes sur les échanges en ligne d'images pédo-pornographiques. Le Garde des Sceaux avait pourtant indiqué à plusieurs reprises, au cours des débats parlementaires qui ont préparé le vote de la loi, que «*la criminalité organisée (...), ce sont les enlèvements, les trafics de stupéfiants, le terrorisme, la traite des êtres humains, les meurtres en bande organisée, les braquages en bande organisée, le proxénétisme aggravé, la pédo-pornographie par Internet*<sup>132</sup>.»

Certains représentants des autorités répressives souhaitent que les procédures spéciales prévues par la loi du 9 mars 2004 soient élargies à la recherche des auteurs de faits de diffusion d'images pédo-pornographiques, permettant ainsi aux enquêteurs de recourir, dans un cadre proprement défini par la loi, à l'emploi d'identités d'emprunt ou fictives, et de procéder légitimement à la recherche proactive de contenus illicites, à l'exclusion de toute démarche de provocation. Cette évolution maîtrisée des moyens procéduraux des services de police permettrait également d'encadrer l'utilisation par les enquêteurs de moyens de paiement, lorsqu'ils sont requis à l'entrée d'un site ou d'un service en ligne, pour vérifier une infraction.

---

132. Dominique Perben, Garde des Sceaux. Assemblée nationale, Troisième séance du jeudi 5 février 2004 -154<sup>e</sup> séance de la session ordinaire 2003-2004 – <http://www.assemblee-nat.fr/12/cri/2003-2004/20040154.asp>.

L'élargissement des moyens de procédure prévus par la loi du 9 mars 2004 ne peut toutefois être envisagé sans étude spécifique des conséquences de l'extension éventuelle de ces moyens à la recherche des auteurs de faits de diffusion d'images pédo-pornographiques, particulièrement en matière de sauvegarde des libertés publiques. Un dispositif alternatif à l'extension des moyens de procédures prévus par la loi du 9 mars 2004 pourrait ainsi être imaginé pour répondre aux principales demandes des enquêteurs.

**Le Forum recommande également aux pouvoirs publics d'examiner l'opportunité d'élargir certaines des dispositions de la loi du 9 mars 2004, comme l'infiltration, aux enquêtes portant sur la diffusion de matériels pédo-pornographiques sur l'internet. Les pouvoirs publics pourraient également choisir de privilégier un dispositif alternatif permettant aux agents des forces de l'ordre de rechercher ces infractions sous le couvert d'une identité d'emprunt ou fictive, et de les constater sur des serveurs auxquels l'accès est conditionné par l'utilisation d'un moyen de paiement. Ces opérations devraient être réalisées sous le contrôle de l'autorité judiciaire.**

### **13) Adapter l'organisation des services d'enquête.**

Les services d'enquête prenant part à la lutte contre la pédo-pornographie sur l'internet se sont pour l'essentiel organisés au gré des compétences et des initiatives de certains enquêteurs. L'efficacité de cette lutte paraît souffrir de la dispersion de l'information utile aux enquêtes et du manque de coordination entre services.

Le Forum des droits sur l'internet approuve le projet présenté le 7 septembre 2004 par le ministre de l'Intérieur, de la sécurité intérieure et des libertés locales de faire de certains services d'enquête des référents nationaux pour certaines infractions commises par le biais de l'internet et des réseaux.

**Le Forum recommande que le pôle de compétence chargé de la veille des contenus pédo-pornographiques sur l'internet dispose des moyens nécessaires à l'exercice de sa mission, et agisse en totale synergie avec les autres services concernés de l'État.**

**Le Forum des droits sur l'internet recommande que ce pôle soit conçu comme un outil de mutualisation des informations relatives à toutes les enquêtes en matière de pédo-pornographie sur l'internet, rassemblant et favorisant le partage et le recoupement de ces informations entre tous les services concernés aux niveaux national et international.**

Le Centre national d'analyse des images pédo-pornographiques (CNAIP), qui centralise les images saisies dans le cadre des enquêtes de police et de gendarmerie et met le produit de leur analyse à la disposition des services d'enquête, fonctionne déjà selon ce principe.

En revanche, un tel pôle de veille ne saurait toutefois se substituer aux services d'enquête. Ses pratiques se conformeraient naturellement aux règles qui régissent la protection des données à caractère personnel.

Le Forum des droits sur l'internet recommande que le pôle de veille établisse et remette aux ministres concernés un rapport d'activité annuel faisant notamment état de la coopération entre les services.

**14) Former enquêteurs et magistrats aux techniques et aux procédures de la recherche d'infractions sur l'internet et les supports informatiques.**

Le Forum des droits sur l'internet approuve résolument le projet annoncé en septembre 2004 par le ministre de l'Intérieur, de la sécurité intérieure et des libertés locales d'accélérer l'effort de formation des enquêteurs spécialisés au sein de la police et de la gendarmerie et d'en porter le nombre à 700 à l'horizon 2007.

**Le Forum recommande également que des magistrats référents en matière de cybercriminalité soient spécifiquement formés et renforcent les ressources des parquets généraux et des chambres d'instruction de chaque ressort de cour d'appel.**

**15) Clarifier le dispositif encadrant la conservation des données de connexion.**

Les autorités de police et de gendarmerie sont fréquemment amenées à requérir la transmission d'informations permettant l'identification d'utilisateurs du réseau auprès des opérateurs et exploitants de services de la société de l'information. Les décrets d'application de l'article L. 34-1 du code des postes et des communications électroniques et des dispositions de l'article 6-II de la loi du 21 juin 2004 pour la confiance dans l'économie numérique doivent encore préciser la nature et la durée de stockage des données de connexion à conserver par les opérateurs techniques. Ces décrets doivent aussi éclaircir les modalités d'exécution des réquisitions judiciaires.

**Le Forum des droits sur l'internet recommande que les pouvoirs publics fixent rapidement le cadre réglementaire relatif à la conservation des données de connexion,** satisfaisant aux impératifs des forces de sécurité comme aux contraintes des opérateurs et exploitants de services, dans le respect des libertés publiques.

## Renforcer la coopération internationale policière et judiciaire

La coopération et l'entraide internationale sont l'un des dispositifs fondamentaux d'une lutte efficace contre la diffusion de contenus illicites sur l'internet, et tout particulièrement de pédo-pornographie. De nombreux dispositifs internationaux pertinents restent toutefois inappliqués.

**16) Mettre en œuvre et promouvoir les dispositions de la Convention sur la cybercriminalité en matière de lutte contre la pédo-pornographie.**

La Convention sur la cybercriminalité du Conseil de l'Europe peut constituer une avancée considérable en matière d'unification de la politique de lutte contre la diffusion de matériels pédo-pornographiques des États qui y adhèrent, et un outil de coopération policière et judiciaire prometteur. **Le Forum des droits sur l'internet recommande que la France ratifie et adopte au plus tôt les dispositions de la Convention sur la cybercriminalité relatives à la lutte contre la diffusion de contenus pédo-pornographiques sur l'internet.**

**Le Forum des droits sur l'internet recommande que la France encourage certains États membres ou associés du Conseil de l'Europe, en particulier la Fédération de Russie, à signer et ratifier la Convention sur la cybercriminalité. Le Forum des droits sur l'internet recommande également que la France conclue, avec les principaux États non signataires de la Convention sur la cybercriminalité, des conventions bilatérales de coopération policière et d'entraide judiciaire en matière pénale renforçant les moyens de la lutte contre la cybercriminalité.**

Le Forum recommande que les ministères concernés préparent un bilan national de la coopération d'entraide judiciaire et policière entre les États, concernant notamment les mesures préconisées par la Convention sur la cybercriminalité, afin d'en évaluer l'efficacité et, le cas échéant, de proposer des aménagements du texte au Conseil de l'Europe.

#### **17) Renforcer la coopération, l'entraide judiciaire et les échanges de bonnes pratiques au sein de l'Union européenne.**

Le Forum des droits sur l'internet recommande que s'intensifient la coopération policière, l'entraide judiciaire et les échanges de bonnes pratiques au niveau européen.

La Convention d'entraide de l'Union européenne promet la simplification et l'accélération des demandes d'entraide judiciaire entre États membres, de magistrat à magistrat, et conformément aux procédures et aux formalités ayant cours dans l'État requérant. **Le Forum des droits sur l'internet recommande que la France ratifie au plus tôt la Convention d'entraide judiciaire de l'Union européenne.**

Le Forum des droits sur l'internet recommande également que les pouvoirs publics français favorisent l'organisation de rencontres informelles entre les autorités nationales et certains de leurs homologues européens, qui pourront les faire bénéficier de leur expérience et de leurs bonnes pratiques en matière de lutte contre la pédopornographie et la pédophilie sur l'internet.

## Conclusion

### **Poursuivre la réflexion sur les réseaux mobiles et les nouveaux supports d'accès à l'internet**

Les présentes recommandations dessinent un ensemble de pistes d'action tendant à renforcer les moyens de lutter contre la représentation et la préparation, sur l'internet, d'atteintes sexuelles à l'encontre de mineurs. Elles réaffirment la détermination des acteurs français de l'internet à défendre l'avenir des «Enfants du Net», et ont pour vocation d'inspirer l'action de l'ensemble des acteurs, et tout particulièrement des pouvoirs publics.

Les responsables politiques se sont désormais associés à cette réflexion : le ministre des Solidarités, de la Santé et de la Famille a annoncé en décembre 2004 que «/a



sécurisation des usages de l'Internet par les mineurs afin de participer à la lutte contre la pédo-pornographie» ferait l'objet de l'un des groupes de travail de la conférence de la famille 2005; le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales a annoncé, en septembre 2004, sa décision de renforcer spécifiquement les moyens des services de police et de gendarmerie en matière de cybercriminalité; le ministre de la Jeunesse, de l'Éducation nationale et de la Recherche avait dévoilé, en janvier 2004, son plan pour la sécurisation des usages de l'internet à l'école. Lors d'une conférence organisée à Bruxelles en novembre 2004, l'association belge Child Focus a su attirer l'attention des «*First Ladies*» de grands pays d'Europe et de nombreux décideurs européens sur certains usages de l'internet potentiellement particulièrement préjudiciables aux mineurs.

\*

\* \*

Ces recommandations traitent des usages de l'internet accessibles depuis les terminaux d'accès à l'internet les plus communs que sont les micro-ordinateurs. Ces applications ne doivent pas occulter les prochains usages de l'internet et les promesses des nouveaux supports d'accès au réseau.

Les dernières générations de réseaux et de téléphones mobiles sont en particulier devenues de véritables plates-formes multimédias donnant accès à de nombreux usages interactifs: courrier électronique, *chat*, enregistrement et diffusion d'images fixes ou animées, visioconférence, partage de fichiers, par exemple.

À ces nouveaux usages peuvent correspondre de nouveaux mésusages qu'il conviendra de prendre en compte dans l'intérêt de la protection des mineurs, d'autant plus que ces derniers sont nombreux à posséder un téléphone mobile<sup>133</sup>, et parmi les premiers à en explorer les nouveaux usages.

Les opérateurs de téléphonie mobile français sont sensibles à ces enjeux et souhaitent engager une réflexion sur les moyens spécifiques à mettre en œuvre pour renforcer la protection des mineurs dans le cadre de l'utilisation d'applications multimédias mobiles.

Le Forum des droits sur l'internet encourage cette démarche et recommande que de prochains travaux étudient les réponses spécifiques aux applications et aux supports mobiles qui pourraient être apportées en matière de protection des mineurs.

---

133. Selon le CREDOC, 63% des 12-17 ans étaient équipés d'un téléphone mobile en juin 2003 (Régis Bigot, op. cit.), ainsi que 5% des 7-10 ans interrogés dans le cadre d'une étude TNS) 5% des 7-10 ans interrogés dans le cadre d'une étude TNS (TNS-SOFRES, juin 2004).

## Annexe 1

### **Composition du groupe de travail**

**Odile AMBRY**, vice-présidente, Internet Society (ISOC), chapitre français

**Patrice BLANC**, secrétaire général, institution du Défenseur des Enfants

**Martine BROUSSE**, présidente, La Voix de l'Enfant

**Philippe CAILLOL**, chef du bureau du régime juridique de la presse et des services d'information, Direction du développement des médias (DDM) – Premier ministre

**Coralie CAPILLON**, juriste, La Voix de l'Enfant

**Estelle DE MARCO**, juriste, Association des fournisseurs d'accès et de services internet (AFA)

**Isabelle FALQUE-PIERROTIN**, déléguée générale, le Forum des droits sur l'internet

**Joël FERRY**, officier de gendarmerie, ministère de la Justice, Direction des affaires criminelles et des grâces (DACG)

**Axelle HOVINE**, adjointe au chef du bureau du régime juridique de la presse et des services d'information, Direction du développement des médias (DDM) – Premier ministre

**Guillaume LE FRIANT**, Lead Programming Manager, MSN France

**Jean-Paul LEROUX**, responsable concurrence et déontologie, Orange France

**Stéphane MARCOVITCH**, délégué général, Association des fournisseurs d'accès et de services internet (AFA)

**Olivier PERALDI**, adjoint au délégué, Délégation interministérielle à la famille (DIF)

**Myriam QUEMENER**, magistrate, chef du Bureau des politiques pénales générales et de la protection des libertés individuelles, Direction des affaires criminelles et des grâces (DACG), ministère de la Justice

**Jean-Pierre QUIGNAUX**, chargé de mission, Union nationale des associations familiales (UNAF)

**Anne TERRIER**, chargée de mission, institution du Défenseur des enfants

*Rapporteur du groupe de travail :*

**Matthieu LERONDEAU**, chargé de mission, Le Forum des droits sur l'internet

## Annexe 2

### **Auditions et entretiens par le groupe de travail**

**Chantal d'ABOVILLE** (entretien), administratrice, Innocence en danger

**Alain BOULAY**, président, Association d'aide aux parents d'enfants victimes (APEV)

**Catherine CHAMBON**, Commissaire divisionnaire, Office central de lutte contre la criminalité liée aux technologies de l'information (OCLCTIC)

**Sylvie CLEYET**, responsable du projet Assurnet contre la cyberpédocriminalité, région Rhône-Alpes

**Marcel FAURE**, commissaire divisionnaire, division nationale pour la répression des atteintes aux biens et personnes (DNRAPB)

**Divina FRAU-MEIGS**, professeur de sociologie des médias, universités d'Orléans et Paris I Panthéon-Sorbonne

**Eric FREYSSINET** (entretien), chef d'escadron de gendarmerie, Chef du département INL, Institut de recherche criminelle de la gendarmerie nationale (IRCGN)

**Fabrice GAUTHIER**, Commandant de police, Brigade de protection des mineurs (BPM) de Paris

**Arnaud GRUSELLE**, président, Fondation pour l'enfance

**Philippe JARLOV**, adjudant-chef de gendarmerie, Section des recherches de Bordeaux

**Philippe JEAMMET**, professeur de psychiatrie, Institut mutualiste Montsouris (IMM), université Paris-V René Descartes, président, École des parents et des éducateurs (EPE)

**Marie LAJUS**, commissaire de police, Brigade de protection des mineurs (BPM) de Paris

**Yvon TALLEC**, Premier substitut du procureur, chef du parquet des mineurs, Tribunal de grande instance (TGI) de Paris

**Bernard VALADON**, président, Le Bouclier

**Grégory VERET**, Action Innocence Group (AIG)

## Annexe 3

# Bibliographie

### Ouvrages et rapports

John CARR, *Child abuse, child pornography and the Internet*. NCH, 2004.

CONSEIL DE L'EUROPE, *L'impact de l'utilisation des nouvelles technologies de l'information sur la traite des êtres humains aux fins d'exploitation sexuelle. Rapport final du groupe de spécialistes EG-S-NT*. Conseil de l'Europe (Direction générale des droits de l'homme, Division égalité entre les femmes et les hommes), septembre 2003.

LE FORUM DES DROITS SUR L'INTERNET, *Les enfants du net (I) : Les mineurs et les contenus préjudiciables sur l'internet*. Le Forum des droits sur l'internet, 2004.  
<http://www.foruminternet.org/recommandations/lire.phtml?id=694>

HOME OFFICE TASK FORCE ON CHILD PROTECTION ON THE INTERNET, *Good practice models and guidance for the internet industry on: chat services, instant messaging (IM), web based services*. Home Office Communication Directorate, janvier 2003.  
[http://www.homeoffice.gov.uk/docs/ho\\_model.pdf](http://www.homeoffice.gov.uk/docs/ho_model.pdf)

INTERNET WATCH FOUNDATION. *Annual Report 2003*. Internet Watch Foundation, 2003.

Kenneth V. LANNING, *Child Molesters: A Behavioral Analysis*. National Center for Missing & Exploited Children, National Center for Missing & Exploited Children (NCMEC), U.S. Department of Justice (Office of Juvenile Justice and Delinquency Prevention), septembre 2001.  
[http://www.missingkids.org/en\\_US/publications/NC70.pdf](http://www.missingkids.org/en_US/publications/NC70.pdf)

Agathe LEPAGE, *Libertés et droits fondamentaux à l'épreuve de l'internet*. éditions du Juris-Classeur, 2002.

Sheridan MORRIS, *The future of netcrime now*. Online Report 62/04. Home Office, décembre 2004.

Part 1, *Threats and challenges*

<http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6204.pdf>

Part 2, *Responses*

<http://www.homeoffice.gov.uk/rds/pdfs04/rdsolr6304.pdf>

SÉNAT (Service des affaires européennes). «La lutte contre la pornographie enfantine». *Les documents de travail du Sénat. Série Législation comparée*, mai 2001, n° 90.

<http://www.senat.fr/lc/lc90/lc90.html>

Alex TURK, *Quand les policiers succèdent aux diplomates*. Rapport d'information 523 (97-98). Sénat, 25 juin 1998.

<http://www.senat.fr/rap/r97-523/r97-523.html>

UNITED STATES GENERAL ACCOUNTING OFFICE. *File-Sharing Programs. Peer-to-Peer Networks Provide Ready Access to Child Pornography*. Report to the Chairman and Ranking Minority Member, GAO-03-351. House of Representatives (Committee on Government Reform), février 2003.

<http://www.gao.gov/cgi-bin/getrept?GAO-03-351>

Janis WOLAK, Kimberly MITCHELL, David FINKELHOR, *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. National Center for Missing & Exploited Children (NCMEC), U.S. Department of Justice (Office of Juvenile Justice and Delinquency Prevention), novembre 2003.

[http://www.missingkids.org/en\\_US/publications/NC132.pdf](http://www.missingkids.org/en_US/publications/NC132.pdf)

## Articles

Frédéric BARILLE, «Le pédophile chassait sur Internet». *Ouest-France*, 24 novembre 2004.

<http://www.brest.maville.com/actu/detail.asp?idDoc=181602&IdCla=19>

Martin BRIGHT, «BT puts block on child porn sites». *The Observer*, 6 juin 2004.

[http://observer.guardian.co.uk/uk\\_news/story/0,6903,1232422,00.html](http://observer.guardian.co.uk/uk_news/story/0,6903,1232422,00.html)

Roger DARLINGTON, «Sex on the Net», version du 2 août 2004.

<http://www.rogerdarlington.co.uk/sexonnet.html>

Arnaud DEVILLARD, «MSN ferme ses salons pour cause de dérive pornographique». *01Net*, 24 septembre 2003.

<http://www.01net.com/article/217608.html>

Jacky DURAND, «Villepin pour une lutte Net et sans bavure». *Libération*, 8 septembre 2004.

<http://www.liberation.fr/page.php?Article=237065>

Estelle DUMOUT, Jérôme THOREL, «LCEN: le Conseil constitutionnel censure l'amendement Devedjian». *ZDNet France*, 15 juin 2004.

<http://www.zdnet.fr/actualites/internet/0,39020774,39157007,00.htm>

Will GARDNER, «The Sexual Offences Bill: Progress and the Future». Discours prononcé lors de la conférence «Tackling Sexual Grooming», Londres, 29 septembre 2003.

<http://www.childnet-int.org/downloads/online-grooming2.pdf>

Margaret A. HEALY, «Child pornography: an international perspective». Document de travail. Congrès mondial contre l'exploitation sexuelle commerciale des enfants, Stockholm, 27-31 août 1996.

[http://www.usemb.se/children/csec/child\\_pornography.html](http://www.usemb.se/children/csec/child_pornography.html)

Robert JACQUES, «Blair backs BT child porn prevention filter». *VNUNet.com*, 22 juillet 2004.

<http://www.vnunet.com/news/1156795>

Isabelle DE SCHRIJVER, Tom VAN RENTERGHEM, Heidi DE PAUW, «Child Pornography on the Internet». Présentation lors de la conférence «The Challenge of Cybercrime» (Conseil de l'Europe), Strasbourg, 15-17 septembre 2004.

[http://www.cœ.int/T/E/Legal\\_affairs/Legal\\_co-operation/Combating\\_economic\\_crime/Cybercrime/International\\_conference/Child%20Pornography%20on%20the%20Internet.pdf](http://www.cœ.int/T/E/Legal_affairs/Legal_co-operation/Combating_economic_crime/Cybercrime/International_conference/Child%20Pornography%20on%20the%20Internet.pdf)

« Online child safety drive launched ». *BBC News – World Edition*, 6 janvier 2003.  
[http://news.bbc.co.uk/2/hi/uk\\_news/2629611.stm](http://news.bbc.co.uk/2/hi/uk_news/2629611.stm)

« Cyber-cops to patrol Internet chatrooms ». *CNN*, 9 juin 2004.  
<http://www.cnn.com/2004/TECH/internet/06/09/crime.internet.reut/>

## **Enquêtes et sondages**

David FINKELHOR, Kimberly MITCHELL, Janis WOLAK, *Online Victimization: A Report on the Nation's Youth*. National Center for Missing & Exploited Children (NCMEC), U.S. Department of Justice (Office of Juvenile Justice and Delinquency Prevention), juin 2000.  
[http://www.missingkids.org/en\\_US/publications/NC62.pdf](http://www.missingkids.org/en_US/publications/NC62.pdf)

David FINKELHOR, Kimberly MITCHELL, Janis WOLAK, « Highlights of the Youth Internet Safety Survey ». *OJJDP Fact Sheet*, mars 2001, n° 4.  
[http://www.missingkids.org/en\\_US/documents/internetsafety\\_surv.pdf](http://www.missingkids.org/en_US/documents/internetsafety_surv.pdf)

Sonia LIVINGSTONE, Magdalena BOBER, *UK Children Go Online. Surveying the experiences of young people and their parents*. Economic & Social Research Council (ESRC), Juillet 2004.  
<http://www.children-go-online.net/>

Céline METTON, « Ils s'aiment par Internet ». *Informations sociales*, novembre 2003, n° 111, pp. 32-41.

EUROPEAN UNION OPINION RESEARCH GROUP (EEIG), « Illegal and harmful content on the Internet ». Special Eurobarometer 203/Wave 60.2, mars 2004.  
[http://europa.eu.int/information\\_society/programmes/iap/docs/pdf/reports/eurobarometer\\_survey.pdf](http://europa.eu.int/information_society/programmes/iap/docs/pdf/reports/eurobarometer_survey.pdf)

RÉSEAU EDUCATION-MÉDIAS, *Young Canadians in a Wired World. Phase II. Focus Groups*. Réseau Education-Médias, février 2004.  
[http://www.media-awareness.ca/english/special\\_initiatives/surveys/index.cfm](http://www.media-awareness.ca/english/special_initiatives/surveys/index.cfm)

# Liens commerciaux : prévenir et résoudre les atteintes aux droits des tiers

*Recommandation publiée le 26 juillet 2005*

## Introduction

### Contexte et objectifs

Les liens commerciaux constituent l'une des toutes dernières techniques publicitaires pratiquées sur l'internet. C'est le format de publicité en ligne qui connaît, depuis sa création, la plus forte croissance, et c'est désormais l'un des plus employés : d'après l'*Internet Advertising Bureau* (IAB), les liens commerciaux représentaient en 2004 plus de 40 % des investissements publicitaires sur l'internet aux États-Unis<sup>134</sup>. Ils pourraient approcher près d'un tiers de ces dépenses en France. D'après le cabinet d'études *Forrester Research*, le chiffre d'affaires du marché européen des liens sponsorisés avoisinait 1,5 milliard d'euros en 2004. En France, il est estimé à 267,5 millions d'euros pour 2005, et pourrait s'élever à 822,5 millions d'euros d'ici 2010<sup>135</sup>. Les liens commerciaux soutiennent désormais ainsi la croissance de certaines des plus grandes entreprises de l'internet.

Les membres du groupe de travail sur la publicité en ligne du Forum des droits sur l'internet ont souhaité aborder le sujet des liens commerciaux pour contribuer, en formulant des recommandations à l'attention de l'ensemble des acteurs (personnes s'estimant victimes, annonceurs, fournisseurs de liens commerciaux), à prévenir et à résoudre des atteintes aux droits des tiers susceptibles de survenir dans le cadre de l'utilisation de ces liens.

En effet, un débat a vu le jour à l'occasion d'actions judiciaires récentes ; il porte notamment sur la question de la responsabilité de chacun des acteurs lors de la sélection de mots-clés permettant l'affichage des messages publicitaires. Les réponses à ces questions se construiront au fil de la jurisprudence. Dans cette attente, le groupe de travail constitué au sein du Forum des droits sur l'internet s'est accordé à encourager la collaboration de l'ensemble des acteurs pour mettre fin, le plus efficacement et le plus rapidement possible, aux préjudices subis par des tiers du fait de la sélection abusive, fautive, ou simplement par erreur, d'un mot-clé pour générer l'affichage d'un lien commercial.

---

134. Source : PriceWaterHouseCoopers – Internet Advertising Bureau. *IAB Internet Advertising Revenue Report. 2004 Full-Year Results*. Avril 2005. [http://www.iab.net/resources/adrevenue/pdf/IAB\\_PwC\\_2004full.pdf](http://www.iab.net/resources/adrevenue/pdf/IAB_PwC_2004full.pdf)

135. Source : Forrester Research Inc.

**Le présent document décrit les règles de conduite dont la mise en œuvre est recommandée à chacun des acteurs concernés pour prévenir et mettre fin, en dehors de toute procédure judiciaire, aux dommages qui pourraient être causés par la sélection d'un ou plusieurs mots-clés. Elles n'ont pas pour but de définir les contours du régime de responsabilité applicable aux acteurs intervenant dans le cadre de l'établissement de liens commerciaux.**

**De la même manière, certaines questions spécifiques à la création de liens commerciaux dans le cadre de programmes d'affiliation ne sont pas abordées dans ces recommandations.**

Ces recommandations ont été approuvées par le Conseil d'orientation du Forum des droits sur l'internet le 26 juillet 2005.

## Fonctionnement des liens commerciaux et rôle des acteurs dans la sélection des mots-clés

Lorsqu'un internaute lance une recherche sur certains annuaires ou moteurs de recherche, lorsqu'il consulte les pages ou utilise les services de certains sites *web*, des liens publicitaires composés d'un titre, d'un descriptif et d'une URL sont susceptibles d'apparaître en marge des contenus proprement dits, sous la mention «liens sponsorisés» ou «liens promotionnels», par exemple<sup>136</sup>. Ces liens commerciaux apparaissent en fonction des mots saisis par l'internaute lors de sa recherche ou en fonction des termes présents dans les pages de contenu où ils s'affichent. On parle de publicité contextuelle.

On distingue deux principaux acteurs dans le processus d'élaboration de ces liens commerciaux :

–l'annonceur ou son représentant, dont l'objectif est de faire connaître un produit ou un service aux utilisateurs de certains sites *web* ou services en ligne par le moyen de publicités contextuelles ;

et

–le prestataire de liens commerciaux, qui propose des services permettant l'affichage de ces publicités sur les pages de résultats de certains moteurs de recherche et sur les pages de certains sites partenaires dont les contenus correspondent aux mots-clés sélectionnés par l'annonceur ou son représentant.

Plus de 10 000 annonceurs de secteurs d'activité variés auraient aujourd'hui recours aux services des prestataires de liens commerciaux opérant en France. Leurs campagnes peuvent mobiliser de quelques mots-clés à plusieurs dizaines de milliers de termes.

En fonction des objectifs et de la nature de sa campagne, l'annonceur a le choix entre :

---

136. Apparus à l'origine sur la *web*, les liens commerciaux se développent à présent sur d'autres supports, comme par exemple les paquets de données au format RSS (Really Simple Syndication), abondamment exploités par les *blogs*, notamment.



– créer et gérer lui-même ses liens commerciaux et mots-clés directement en ligne ;  
ou

– avoir recours aux services « physiques » du prestataire de liens commerciaux, par lesquels un dialogue s’instaure entre le client et un gestionnaire de compte qui l’assiste dans l’élaboration et la gestion de ses liens commerciaux. Ainsi, à la demande du client, le prestataire peut l’assister dans l’optimisation des campagnes en travaillant sur les listes de mots-clés, afin d’améliorer leur pertinence et leur performance, eu égard aux statistiques des mots recherchés sur leur plate-forme.

Quel que soit le type de service choisi, le prestataire de liens commerciaux offre à l’annonceur la possibilité d’utiliser s’il le souhaite un outil (parfois intitulé « Générateur de mots-clés », ou « Voir les mots-clés recherchés ») énumérant sur une base statistique les requêtes les plus fréquemment formulées par les internautes contenant certains termes ou se rapportant à certains concepts. Cet outil peut aider l’annonceur à faire son choix de mots-clés pertinents dans le cadre de sa campagne, et à exclure les expressions qui ne le seraient pas, pour que son contenu s’affiche de manière ciblée.

L’annonceur ou son représentant indique pour chaque mot-clé sélectionné – généralement via un système d’enchères – le montant qu’il est prêt à payer pour chaque clic que recevra son lien commercial (on parle alors de « coût par clic »). Le lien commercial est affiché sur la page de résultats de certains moteurs de recherche partenaires ou sur les pages de sites partenaires contenant le ou les mots-clés sélectionnés. Dans l’hypothèse où plusieurs annonceurs apparaîtraient sur cette page, leur ordre de présentation variera notamment en fonction du « coût par clic » choisi par chaque annonceur.

L’annonceur valide ensuite la liste de mots à partir desquels son message publicitaire sera affiché.

Après positionnement, les annonceurs se voient attribuer un « outil de gestion des comptes en ligne » leur permettant de gérer eux-mêmes leur campagne via une interface. Grâce à celle-ci, ils peuvent ainsi, à tout moment, ajouter ou retirer des mots-clés de la liste qu’ils ont validée.

Le chiffre d’affaires généré par les clics des internautes est partagé entre le fournisseur de liens commerciaux et le support ou le partenaire de distribution.

## **Recommandation aux personnes s’estimant victimes d’une atteinte portée à leurs droits**

1) Le Forum des droits sur l’internet recommande aux personnes s’estimant victimes d’une atteinte portée à l’un de leurs droits en raison de l’apparition d’une annonce sur un service fournissant des liens commerciaux de formuler toute demande de suspension à l’annonceur et/ou au fournisseur de liens commerciaux.

Cette demande devra être formulée précisément par le titulaire des droits et être accompagnée :

–des documents justifiant qu’il a été porté atteinte à ses droits par l’utilisation de ses signes distinctifs, sans son accord, pour générer l’apparition de l’annonce (copie d’écran...);

–des documents justifiant de ses droits, notamment de propriété intellectuelle, sur les noms générant l’apparition de l’annonce;

–dans le cas où la demande est formulée auprès du prestataire fournisseur de liens commerciaux, une déclaration du plaignant selon laquelle l’annonceur ne s’est vu concéder aucun droit d’utiliser ce signe à titre de mot-clé (en vertu, par exemple, d’un contrat de licence ou en qualité de revendeur).

2) Les personnes s’estimant victimes pourront adresser leurs demandes directement auprès de l’annonceur concerné, qui est le plus à même de répondre de façon rapide et circonstanciée aux réclamations.

En cas d’insuccès auprès de l’annonceur, ou en cas d’impossibilité de le contacter ou de l’identifier, elles pourront formuler la demande de suspension auprès du prestataire fournisseur de liens commerciaux.

## **Recommandation aux annonceurs**

Le Forum des droits sur l’internet recommande aux annonceurs et à leurs représentants qui utilisent les services des fournisseurs de liens commerciaux de :

1) Vérifier que les mots-clés qu’ils souhaitent sélectionner pour faire apparaître leurs annonces ne porteront pas atteinte aux droits d’un tiers ou qu’ils disposent, le cas échéant, des droits nécessaires pour en faire usage (en qualité de distributeur agréé, par exemple).

2) Délivrer au prestataire fournisseur de liens commerciaux, sur première demande, la preuve des droits dont ils disposent ou qu’ils ont négocié pour employer dans le cadre de publicités en ligne, les termes qu’ils utilisent à titre de mots-clés.

3) Retirer dans les meilleurs délais le mot-clé litigieux qui a généré l’apparition de leur annonce, lorsqu’ils ont connaissance du fait que cette situation porte atteinte aux droits d’un tiers.

Le Forum des droits sur l’internet rappelle aux annonceurs et à leurs représentants les dispositions de l’article 6 de la loi n° 2004-575 du 21 juin 2004, selon lequel «*les personnes dont l’activité est d’éditer un service de communication au public en ligne mettent à disposition du public, dans un standard ouvert*», toutes les informations permettant de les identifier et d’entrer en contact avec elles. Ces informations devront donc être accessibles sur les sites auxquels renvoient les liens commerciaux.

## **Recommandation aux fournisseurs de liens commerciaux**

À titre liminaire, le Forum des droits sur l’internet se félicite des bonnes pratiques des fournisseurs de liens commerciaux qui ont pour effet direct ou indirect d’empêcher

l'emploi, dans le texte des annonces ou à titre de mots-clés, de termes susceptibles de porter atteinte aux droits des tiers. Certains prestataires fournisseurs de liens pratiquent par exemple un contrôle de l'adéquation entre les mots-clés sélectionnés et les contenus ou les services proposés par l'annonceur. Ce contrôle, sans s'apparenter à un contrôle de propriété intellectuelle, permet toutefois d'écarter certaines atteintes évidentes aux droits des tiers. Certains prestataires opèrent également des contrôles tendant à vérifier que les termes employés par les annonceurs ne sont pas inscrits dans des listes de signes distinctifs dont l'utilisation a été restreinte à la demande des titulaires des droits correspondants.

Le Forum recommande aux fournisseurs de liens commerciaux de :

- 1) Mettre formellement en garde les annonceurs, aux premiers niveaux de la relation commerciale, contre la sélection de mots-clés pouvant porter atteinte aux droits des tiers. De préciser en particulier qu'aucun annonceur ne doit sélectionner un mot-clé – ou un ensemble de mots-clés – correspondant à une marque ou au nom commercial d'une société concurrente. De renvoyer vers un ou plusieurs services permettant à l'annonceur de vérifier que les mots-clés qu'il souhaite choisir ne sont pas des noms protégés.
- 2) Préciser le rôle des générateurs de mots-clés, afin que ces outils ne soient pas présentés comme « conseillant » ou « suggérant » de sélectionner des mots-clés. Rappeler de façon très apparente à l'annonceur qu'il convient de vérifier la disponibilité des signes sélectionnés parmi ceux affichés par le générateur de mots-clés.
- 3) Suspendre l'utilisation des mots-clés litigieux dans les meilleurs délais lorsqu'ils ont connaissance du fait que cette situation porte atteinte aux droits d'un tiers suite à une réclamation complète et motivée effectuée par le titulaire des droits et contenant les éléments précisés précédemment.
- 4) Sous réserve des possibilités techniques, du respect des secrets industriels, et de la confidentialité de la relation entre l'annonceur et le prestataire de liens commerciaux, permettre à toute personne s'estimant victime d'une atteinte portée à l'un de ses droits de connaître le motif technique de l'affichage de l'annonce d'un concurrent en réponse à une requête comportant ses noms protégés.
- 5) Afficher sur leurs sites une information visible permettant aux titulaires de signes distinctifs de signaler une éventuelle atteinte à leurs droits dans le cadre d'un programme de liens commerciaux.

## Annexe 1

### Composition du groupe de travail

Association des fournisseurs d'accès et de services internet (AFA):

**Estelle DE MARCO**, juriste, chargée de mission

**Stéphane MARCOVITCH**, délégué général

Bureau de vérification de la publicité (BVP):

**Anne CHANON**, conseiller de la direction générale, en charge du développement déontologique

**Mohamed MANSOURI**

Consommation, logement, cadre de vie (CLCV):

**Frédérique PFRUNDER**, chargée de mission

Direction du développement des médias (DDM) – Premier ministre:

**Axelle HOVINE**, adjointe du chef du bureau du régime juridique de la presse et des services d'information

Google:

**Mats CARDUNER**, Managing Director, Google France

**Catherine GLAUBERT**, Paralegal, Google France

**Patricia MOLL**, European Policy Manager, Google Europe

Internet Advertising Bureau (IAB) France:

**Claudie VOLANT-RIVET**, déléguée générale

Observatoire des usages de l'internet (OUI):

**Michel ELIE**, président

Overture:

**Sophie PRADERE**, European Legal Counsel

Société générale:

**François COUPEZ**, juriste

**Stéphane VENDRAMINI**, juriste

Union des annonceurs (UDA):

**Laura BOULET**, juriste

**Christine REICHENBACH**, directeur juridique

**Françoise RENAUD**, directrice marketing relationnel et nouvelles technologies

Expert:

**Alain HAZAN**, avocat au barreau de Paris

*Rapporteur des travaux:*

**Matthieu LERONDEAU**, Le Forum des droits sur l'internet, chargé de mission

*Les travaux ont été préparés par:*

**Lionel THOUMYRE**, Le Forum des droits sur l'internet, juriste, chargé de mission

## Annexe 2

### **Auditions réalisées par le groupe de travail**

E-Spotting :

**Alain SANJAUME**, directeur général

Overture :

**Christophe PARCOT**, Managing Director Southern Europe

Real Media France :

**Amaury DELLOYE**, directeur commercial

Association Vivrelenet :

**Antoine DROCHON**, ingénieur consultant

Yahoo! France :

**Isabelle BORDRY**, présidente

**Hélène LANGLOIS**, responsable juridique

Experts :

**Nicolas BRAULT**, avocat au Barreau de Paris

**Gilles BUIS**, avocat au barreau de Paris

**Cyril FABRE**, avocat au barreau de Paris

**Jean-Philippe HUGOT**, avocat au barreau de Paris

**Thibault VERBIEST**, avocat aux barreaux de Bruxelles et Paris

# Commerce entre particuliers sur l'internet: quelles obligations pour les vendeurs et les plates-formes de mise en relation ?

*Recommandation publiée le 8 novembre 2005*

## Introduction

La France dénombrait<sup>137</sup>, en juin 2005, 24,7 millions d'internautes dont 11,5 millions de cyber-acheteurs. Parmi ceux-ci, certains pratiquent une nouvelle forme d'achat sur l'internet, ayant recours à des plates-formes permettant d'acquérir des biens, neufs ou d'occasion, auprès de particuliers voire d'entreprises. Cette nouvelle tendance a été mesurée dans l'étude Fevad/Mediametrie de juin 2005. Il s'avère que la fréquentation des plates-formes de mise en relation d'un acheteur avec un vendeur s'est accrue de 55 % entre les mois d'avril 2004 et avril 2005. Aujourd'hui, 39,4 % des cyber-acheteurs ont déjà eu recours à ce mécanisme d'achat, ce qui représente près de 5 millions de Français.

Ainsi, et grâce à l'internet, des particuliers ont dorénavant la possibilité de mettre en vente tous les produits d'occasion dont ils souhaitent se défaire, que ce soient des objets de collection, des livres, des meubles ou des biens plus importants comme des véhicules automobiles. Le particulier devient donc un véritable acteur du développement du commerce électronique.

Le succès de cette activité via internet n'a jamais été envisagé par le droit. En effet, le droit des contrats à distance a toujours été conçu comme protecteur du consommateur face à un professionnel. L'objectif était d'assurer une protection renforcée, justifiée par l'absence de rencontre physique avec le bien et d'évaluation de ce dernier et par le déséquilibre existant entre deux acteurs, l'un faible économiquement et mal informé (le consommateur), l'autre fort économiquement et averti (le professionnel)<sup>138</sup>. Or, les relations commerciales entre particuliers remettent en cause ce schéma. Elles font intervenir deux acteurs économiquement faibles et souvent mal informés sur leurs droits et obligations, pouvant créer une certaine insécurité juridique.

---

137. Étude Fevad/Mediametrie, juin 2005.

138. La finalité du droit de la consommation est aujourd'hui remise en cause, sous l'effet notamment du droit communautaire. En effet, les textes communautaires ont ajouté à l'objectif de protection, un autre but, « celui de faire du consommateur un véritable acteur du marché, utilisant les libertés prévues par les traités (...) le droit de la consommation bascule vers une application objective, sans considération du déséquilibre qui est présumé et vers une objectivisation des rapports entre professionnels et consommateurs », Rapport, *Le droit de la consommation, son périmètre, sa finalité, son efficience*, Institut national de la consommation, juin 2005.

Dès lors que ce nouveau canal de distribution transforme le particulier en acteur économique, il est apparu nécessaire de s'interroger sur les obligations respectives de l'acheteur, du vendeur ainsi que des plates-formes de mise en relation. Cet objectif est d'autant plus justifié que les plates-formes sont également utilisées par des professionnels, qui, eux, ont des obligations spécifiques.

Ces plates-formes sont donc au centre de ces nouvelles relations commerciales. Elles offrent un terrain à des vendeurs, particuliers et professionnels, afin d'exercer leur activité économique, que ce soit de manière ponctuelle ou récurrente. De par leur rôle d'intermédiaire technique et d'intermédiaire de vente, elles jouent un rôle pivot dans cette activité économique et apportent, à ce titre, leur tribu à la construction de la confiance sur le réseau.

L'objet de la présente étude réalisée par le Forum des droits sur l'internet à partir de mai 2004 à la suite, notamment, des conclusions de son premier rapport d'observation des pratiques de la cyber-consommation<sup>139</sup>, est donc de clarifier le régime juridique applicable aux relations commerciales entre particuliers et le rôle de chacun des acteurs.

## Méthodologie suivie

Le Forum des droits sur l'internet a composé, en juin 2004, un groupe de travail (composition en annexe) constitué de représentants des principales plates-formes de mise en relation, d'association de consommateurs, d'experts du droit de la consommation et du droit des nouvelles technologies ainsi que des administrations concernées.

Le groupe de travail a procédé, en complément de ses séances de travail collectif, à des auditions de personnalités désignées pour leurs connaissances et leurs expériences des relations commerciales entre particuliers (liste des auditions en annexe). Il a également entendu quelques utilisateurs ayant recours, de manière importante, à ces plates-formes.

La présente recommandation a été soumise pour validation aux membres du Forum des droits sur l'internet et a été adoptée par le Conseil d'orientation, par voie électronique, le 4 novembre 2005.

## Plan du rapport

Afin d'appréhender plus précisément le phénomène des relations commerciales entre particuliers, le rapport dresse un état des lieux des pratiques actuelles et précise le cadre de responsabilité applicable aux plates-formes de mise en relation (I). Ces éléments permettent de clarifier les obligations respectives de l'acheteur, du vendeur, qu'il soit professionnel ou non, ainsi que le rôle des plates-formes de mise en relation (II).

---

139. «Cyber-Consommation: les nouvelles tendances», Premier rapport du Forum des droits sur l'internet sur la cyberconsommation, 30 mars 2004.<http://www.foruminternet.org/publications/lire.phtml?id=707>

## **Le cadre général de la vente par un particulier sur l'internet**

Dans un premier temps, quelques précisions doivent être apportées afin de décrire les pratiques actuelles, déterminer le rôle de chaque acteur dans les processus contractuels et délimiter le cadre juridique du régime de responsabilité applicable.

### Les plates-formes de mise en relation : une relation tripartite aux contours juridiques difficiles

Lorsqu'une relation commerciale est nouée par l'intermédiaire d'une plate-forme de mise en relation, trois acteurs sont présents :

- l'acheteur,
- le vendeur,
- la plate-forme de mise en relation.

Ces acteurs sont reliés par plusieurs relations contractuelles. Tout d'abord, l'acheteur et le vendeur concluent chacun un contrat de prestation de service avec la plate-forme dont l'objet est la fourniture d'un outil technique de mise en relation et d'aide à la conclusion d'une vente. Ensuite, l'acheteur et le vendeur concluent, de gré à gré, un contrat de vente du bien commercialisé par l'intermédiaire de la plate-forme.

Cette organisation contractuelle de forme triangulaire n'est pas figée. Elle varie selon le rôle reconnu à la plate-forme dans le contrat conclu entre le vendeur et l'internaute/acheteur. Il est apparu, en effet, dans la pratique, que le site pouvait soit être un intermédiaire technique dans la relation commerciale, soit avoir le statut de mandataire du vendeur.

### **La plate-forme, représentante du vendeur : le mandataire**

Une première pratique consiste, pour la plate-forme, à être titulaire d'un mandat donné par le vendeur. Ce mandat consiste pour le site à intervenir aux côtés du vendeur dans la transaction finale qu'il conclura avec l'internaute.

Aux termes de l'article 1984 du Code civil, «*le mandat ou procuration est un acte par lequel une personne donne à une autre le pouvoir de faire quelque chose pour le mandant et en son nom*». Dans le secteur examiné, le contrat de mandat est conclu lors de l'acceptation par l'utilisateur du contrat de prestation de service proposé par la plate-forme. L'utilisateur souhaitant vendre ses biens donnera alors mandat au site de procéder en son nom et pour son compte à la perception, auprès de l'acheteur, du montant la vente, voire au traitement des contentieux qui pourraient naître entre acheteur et vendeur à la suite de cette vente.

**Le recours au contrat de mandat n'est, actuellement, le fait que des plates-formes proposant, de manière exclusive, des ventes à prix fixe.** En effet, si des plates-formes de ventes sous forme d'enchères procédaient de la même manière, elles seraient susceptibles de relever du régime spécial institué par les articles L. 321-1 et suivants du Code de commerce applicables en matière de ventes aux enchères publiques électroniques. Le premier alinéa de l'article L. 321-3 du Code du commerce précise, en effet, que «*le fait de proposer, en agissant comme mandataire du proprié-*



taire, un bien aux enchères publiques à distance par voie électronique pour l'adjuger au mieux-disant des enchérisseurs constitue une vente aux enchères publiques au sens du présent chapitre». Les sites qui relèveraient de cette définition pourraient alors être soumis à des obligations supplémentaires (agrément du Conseil des ventes volontaires, régime spécial de responsabilité, etc.)<sup>140</sup>.

## **La plate-forme, simple intermédiaire technique : le courtier en ligne**

Une seconde pratique consiste pour la plate-forme à agir comme un intermédiaire technique, simple outil de mise en relation entre un vendeur et un acheteur. La plate-forme est alors une partie tierce au contrat de vente conclu de gré à gré entre ses utilisateurs. Cette activité est classiquement dénommée « courtage en ligne ».

Le courtage en ligne constitue une activité n'ayant fait l'objet d'aucune définition légale ou réglementaire de portée générale. Les définitions existantes font systématiquement référence, soit à un domaine défini n'intégrant pas le commerce en ligne<sup>141</sup>, soit pour ce canal, à un domaine particulier d'application<sup>142</sup>.

La doctrine française a néanmoins tenté de définir l'activité de courtage par rapport à d'autres concepts juridiques connus. Ainsi, MM. Jauffret et Mestre ont pu préciser que « le courtage se distingue nettement de la commission en ce qu'il n'est pas une variété de mandat. Le courtier ne conclut pas le contrat pour le compte du commettant. Il se borne à rechercher, pour son client (dénommé donneur d'ordres), un cocontractant, à préparer la conclusion du contrat en s'efforçant de rapprocher les parties pour les amener à un accord, mais laisse ensuite les parties conclure le contrat elles-mêmes<sup>143</sup> ».

De même, M<sup>me</sup> Dekeuwer-Defossez estime que « le courtier est un commerçant indépendant qui met en relation deux personnes désireuses de contracter. Il n'est le mandataire ni de l'un ni de l'autre. Son activité n'est réglementée par aucun texte relatif au courtage en général<sup>144</sup> ».

En pratique, le courtage est donc « un contrat par lequel le courtier est chargé, moyennant une rémunération, soit d'indiquer à l'autre partie l'occasion de conclure

---

140. Pour de plus amples développements sur ce point, voir « Le courtage en ligne de biens culturels », Recommandation du Forum des droits sur l'internet, 22 juillet 2004. <http://www.foruminternet.org/recommandations/lire.phtml?id=756>

141. Voir à ce titre, l'article L. 131-1 du Code du commerce qui dispose que « il y a des courtiers de marchandises, des courtiers interprètes et conducteurs de navires, des courtiers de transport par terre et par eau » ou les articles L. 530-1 du Code des assurances relatifs au courtage d'assurances.

142. Voir à ce titre, l'article L. 321-3 du Code du commerce concernant le courtage en ligne, sous forme d'enchères, de biens culturels.

143. Alfred Jauffret et Jacques Mestre, *Manuel de droit commercial*, 23<sup>e</sup> édition, LGDJ, Paris, 1997, p. 53.

144. Françoise Dekeuwer-defossez, *Droit Commercial*, 7<sup>e</sup> édition, Domat, Montchrestien, 2001.

*une convention [activité de mise en relation], soit de lui servir d'intermédiaire pour la négociation d'un contrat*<sup>145</sup>».

Derrière cette définition générique se cachent de multiples formes. Ainsi, le courtage sur l'internet pourra être à prix fixe (principe de l'achat immédiat réalisé avec l'aide d'un tiers), sous forme d'enchère (où le prix est fixé à la suite d'un processus d'enchères) voire d'enchères inversées (dans le secteur des relations BtoB).

## Le régime de responsabilité des plates-formes de mise en relation

Dans le cadre de leur activité de mise en relation d'un vendeur avec un acheteur, les plates-formes sont susceptibles d'encourir deux types de responsabilité : une responsabilité du site suite à la mise en ligne par le vendeur d'une annonce de nature illicite et une responsabilité du site en cas de difficultés rencontrées par le vendeur ou l'acheteur lors de l'exécution du contrat conclu entre eux.

À titre préalable, il faut préciser qu'il n'est pas possible d'opérer une transposition pure et simple du régime de responsabilité applicable aux journaux de petites annonces. En effet, à l'inverse de ce canal ayant recours au papier, les plates-formes de mise en relation fournissent aux utilisateurs non seulement de l'information mais aussi un service permettant la conclusion en ligne d'un contrat de vente. Ces sites jouent donc un rôle dans la relation contractuelle qui s'éloigne du strict rôle d'éditeur que peuvent avoir les journaux de petites annonces.

### **La responsabilité du fait du contenu des annonces**

En matière de contenu diffusé sur l'internet, deux régimes de responsabilité distincts sont présents au sein du droit français : le régime de l'éditeur et celui de l'hébergeur. Alors que le premier est pleinement responsable de l'ensemble des contenus qu'il diffuse, le second bénéficie d'un régime aménagé en raison de son rôle de prestataire technique. Il convient donc de s'interroger sur la qualification à donner aux plates-formes de mise en relation.

Aux termes de l'article 14 de la directive du 8 juin 2000 : *«Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que : a) le prestataire n'ait pas effectivement connaissance de l'activité ou de l'information illicites et, en ce qui concerne une demande en dommages et intérêts, n'ait pas connaissance de faits ou de circonstances selon lesquels l'activité ou l'information illicite est apparente ou b) le prestataire, dès le moment où il a de telles*

---

145. Éric Barbry et Sophie Pradere, Le courtage aux enchères menacé, *Gaz. Pal.* 24 avril 2003, n° 114, p.29.

*connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible*»<sup>146</sup>.

Ce texte a été transposé aux articles 6-I-2 et 6-I-3 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique. Le premier précise que «*les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible*». Une rédaction quasiment analogue est prévue à l'article 6-I-3 qui estime que «*Les personnes visées au 2 ne peuvent voir leur responsabilité pénale engagée à raison des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de l'activité ou de l'information illicites ou si, dès le moment où elles en ont eu connaissance, elles ont agi promptement pour retirer ces informations ou en rendre l'accès impossible*».

Au cours des débats parlementaires sur le projet de loi pour la confiance dans l'économie numérique<sup>147</sup>, les parlementaires ont souhaité intégrer le courtage en ligne dans le domaine de l'hébergement: «*La définition des opérateurs visés par l'article ne fait pas de distinction: sont concernés tous les intermédiaires dont l'activité consiste à stocker durablement des données (stockage «permanent»), sans intervenir sur leur contenu (stockage «direct»), de façon à les rendre accessible au public au moyen d'un service de communication publique en ligne. Peu importe qu'il s'agisse d'informations fournies par des éditeurs de professionnels de sites, par des utilisateurs de places de marché ou de sites d'enchères en ligne, ou encore par des contributeurs à un forum. L'article n'entre pas dans ce détail des auteurs et de contenus, de même qu'il n'utilise pas, volontairement, le terme «d'hébergeur», aujourd'hui trop caractérisé.*»

Cette orientation a été suivie par la jurisprudence étrangère<sup>148</sup> qui a estimé que *l'activité de courtage en ligne* telle que pratiquée par les sociétés présentes sur le marché français relève de la qualification d'hébergeur et bénéficie du régime de

---

146. Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur

147. Michèle Tabarot, député, Avis n° 608 présenté au nom de la Commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur le projet de loi confiance dans l'économie numérique le 11 février 2003, JOAN.

148. Dans un courrier de la Direction générale 'Marché Intérieur' de la Commission européenne adressé à l'Association européenne des fournisseurs de service Internet, Margot Froehlinger indiquait: «*je peux vous assurer que les dispositions de l'article 14 ne se limitent pas à un type spécifique d'hébergement. L'article 14 ne fait pas de distinctions sur les types d'information hébergées ainsi que sur l'activité elle-même*». Les juges américains confirment également cette interprétation en faisant bénéficier la société eBay du régime dérogatoire prévu au sein du *Communications Decency Act* (*Superior court of the State of California for the county of Los Angeles*, 28 avril 2003, R. Grace c/ T. Neely et Société eBay, *Com. com. élec.* Juin 2003, comm. n° 61, note Luc Grynbaum).

responsabilité ainsi aménagé par la loi. La responsabilité de la société de courtage ne pourra, dès lors, être engagée que si celle-ci, ayant connaissance de l'activité illicite, laisse perdurer cette activité<sup>149</sup>. Certaines décisions françaises<sup>150</sup> ont adopté ce point de vue précisant également que le régime de responsabilité aménagé n'a pas vocation à s'appliquer dès lors que le courtier est lui-même partie prenante à l'activité illicite<sup>151</sup>, par exemple en créant des rubriques incitant à la vente d'objets interdits sur le territoire français. L'activité illicite pourra également consister en la mise en ligne, par le vendeur ou l'acheteur, de propos diffamatoires ou injurieux. Leur responsabilité pourra également être recherchée pour avoir laissé perdurer, en connaissance de cause, des contenus manifestement illicites dont la nature même, telle que décrite dans l'annonce est suffisante en soi pour établir le caractère illicite, sans nécessiter d'informations, d'hypothèses ou de vérifications supplémentaires.

La question de la responsabilité du fait du contenu des annonces rencontre une difficulté supplémentaire en matière de droit de la consommation. En effet, le Code de la consommation – et en particulier son article L. 121-18 – punit l'absence de diffusion de certaines informations au sein de l'offre. Une offre se définit comme «*une proposition qui comporte tous les éléments du contrat projeté. L'offre exprime déjà le consentement de son auteur: il faut donc qu'elle soit assez précise et complète pour pouvoir être acceptée telle quelle et que le contrat en découle*». En matière de commerce électronique, **l'offre est constituée non seulement des éléments de l'annonce**

---

149. À ce propos, voir la décision 2004-496 DC du Conseil constitutionnel du 10 juin 2004 qui a pu juger que «*Ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge*».

150. TGI Paris, 11 février 2003, n° 104305259, Amicale des déportés d'Auschwitz et des camps de Haute Silésie c/ Timothy Koogle, D. 2003, inf. rap., p. 603, *Legipresse*, 2003, n° 202, III, p. 93, note Jean-Philippe Hugot. Le tribunal jugeait à propos du service de courtage en ligne proposé par Yahoo! que cela constitue une activité d'hébergement dès lors qu'elle «*stocke, pour leur mise à disposition du public, les annonces rédigées par les vendeurs d'objets et justifie d'ailleurs, de ce qu'elle conserve et détient les données de nature à permettre l'identification de ces créateurs de contenu, conformément aux dispositions de l'article 43-9 de la loi du 30 septembre 1986*». Voir également TGI Paris, 26 octobre 2004, SA Poiray France et M<sup>me</sup> Nathalie C. c/ SARL CJSF, Ophélie, Ibazar et SA eBay France. Le tribunal a pu estimer à propos du site eBay que «*les offres de vente n'ont pas été apportées par la société eBay qui définit et fournit des pages préformatées permettant aux utilisateurs de déposer leurs offres de vente et d'enchérir (...) que le processus des enchères s'effectue grâce à la mise à disposition des utilisateurs d'un logiciel dans l'exécution duquel la société eBay n'a aucun autre rôle que celui d'exécutant technique (...) Dans ces conditions, faute pour la société eBay de participer autrement que par une activité de courtage à l'offre en vente et à la vente du modèle de bijou contrefaisant, le grief de contrefaçon formulé à son encontre n'est pas fondé*».

151. En cela, suivons l'interprétation donnée par TGI Paris, 11 février 2003, n° 0104305259, Amicale des déportés d'Auschwitz et des camps de Haute Silésie c/ Timothy Koogle, préc.. Les juges ont considéré que Yahoo! était responsable, en sa qualité d'éditeur du service, «*des sélections d'annonces ou de catégories qu'elle offre plus particulièrement à l'attention des acheteurs sur la page d'accueil du site*». Ainsi, «*Les dispositions de l'article 43-8 [de la loi de 1986] ne sont pas susceptibles d'être invoquées par le prévenu si sa responsabilité est recherchée au titre de l'activité d'éditeur de service de communication en ligne de la société YAHOO INC, ce qui est le cas, en l'espèce, la citation visant, notamment, le fait d'avoir délibérément maintenu une rubrique préalablement fixée de vente aux enchères d'objets nazis», ce qui renvoie, sans aucun doute, à l'architecture du site, soit à un contenu créé par l'éditeur*».

**(photographie, descriptif), mais également des pages accessibles à partir de celle-ci** (conditions générales de vente, etc.).

L'absence, en phase précontractuelle, d'une des mentions imposées par le Code de la consommation, soit dans les annonces, soit dans les pages annexes, aurait pour effet de vicier l'offre dans son intégralité et donc de rendre illicite les contenus hébergés. Pour autant, la responsabilité du courtier ne pourrait être retenue dès lors que ces contenus ne peuvent être qualifiés de «manifestement illicites»<sup>152</sup> au regard des dispositions de la loi pour la confiance dans l'économie numérique telles qu'interprétées par le Conseil constitutionnel. En effet, selon une explication de la réserve d'interprétation livrée lors de la conférence de presse du Conseil constitutionnel, le caractère manifestement illicite d'un contenu doit rester limité aux messages incitant à la haine raciale et aux images pédo-pornographiques<sup>153</sup>.

L'acquisition de la connaissance de l'existence de ces messages ne saurait se faire cependant au travers d'une surveillance générale de l'ensemble des annonces publiées, l'article 15 de la directive du 8 juin 2000 précisant que «*les États membres ne doivent pas imposer aux prestataires [...] une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites*». Ce principe a été transposé à l'article 6-1-7 qui énonce que les hébergeurs «*ne sont pas soumis à une obligation générale de surveiller les informations qu'[ils] transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites*».

Une analyse analogue peut être réalisée en matière de régime de responsabilité applicable aux *plates-formes agissant comme mandataire du vendeur*. En effet, malgré l'existence du mandat, leur activité consiste, vis-à-vis du contenu des annonces, à «*stocker durablement des données (stockage «permanent»), sans intervenir sur leur contenu (stockage «direct»), de façon à les rendre accessible au public au moyen d'un service de communication publique en ligne*». Dans ces conditions, ces sites ne pourraient voir leur responsabilité engagée du fait du contenu hébergé que dans les conditions énumérées aux articles 6-1-2 et 6-1-3 de la loi du 21 juin 2004.

**Cette application du régime de responsabilité de l'hébergeur à l'ensemble des plates-formes de mise en relation a déjà été appliquée par la jurisprudence (voir supra)**. Il convient cependant de préciser que l'article 6-1-2 alinéa 2 prévoit une dérogation «*lorsque le destinataire du service agit sous l'autorité ou le contrôle de la personne visée audit alinéa*». Une divergence existe selon la doctrine sur l'interprétation de ces notions. Pour certains, «*si l'on reprend les travaux parlementaires, on*

---

152. Lionel Thoumyre, «Les hébergeurs en ombres chinoises – Une tentative d'éclaircissement sur les incertitudes de la LCEN», *RLDI*, mai 2005, p.58. Dans cet article, l'auteur précise que l'expression «*manifestement illicite*» viseraient «*principalement les contenus d'une gravité avérée et dont le caractère illicite ne semble pas discutable. Il s'agit, par exemple, des contenus à caractère pédopornographique, des écrits faisant l'apologie des crimes de guerre ou qui provoquent directement aux actes de terrorisme. En revanche, les cas de diffamation classique (...) ne semblent pas pouvoir relever*» de cette notion.

153. Estelle Dumout, Jérôme Thorel, «LCEN : le Conseil constitutionnel censure l'amendement Devedjian», Paris, *ZDNet France*, 15 juin 2004.

se rend compte que cette disposition est censée écarter «du bénéfice aménagé de responsabilité des hébergeurs les prestataires exerçant des activités d'intermédiation». Ces prestataires seraient ceux qui ont un rôle actif d'animation commerciale du site tels que les sociétés de courtage en ligne »<sup>154</sup>. Pour d'autres et «selon la Commission européenne, le terme «contrôle» fait référence au «contrôle des activités et non à celui des informations elles-mêmes» »<sup>155</sup> justifiant l'application du régime de responsabilité aménagé aux plates-formes de mises en relation.

S'appuyant sur cette interprétation communautaire, et sur la jurisprudence, **le Forum des droits sur l'internet recommande de soumettre les plates-formes de mise en relation au régime de responsabilité de l'hébergeur prévu par les dispositions des articles 6-I-1 et suivants de la loi pour la confiance dans l'économie numérique.**

**Dès lors, les éventuelles infractions par les vendeurs au non-respect des mentions légales, telles que celles mentionnées ci après, relèveraient de ce régime de responsabilité, nonobstant l'application du régime de responsabilité prévu par le droit de la consommation, qui reste applicable aux vendeurs.**

Enfin, il convient de rappeler qu'en leur qualité d'hébergeur, ces plates-formes sont tenues en application de l'article 6-I-7 de «mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance » certaines infractions énumérées au second alinéa de cet article<sup>156</sup>. **Le Forum recommande que cet outil de notification puisse également permettre aux internautes d'exercer leur vigilance sur tout type d'articles pouvant être mis en vente illégalement et de les notifier à la plate forme pour retrait éventuel des annonces correspondantes.**

## **La responsabilité de la plate-forme du fait d'une inexécution du contrat conclu entre ses utilisateurs**

Un second cas d'engagement de la responsabilité de la plate-forme doit être envisagé: celui lié à une inexécution par l'un ou l'autre des utilisateurs du contrat conclu par son intermédiaire. Il s'agit, par exemple, du régime applicable en l'absence de paiement du bien par l'acheteur ou à défaut de livraison de celui-ci par le vendeur.

S'agissant de la responsabilité du **courtier en ligne**, dans la mesure où le contrat de vente du bien est conclu directement entre l'acheteur et le vendeur, «en dehors» de la plate-forme de courtage, il semble difficile d'invoquer la mise en cause de la responsabilité contractuelle de cette dernière dans la mesure où elle n'est pas partie à ce contrat et ne garantit pas, par ailleurs, la bonne fin de son exécution. Sa **responsabilité contractuelle** ne pourrait être recherchée que si le courtier en ligne n'exécutait

---

154. Éric Caprioli, «La confiance dans l'économie numérique», *LPA* 3 juin 2005, p.5.

155. «Loi pour la confiance dans l'économie numérique, un nouveau cadre juridique pour l'internet», dossier du Forum des droits sur l'internet, 15 juin 2004.<http://www.foruminternet.org/publications/lire.phtml?id=734>

156. Il s'agit des infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et à l'article 227-23 du Code pénal.

pas, vis-à-vis de l'un de ses utilisateurs, l'une des obligations issues du contrat de fourniture de service conclu avec ceux-ci. À ce titre, il faut rappeler que la plate-forme est, en application de l'article 15 de la loi pour la confiance dans l'économie numérique, responsable de plein droit de la bonne exécution des obligations issues du contrat conclu avec ses utilisateurs, à savoir le contrat de fourniture du service (accès et utilisation de la plate forme). Par contre, la responsabilité de plein droit de la plate forme n'a pas vocation à s'étendre aux contrats de vente conclus directement entre les utilisateurs. Enfin, **sa responsabilité civile pourra être engagée, sous réserve d'apporter la preuve d'une faute commise par celle-ci**, dès lors qu'elle demeure tiers au contrat conclu entre ses utilisateurs.

S'agissant de la responsabilité du **mandataire** du fait d'une mauvaise exécution du contrat par le mandant ou par le cocontractant qu'il a présenté à son mandant, ce régime est visé par plusieurs dispositions du Code civil. Ainsi, l'article 1991 énonce que le mandataire «*est tenu d'accomplir le mandat tant qu'il en demeure chargé, et répond des dommages-intérêts qui pourraient résulter de son inexécution*», l'article 1992 poursuivant en indiquant que «*le mandataire répond non seulement du dol, mais encore des fautes qu'il commet dans sa gestion*». Cette responsabilité, précise le second alinéa de cet article, «*est appliquée moins rigoureusement à celui dont le mandat est gratuit qu'à celui qui reçoit un salaire*».

En pratique, le site mandataire ne répond pas d'une bonne ou mauvaise exécution du contrat par l'une ou l'autre des parties à celui-ci<sup>157</sup> dès lors que le contrat conclu entre le mandant et son cocontractant «*ne produit en principe aucun effet à l'égard du mandataire*»<sup>158</sup>.

Néanmoins, sa responsabilité pourrait être recherchée dans deux situations. Il pourrait voir sa responsabilité contractuelle engagée vis-à-vis du mandant en cas d'inexécution des obligations, souvent inhérentes au contrat de mandat (manquement à son obligation de conseil et d'information, etc.). Sa responsabilité civile pourrait être invoquée, vis-à-vis du cocontractant du mandant, pour ses agissements fautifs. Il serait personnellement responsable envers les tiers des délits ou quasi-délits qu'il pourrait commettre à leur préjudice dans l'accomplissement de sa mission<sup>159</sup>. Tel serait le cas, par exemple, de l'incrimination de recel de biens d'origine frauduleuse<sup>160</sup> qui, si elle n'implique pas nécessairement la détention matérielle des biens, nécessite que le mandataire ait eu connaissance de l'origine frauduleuse des biens dont il assurait la vente.

---

157. Civ. 1, 14 novembre 1978, *Bull. civ. I*, n° 346; Civ. 1, 4 mars 1986, *D.* 1986, IR. 168.

158. Alain Benabent, *Droit Civil – les contrats spéciaux civils et commerciaux*, 6<sup>e</sup> éd., MontChrestien, p.438.

159. Civ. 3, 6 janvier 1999, *Bill. civ. III*, n° 3; *D.* 2000, p. 426, note C. Asfar.

160. Crim., 30 novembre 1999, *Bull. crim.*, n° 282.

## Conclusion

En conclusion, les plates-formes de courtage en ligne et les plates-formes mandataires obéissent à deux régimes distincts de responsabilité.

**La plate-forme mandataire** sera responsable, au nom et pour le compte du vendeur, de la bonne exécution des obligations mises à la charge de celui-ci dans le cadre du contrat de mandat (perception du paiement, exercice du droit de retour, etc.).

Elle sera en outre tenue, en application du contrat de mandat, à un devoir de conseil et d'information vis-à-vis de son mandant sur ces questions.

Vis-à-vis de l'acheteur, la plate-forme sera responsable civilement ou pénalement des fautes qu'elle pourrait commettre. De même, sa responsabilité pourra être retenue si, ayant eu connaissance d'un contenu manifestement illicite, elle n'a pas procédé à son retrait ou à sa suspension.

Concernant le courtier en ligne, sa responsabilité civile ou pénale pourrait être engagée, vis-à-vis de l'acheteur, si une faute est démontrée (cas de la vente d'un bien recelé en toute connaissance de cause, etc.). De même, sa responsabilité pourra être retenue si, ayant eu connaissance d'un contenu manifestement illicite, elle n'a pas procédé à son retrait ou à sa suspension.

Vis-à-vis du vendeur, sa responsabilité contractuelle de plein droit pourrait être engagée en cas de mauvaise exécution du contrat de prestation de service portant sur la fourniture d'un outil de mise en relation de deux internautes.

Enfin, et comme tout professionnel, le courtier en ligne – qui est lié contractuellement aux utilisateurs de la plate-forme, est soumis à une obligation d'information à destination de l'acheteur et du vendeur. Sa responsabilité contractuelle peut donc être retenue à ce titre.

## Les principaux acteurs de la mise en relation

### Un exemple de mandataire : Priceminister

La société Priceminister a été fondée par 5 Français en août 2000. Le site, ouvert en janvier 2001, connaît depuis une forte croissance en termes de volume et de nombre de transactions. À la fin du mois d'août 2004, le site comptait plus de 2 millions de membres et 7 millions de produits en vente à chaque instant.

Les produits mis en vente par les internautes sont variés : produits culturels, high-tech, électroménager, voitures. Un service « voyage en ligne » est disponible mais est géré en partenariat avec une agence de voyages. Le site s'adresse essentiellement à des internautes situés en Europe francophone.

Deux particularités doivent être relevées en matière de fonctionnement de la plate-forme :

– une base de données « produits » intégrant différentes informations (prix, description, image, etc.) permet de préremplir les offres émises par les vendeurs, ces derniers conservant la faculté d'ajouter des commentaires complémentaires ;



–un système d'intermédiation de paiement est intégré: l'acheteur verse l'argent à Priceminister, qui contractuellement a reçu mandat de la part du vendeur pour percevoir cette somme. Celui-ci ensuite le reverse au vendeur dès qu'il reçoit la confirmation de la réception du bien. Pour mener à bien ce mécanisme, il existe un compte de séquestre différent de celui de l'entreprise.

### **Le processus de transaction**

L'acheteur sélectionne un produit et paye sa commande directement sur la plateforme de paiement sécurisé de PriceMinister. Le vendeur dispose alors d'un délai de trois jours ouvrables pour confirmer la vente (cas du vendeur en vacances, PC en panne, vente de l'objet par un autre canal). Si le vendeur ne confirme pas, la vente est annulée et l'acheteur n'est pas débité. À l'inverse, si le vendeur confirme l'envoi, il doit adresser le bien sous 48 heures, tandis que l'acheteur est débité du montant.

Ensuite, à réception du bien, l'acheteur doit confirmer celle-ci afin de déclencher le paiement au vendeur. En tout état de cause, une confirmation tacite est appliquée à l'expiration d'un délai de trente jours.

L'acheteur a la possibilité de payer par carte bancaire ou par chèque. Pour le paiement, par chèque, il doit néanmoins passer par l'intermédiaire d'un «porte-monnaie» électronique associé à son compte utilisateur.

### **Le rôle de Priceminister**

Tout vendeur utilisant le service donne mandat à PriceMinister d'organiser la mise en ligne des annonces et la collecte du paiement, et accepte son arbitrage en cas de litige. À ce titre, PriceMinister assure plusieurs rôles. Il reçoit le paiement, au nom et pour le compte du vendeur, et, à ce titre, est tiers de confiance dans la transaction. Par ailleurs, il gère un premier niveau de service client. En effet, en cas d'insatisfaction, l'acheteur doit s'adresser directement à PriceMinister qui peut, dans certaines situations, procéder au remboursement de la transaction (rétractation, article non reçu ou non conforme).

Le fait que PriceMinister combine les rôles d'intermédiaire de paiement et de tiers de confiance semble constituer un facteur de prévention important. En effet, les acheteurs sont protégés contre les éventuelles escroqueries puisque les vendeurs sont payés après confirmation par l'acheteur (au plus tard, un mois après la date de commande) tandis que les vendeurs sont garantis contre les faux acheteurs et les risques d'impayés, ceux-ci étant pris en charge intégralement par PriceMinister.

### **Les utilisateurs de la plate-forme**

Lors de la création du site, la majorité des vendeurs étaient des professionnels qui avaient été sollicités préalablement à l'ouverture du service pour se voir proposer la mise en vente de leurs produits via la plate-forme. Avec l'arrivée massive d'utilisateurs particuliers, la part des professionnels atteint dorénavant 25 à 35% en valeur. Les utilisateurs de la plate-forme ont donc le profil suivant :

- les professionnels faisant du déstockage massif sur de gros volumes ;
- les particuliers faisant des ventes portant sur des biens en très faible quantité.

Les acheteurs peuvent accéder à diverses informations concernant un offreur déterminé. Elles concernent notamment son pseudonyme, le nombre de ventes déjà réalisées, la notation moyenne attribuée par ses précédents cocontractants, sa date d'inscription.

Afin de compléter les informations mises en ligne par le vendeur dans son annonce, Priceminister propose à ses utilisateurs un outil de dialogue. Un internaute peut ainsi poser une question à l'offreur. Celle-ci, ainsi que la réponse apportée, seront accessibles à tous les utilisateurs. Un filtrage a néanmoins été mis en place afin, par exemple, de ne pas permettre de négociation directe sur les prix, de ne pas fournir des coordonnées téléphoniques ou une adresse de courriel.

Lors de leur inscription, les professionnels – qui se déclarent comme tels – doivent répondre à des questions complémentaires destinées, en particulier, à leur proposer des outils spécifiques (possibilité d'automatiser l'ajout de nouveaux produits dans sa «boutique», etc.). D'ailleurs, si un vendeur connaît un volume d'activité important, Priceminister prendra contact avec celui-ci afin de lui proposer lesdits outils.

## **Un exemple de courtier en ligne : eBay**

eBay a été créé en 1995 par un Américain d'origine française. Ce service compte 157 millions d'utilisateurs inscrits, est disponible sur 33 sites à travers le monde où sont accessibles, à chaque instant, 50 millions d'objets mis en vente. eBay enregistre quotidiennement 5 millions de nouveaux objets (chiffres avril 2005).

### **Le processus de transaction**

Pour publier une annonce sur eBay, un vendeur est appelé à remplir un formulaire de mise en vente au sein duquel il donnera une description complète de son bien. Il indique une durée de l'annonce et choisit le mode de fixation du prix de vente (vente à prix fixe ou sous forme d'enchères). La plate-forme ne pratique aucune intervention ou contrôle éditorial de l'annonce mise en ligne.

Pour certaines catégories de biens (CD, DVD), une base de données intégrant différentes informations sur ces produits (les cas échéant : artiste, auteur, description, etc.) permet de préremplir les offres émises par les vendeurs, ces derniers conservant la faculté de modifier ou d'ajouter des commentaires complémentaires. Ces annonces «préremplies» apparaissent à partir de la simple indication du code barre de l'objet. Pour les produits culturels et technologiques, les vendeurs peuvent indiquer des attributs complémentaires destinés à préciser l'état du bien. Ces outils permettent ainsi d'avoir une standardisation dans la présentation de l'offre et une amélioration de la pertinence des résultats proposés par le moteur de recherche.

En outre, un champ du formulaire permet aux vendeurs d'indiquer leur politique de retour (existence d'un droit de rétractation, etc.) et leurs conditions générales de vente.

Enfin, eBay a récemment mis en place une nouvelle fonctionnalité permettant aux vendeurs inscrits à titre professionnel de créer, depuis la section du site Mon eBay, une rubrique d'information pouvant être automatiquement insérée dans leurs

annonces. Ce modèle leur permet d'indiquer les informations requises par la loi, relatives à leur identité et à leurs conditions de vente.

Ces informations sont complétées, pendant la durée de la transaction, par les questions posées aux vendeurs par les internautes. Celles-ci, ainsi que les réponses apportées, peuvent être accessibles en marge de l'annonce, si le vendeur le décide.

En tout état de cause, les vendeurs ont un double intérêt à diffuser un grand nombre d'informations sur la vente. En effet, pour un même produit, une comparaison entre différents vendeurs est toujours possible; un consommateur préférant naturellement conclure avec un vendeur diffusant le maximum d'information. Par ailleurs, dès lors que la mise en vente est facturée par des frais d'insertion, un vendeur prendra un soin important à la rédaction de son offre.

Enfin, un dernier élément permet à un utilisateur de pouvoir identifier le meilleur cocontractant. Le site a, en effet, développé un mécanisme d'évaluation réciproque des parties à l'issue de la transaction. Le vendeur attribuera une évaluation accompagnée d'un commentaire sur la transaction à l'acquéreur et réciproquement (-1 : non satisfait, 0 : neutre ; 1 : parfait). L'historique des évaluations des utilisateurs est ensuite accessible à tous les internautes.

### **Le rôle d'eBay**

L'intégralité de la mise en relation du vendeur et de l'acheteur s'opère par l'intermédiaire de la plate forme technique eBay. Le contrat de vente est ensuite conclu de gré à gré entre acheteur et vendeur, y compris pour les modalités relatives au transport et au paiement.

eBay propose, sous certaines conditions, une procédure d'indemnisation de l'acheteur dans un délai de 90 jours suivant la fin de la transaction. Cette indemnisation est plafonnée à un montant de 230 euros (avec des frais de dossier de 28€). Au-delà de ce montant, eBay recommande le recours aux services d'un tiers de confiance (service fourni par la société TripleDeal).

### **Les utilisateurs de la plate-forme**

Lors de l'inscription, eBay propose deux formulaires distincts à ses utilisateurs. Le premier s'adresse aux particuliers tandis que le second est destiné aux professionnels qui doivent communiquer des informations complémentaires (numéro de TVA intracommunautaire, etc.). Une vérification des vendeurs peut ensuite être opérée. Ceux-ci devront communiquer, soit un numéro de carte bancaire, soit une adresse postale à laquelle sera adressé un code d'activation de leur compte.

Il convient de noter qu'eBay a récemment mis en place une nouvelle fonctionnalité permettant l'identification des vendeurs professionnels. Ainsi, toute personne s'inscrivant à titre professionnel sur le site sera automatiquement identifiée comme tel dans ses annonces.

Par ailleurs, le site a mis en ligne des pages «entreprendre sur eBay» rappelant aux professionnels leurs principales obligations légales et détaillant les outils marketing proposés. Complétant ce dispositif d'information, eBay adresse aux vendeurs ayant

une activité importante des avertissements dans la plupart des messages envoyés à l'issue de chaque transaction. Cette alerte est destinée à attirer l'attention des vendeurs sur le fait qu'il pourrait être qualifié juridiquement de professionnel de la vente à distance et ainsi être soumis à des obligations, notamment fiscales et sociales, complémentaires.

Enfin, chaque utilisateur bénéficie d'outils supplémentaires :

–des « pages perso » : il s'agit d'un espace vierge où l'utilisateur peut s'identifier et indiquer ses conditions générales de vente ;

–des « boutiques » : il s'agit d'un espace plus complet, payant (5 à 50 € par mois) s'adressant à des vendeurs importants. Cet outil n'est pas réservé aux professionnels, les particuliers pouvant aussi en bénéficier.

## **Le régime juridique de la vente par un particulier sur l'internet**

Toute vente, réalisée à distance depuis la France, est soumise à un régime juridique fixé par plusieurs textes : les dispositions générales du Code civil sur le droit des contrats, celles du Code de la consommation en matière de vente à distance, la loi du 21 juin 2004 pour la confiance dans l'économie numérique applicable aux contrats conclus par voie électronique, les arrêtés de 1987 sur les prix.

Certaines règles viennent en outre régir spécifiquement les contrats conclus entre un vendeur professionnel et un acheteur non professionnel. Prévues par le Code de la consommation, elles visent à rééquilibrer la relation contractuelle qui se noue entre un vendeur, informé et spécialiste de sa matière, et un consommateur, partie faible au contrat.

Dans le cadre de la présente analyse, une distinction doit donc être réalisée, en matière de commerce électronique, entre les règles applicables à tout vendeur et les dispositions encadrant spécifiquement les contrats conclus par un professionnel de la vente à distance.

### **Les règles applicables à tout vendeur sur l'internet**

Trois étapes successives doivent être distinguées : la période précontractuelle au cours de laquelle le vendeur est soumis à certains devoirs notamment d'information, la période contractuelle qui a été formalisée par la loi pour la confiance dans l'économie numérique et, enfin, la période postérieure à la formation du contrat qui soumet les vendeurs à certaines obligations vis-à-vis des acheteurs.

### **L'information précontractuelle des acheteurs**

Les textes actuellement applicables à tout vendeur lui imposent une obligation d'information. Celle-ci peut être sanctionnée soit, au niveau pénal, lorsqu'une infraction est prévue par le Code de la consommation ou le Code pénal soit, d'un point de vue civil, par l'allocation de dommages et intérêts ou par le prononcé de la nullité du contrat.

**L'information sur l'identité du vendeur  
(nom, adresse, numéro de téléphone, adresse email)**

L'obligation d'information sur l'identité du vendeur est fixée par deux textes. L'article L.121-18 du Code de la consommation énonce que *« l'offre de contrat doit comporter les informations suivantes : 1° Le nom du vendeur du produit ou du prestataire de service, son numéro de téléphone, son adresse ou, s'il s'agit d'une personne morale, son siège social et, si elle est différente, l'adresse de l'établissement responsable de l'offre »*.

Ce principe a été complété par l'article 19 de la loi pour la confiance dans l'économie numérique qui prévoit, sans préjudice des autres obligations d'information prévues par les textes législatifs et réglementaires en vigueur, que *« toute personne qui exerce l'activité définie à l'article 14 [de la LCEN] est tenue d'assurer à ceux à qui est destinée la fourniture de biens ou la prestation de services un accès facile, direct et permanent utilisant un standard ouvert aux informations suivantes :*

- 1) *« S'il s'agit d'une personne physique, ses nom et prénoms et, s'il s'agit d'une personne morale, sa raison sociale ;*
- 2) *« L'adresse où elle est établie, son adresse de courrier électronique, ainsi que son numéro de téléphone ;*
- 3) *« Si elle est assujettie aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de son inscription, son capital social et l'adresse de son siège social ;*
- 4) *« Si elle est assujettie à la taxe sur la valeur ajoutée et identifiée par un numéro individuel en application de l'article 286 ter du code général des impôts, son numéro individuel d'identification ;*
- 5) *« Si son activité est soumise à un régime d'autorisation, le nom et l'adresse de l'autorité ayant délivré celle-ci ;*
- 6) *« Si elle est membre d'une profession réglementée, la référence aux règles professionnelles applicables, son titre professionnel, l'État membre dans lequel il a été octroyé ainsi que le nom de l'ordre ou de l'organisme professionnel auprès duquel elle est inscrite »*.

Alors que l'article L. 121-18 du Code de la consommation ne régit que les offres émanant d'un vendeur professionnel à destination de consommateurs, les dispositions de l'article 19 de la loi pour la confiance dans l'économie numérique, visant *« tout vendeur pratiquant une activité de commerce électronique »*, incluent les vendeurs exerçant cette activité à titre non professionnel.

Cette obligation d'information remplit plusieurs objectifs. Tout d'abord, elle permet au consommateur de connaître précisément l'identité du vendeur, et notamment sa nature juridique (entreprise, particulier).

En outre, l'indication du domicile du vendeur est importante dans le cadre des relations commerciales entre deux particuliers non professionnels. En effet, la loi applicable au contrat sera alors celle du pays du vendeur et non pas de l'acheteur<sup>161</sup>.

---

161. La loi du pays de l'acheteur sera applicable aux contrats conclus entre un vendeur professionnel et un consommateur, quelque soit la localisation géographique du vendeur.

Enfin, la mention du numéro d'inscription au registre du commerce et des sociétés ou au répertoire des métiers est destinée à offrir au consommateur un moyen de vérifier si son futur cocontractant professionnel ne fait pas l'objet d'une procédure collective (redressement, liquidation judiciaire)<sup>162</sup>.

En tout état de cause, **le droit impose que ces informations soient accessibles aux acheteurs préalablement à la conclusion du contrat**, c'est-à-dire dans la phase précontractuelle.

#### ***La pratique actuelle des plates-formes***

Les principales plates-formes françaises interdisent contractuellement à tout vendeur, particulier ou professionnel, de s'identifier directement auprès de l'acheteur dans les annonces publiées sur le site. Celles-ci se présentent donc de façon anonymisée. Une telle stipulation du contrat est destinée à assurer la pérennité du modèle économique de l'intermédiation reposant principalement, non pas sur la perception de frais de mise en ligne (comme dans le cas de la publication de petites annonces), mais sur un pourcentage du montant de la transaction réalisée grâce à la mise à disposition de la plate-forme et du service.

Cependant, le vendeur demeure identifiable, plus ou moins facilement, par l'acheteur car :

- certains sites offrent, sous conditions, des espaces dédiés (rubrique « informations » pouvant être automatiquement insérée dans les annonces des vendeurs inscrits à titre professionnel, pages personnelles, boutiques virtuelles) où une identification complète du vendeur peut avoir lieu ;
- le vendeur est tenu de s'identifier auprès des plates-formes qui détiennent certains éléments soit au titre de leur activité d'hébergeur, soit en raison du contrat existant entre la plate-forme et ses utilisateurs ;
- dans le cadre du processus contractuel, l'acheteur peut, selon la pratique des plates-formes, **une fois le contrat conclu**, soit obtenir automatiquement l'identité du vendeur, soit s'adresser à la plate-forme qui alors s'engage à lui communiquer une telle information sur simple demande.

En tout état de cause et eu égard aux dispositions légales sus-rappelées, la plate-forme qui interdit à un vendeur professionnel de s'identifier avant la conclusion définitive du contrat est susceptible de voir sa responsabilité engagée. En effet, les juges pourraient retenir, au titre de la complicité, sa responsabilité pénale vis-à-vis de l'obligation posée par le Code de la consommation et sanctionnant le défaut d'information en la matière.

Afin de déterminer si une communication des coordonnées du vendeur a lieu en phase précontractuelle, une analyse du mode de conclusion du contrat par l'intermédiaire des principales plates-formes actuellement disponibles en France doit être réalisée.

---

162. Plusieurs sites consultables gratuitement permettent de rechercher certaines informations légales sur les sociétés.

### ***Les schémas contractuels de vente***<sup>163</sup>

La première difficulté en termes de modélisation du schéma contractuel conclu par l'intermédiaire des plates-formes tient à la diversité des pratiques des plates-formes et de leurs utilisateurs.

Concernant les plates-formes de courtage en ligne et notamment dans le schéma établi par eBay, un courriel automatique est adressé à l'acheteur lorsque le vendeur accepte l'offre (cas des ventes sous forme d'enchères) ou lorsque l'acheteur accepte l'offre initiale (cas des ventes à prix fixe). Ce courriel contient les coordonnées du vendeur avec lequel l'utilisateur va ou accepte de contracter.

Si le vendeur professionnel n'a pas au préalable respecté son obligation d'information en incluant toutes les mentions requises dans son annonce ou dans les autres espaces du site à sa disposition, deux situations devront donc être distinguées :

– si le vendeur annonce à l'acheteur, dans le courriel de confirmation, une condition supplémentaire à la conclusion du contrat (modalité de livraison, etc.), l'obligation d'information sera considérée comme respectée. En effet, le courriel délivrant également les éléments d'identification imposés par la loi, la fixation d'une nouvelle condition au contrat a pour effet de reporter sa conclusion à l'acceptation de ce nouvel élément par l'acheteur. Les informations exigées seront donc communiquées préalablement à la conclusion du contrat ;

– si, à l'inverse, le vendeur n'apporte aucune condition supplémentaire au contrat, le contrat sera considéré comme conclu dès le choix de l'acheteur par le vendeur. La communication des éléments d'identification dans le courriel de confirmation, adressé postérieurement à la conclusion du contrat, est donc tardive.

Concernant les plates-formes mandataires du vendeur, les obligations imposées en matière d'identification seront soit à la charge du vendeur, soit à la charge de la plate-forme si le mandat porte sur l'intégralité de la vente.

### ***Recommandations du Forum des droits sur l'internet en matière d'information précontractuelle sur l'identité du vendeur***

**Tout d'abord, et conformément aux dispositions en vigueur, le Forum des droits sur l'internet rappelle que tout vendeur est tenu de s'identifier clairement et précisément. Une telle information ne peut que faciliter le développement de la confiance des utilisateurs dans le commerce électronique.**

**Le Forum recommande aux plates-formes de prévoir dans le contrat qui les lie à leurs utilisateurs, une clause précisant que leurs utilisateurs s'engagent à ce que le contrat qui sera conclu entre eux par l'intermédiaire de la plate-forme le sera sous condition suspensive de révélation, par le vendeur, de ses coordonnées. L'absence d'indication des coordonnées du vendeur dans l'annonce pourra être jugée compatible avec les dispositions du Code de la consommation dès lors que la communication interviendra en phase précontractuelle. Enfin, en**

---

163. Voir Annexe 3.

### **l'absence de communication de ces éléments par le vendeur, le contrat de vente ne pourra connaître d'exécution.**

Si le vendeur a donné mandat à une plate-forme pour procéder à l'intégralité de la vente, il ne sera pas directement soumis à l'obligation d'identification. Il reviendra à la plate-forme de s'identifier elle-même auprès des acheteurs.

### **La vérification de l'identité des utilisateurs par la plate-forme**

Lors de l'inscription sur la plate-forme, les utilisateurs ne font pas l'objet systématiquement d'une vérification de leur identité. En effet, les formulaires proposés par les plates-formes demeurent déclaratifs et sont susceptibles d'être remplis de manière incomplète ou erronée par lesdits utilisateurs.

Or, il apparaît que les consommateurs attendent souvent de la plate-forme un certain contrôle des informations saisies par l'internaute afin de vérifier la validité et l'intégrité de ces informations, voire l'honnêteté de l'utilisateur.

Le droit français n'impose pas, à ce jour, aux sites d'identifier leurs utilisateurs<sup>164</sup>. En outre, si cette obligation leur était imposée, elle serait très difficile à réaliser compte tenu des informations en leur possession. Le processus d'inscription repose sur une communication volontaire d'informations par les internautes qui ne peuvent pas toutes faire l'objet d'une validation par l'intermédiaire de l'interrogation de bases de données existantes, pour des raisons tenant à l'application des principes issus de la loi du 6 janvier 1978 relative à l'informatique et aux libertés.

Pour remédier à cette carence, l'ensemble des plates-formes met en avant un mécanisme de notation consistant pour un acheteur à attribuer une évaluation et/ou un commentaire à son vendeur. Certaines plates-formes permettent également au vendeur d'évaluer l'acheteur. Mis en ligne, ces éléments permettent ainsi à un internaute de connaître les précédents avis des utilisateurs sur ce vendeur ou acheteur. Ce sont donc les internautes eux-mêmes qui construisent la confiance que l'on peut accorder à tel ou tel utilisateur compte tenu de l'historique de ses activités sur le site.

---

164. En leur qualité d'hébergeurs au sens de la loi pour la confiance dans l'économie numérique, les plates-formes sont tenues de détenir et conserver «*les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires*». À ce titre, il est intéressant de relever que le Tribunal de grande instance de Paris a retenu la responsabilité civile d'un hébergeur qui avait détenu et conservé des données d'identification farfelues (TGI Paris, 3<sup>e</sup> Ch., Section 1, 16 février 2005, Dargaud Lombard, Lucky Comics c/ Tiscali Media). *A contrario*, la même juridiction a pu estimer précédemment qu'un hébergeur n'était pas tenu à une telle vérification (TGI Paris, réf., 2 février 2004, Metrobus c/ Ouvaton). À noter qu'à l'occasion des débats parlementaires relatifs à la loi pour la confiance dans l'économie numérique, les parlementaires ont refusé d'imposer une obligation de vérification des données aux hébergeurs: «*La réserve est d'ordre juridique et tient à la compatibilité d'une telle obligation au regard des dispositions de la directive communautaire du 8 juin 2000. Celle-ci ne prévoit en effet aucune obligation de ce type à la charge des intermédiaires techniques de la société de l'information. Elle n'ouvre, par ailleurs, pas expressément aux États membres la faculté d'exiger la vérification de contenus*». in Alex Turk, Sénateur, Avis n° 351 présenté au nom de la Commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi, adopté par l'Assemblée nationale, pour la confiance dans l'économie numérique, 11 juin 2003, JO Sénat.



En outre, certaines plates-formes procèdent également à des vérifications, lors de l'inscription, afin d'éliminer certains vendeurs qui pourraient être jugés fantaisistes (cf. *supra* les descriptifs des plates-formes eBay et Priceminister).

En conséquence **des conseils de prudence doivent être prodigués aux internautes. En l'absence de toute** vérification de l'identité réelle des utilisateurs des plates-formes, ils doivent **agir avec prudence dans le choix de leur futur cocontractant.**

Enfin, **Le Forum recommande aux plates-formes mandataires pour l'ensemble de la vente, sous réserve des contraintes juridiques et techniques, de procéder à l'identification de l'offreur, ou de détenir des éléments le permettant, sous peine de voir leur propre responsabilité être engagée**<sup>165</sup>.

### **L'information sur le prix de vente, les frais de logistique et d'emballage**

Plusieurs dispositions législatives et réglementaires imposent au vendeur d'informer lisiblement l'acheteur du prix total de vente intégrant ainsi une information sur les frais de livraison, de logistique et d'emballage ou le montant des taxes et éventuels droits afférents à la vente.

Ces obligations sont fixées par les articles L. 113-3 et L. 121-18 du Code de la consommation, l'article 1591 du Code civil, l'article 19 de la loi pour la confiance dans l'économie numérique ou les arrêtés de 1987 – complétés par une circulaire de 1988 sur le prix.

Si le vendeur affiche naturellement le prix de vente du bien, dans certaines hypothèses, le montant des frais de livraison n'est pas indiqué. En effet, le vendeur peut, dans certaines situations, difficilement en déterminer le montant exact dès lors que ceux-ci dépendent du lieu de résidence de l'acheteur (France, Europe, étranger, etc.) qui n'est pas encore connu lors de la mise en vente de l'objet, du mode d'expédition du produit (retrait physique, lettre simple, envoi suivi, recommandé avec ou sans valeur déclarée, messagerie express) et de l'accord du vendeur et de l'acheteur sur ces éléments.

Dès lors que ces informations constituent une des caractéristiques essentielles du contrat formant le consentement de l'acheteur<sup>166</sup>, le contrat ne pourra être formé que postérieurement à la transmission de l'information et à son acceptation par l'acquéreur. Celui-ci détiendra, alors, la possibilité de ne pas poursuivre la négociation.

---

165. Civ. 1, 17 novembre 1993, *Bull. civ. I*, n° 329.

166. A noter que dans la théorie générale du contrat, l'absence d'indication du prix n'est pas systématiquement perçue comme étant à l'origine d'un vice du consentement, dès lors que celui-ci est déterminé ou déterminable. Or, en la matière, la détermination du prix total dépendra à la fois d'éléments connus du seul vendeur (modes d'expédition, coût d'emballage) et du seul acheteur (lieu de résidence, etc.). Dans ces conditions, l'acheteur n'est donc pas en mesure en l'absence d'éléments complémentaires de pouvoir déterminer exactement les frais complémentaires qui seront facturés par le vendeur.

**En conséquence, le Forum conseille à tout vendeur de préciser clairement, dans le cadre de son annonce, si le prix de vente s'entend tous frais compris ou si les coûts d'expédition, d'emballage et les taxes et droits afférents ne sont pas inclus.**

**Les plates-formes agissant comme mandataires du vendeur sont tenues, si celles-ci définissent ces frais, de procéder à une information du consommateur sur le montant des frais de livraison avant la conclusion définitive du contrat**<sup>167</sup>.

Il faut noter que **les plates-formes de courtage ne sont, quant à elles, soumises à aucune obligation d'information en la matière.**

### **La promotion d'outils de paiement sécurisé**

Outre les éléments d'information rappelés précédemment, une promotion des outils de paiement sécurisé doit être menée. En effet, même si aucune obligation légale n'est imposée en la matière, la prudence incite à se tourner vers ceux-ci dès lors qu'un certain nombre d'escroqueries provient de l'utilisation d'outils de paiement ne permettant pas aisément un traçage du flux financier.

Deux modes sont principalement visés : le paiement en liquide ou celui utilisant des solutions de transfert de fonds.

Concernant le paiement en liquide, l'article R.3 du Code des postes et communications électroniques sanctionne deux pratiques. Tout d'abord, l'insertion de billets de banque français ou étrangers ou d'autres valeurs au porteur dans les envois ordinaires ou simplement recommandés est une contravention de 5<sup>e</sup> classe (1 500 euros). Néanmoins, la peine ne sera pas encourue lorsque *«l'insertion de tels billets et valeurs dans les lettres recommandées n'excède pas le montant maximum de l'indemnité accordée, en cas de perte, en fonction du taux de garantie choisi par l'expéditeur au moment de l'envoi»*. Ensuite, l'insertion de pièces de monnaie françaises ou étrangères ayant cours légal dans tout envoi autre qu'une lettre ou boîte avec valeur déclarée est également une contravention de 5<sup>e</sup> classe. Dans tous les cas, un acheteur procédant au paiement de sa commande par ce moyen ne pourrait que difficilement apporter la preuve de la bonne exécution de son obligation.

L'utilisation de solutions de transfert de fonds peut également s'avérer délicate dès lors que certains pays n'opèrent pas de contrôle d'identité lors du retrait des sommes envoyées par l'internaute. À ce titre, il faut relever la démarche réalisée par l'un des acteurs de ce secteur, Western Union, qui a pris position en la matière : *«nous vous recommandons de ne pas utiliser un service de virement d'argent pour régler vos achats effectués en ligne. Les services de virement d'argent sont un moyen rapide, facile et pratique pour envoyer des fonds à des gens de connaissance. Ces services ne sont pas adaptés comme moyen de paiement à des inconnus»*.

---

167. Dans la majorité des cas, cette obligation est remplie par la plate-forme mandataire. En effet, celle-ci calcule automatiquement des frais de livraison en fonction de la nature du produit (livre de poche, CD, DVD), le mode d'expédition choisi par l'acheteur (courrier simple, recommandé, etc.) et le lieu d'expédition du produit (France, étranger).

En conséquence, il convient **de recommander aux utilisateurs, ou aux plateformes lorsqu'elles agissent en qualité de mandataire du vendeur d'avoir, recours à des outils de paiement permettant une traçabilité des sommes** comme par exemple le paiement par carte bancaire, le virement postal ou bancaire, le chèque postal ou bancaire (sous réserve du délai imparti à la banque pour examiner la solvabilité du compte du débiteur).

Pour les montants de forte valeur, les plateformes de courtage devraient **inviter les utilisateurs à avoir recours à des solutions plus sûres, par exemple de séquestre financier**<sup>168</sup>. Elles pourraient notamment, dans leurs messages d'information, promouvoir tel ou tel acteur identifié auprès d'elles comme fiable.

Néanmoins, le Forum n'a pas souhaité faire de ce mécanisme de paiement une de ses recommandations majeures dès lors que se sont développées sur l'internet des fraudes consistant en la création de faux sites de « tiers de confiance ». En outre, l'activité de séquestre financier étant peu rentable, il n'existe que de très rares structures proposant de telles solutions. En conséquence, les consommateurs qui souhaiteraient recourir à ces solutions sont invités à consulter les pages d'aide de la plateforme qui peuvent, soit avoir intégré un tel mécanisme, soit avoir conclu des partenariats avec un acteur sûr et déterminé.

#### **L'information sur les caractéristiques essentielles du bien ou du service**

L'article L. 111-1 du Code de la consommation impose à tout professionnel d'informer le consommateur sur les caractéristiques essentielles du bien ou du service mis en vente. Un tel principe s'applique également dans les relations entre deux particuliers dès lors qu'en l'absence de telles informations, l'acheteur pourrait invoquer le dol en matière de vice du consentement et, le cas échéant, le vendeur pourrait également s'exposer à des sanctions pénales sur le fondement de la publicité mensongère visée à l'article L. 121-1 du Code de la consommation.

En pratique, les principales plateformes proposent au vendeur des outils lui permettant d'afficher des éléments complémentaires dans le descriptif des produits qu'il met en vente<sup>169</sup>.

Néanmoins, si les plateformes ont souhaité intervenir à ce stade du processus contractuel afin d'améliorer l'information de ses utilisateurs, **il n'en demeure pas moins que cette obligation essentielle pèse sur le vendeur, professionnel ou**

---

168. Il s'agit d'un tiers entre les mains duquel l'argent est versé et qui procèdera au paiement du vendeur dès qu'il aura reçu confirmation de la bonne livraison de la commande. Si le terme « tiers de confiance » (*escrow* en anglais) est couramment utilisé pour désigner ces activités, les solutions proposées relèvent du séquestre financier dès lors que la prestation porte exclusivement sur la partie financière de la transaction et en aucun cas sur son aspect matériel (conservation du bien afin de procéder à sa livraison).

169. Grâce à des bases de données « produits », le vendeur peut rapidement afficher une annonce pré-remplie en saisissant uniquement le code barre situé au verso du bien mis en vente. Le vendeur conserve la possibilité de modifier les éléments proposés par la base de données.

**non, ou son mandataire<sup>170</sup> et que ceux-ci sont seuls responsables de la bonne description des biens ou produits mis en vente.** Les courtiers en ligne ne sont soumis à aucune obligation en la matière.

Les vendeurs pourraient également réaliser une information plus complète de leur offre en **utilisant des liens hypertextes** vers le site, par exemple, des fabricants ou des éditeurs des objets mis en vente. **Les plates-formes sont donc invitées à ne pas interdire contractuellement la réalisation de liens hypertextes depuis une annonce vers de telles informations complémentaires.**

### **Le cas particulier de l'affichage d'une image dans l'annonce**

La majorité des vendeurs affiche, en marge de leur annonce, une photographie de l'objet mis en vente comme, par exemple, la jaquette d'un CD ou d'un DVD, la couverture d'un livre voire l'image d'un tableau. La mise en ligne de ces images est destinée à assurer l'exécution de leur obligation d'information.

Cependant, cette obligation doit être conciliée avec les règles applicables en matière de droit d'auteur qui interdisent toute reproduction ou représentation d'une œuvre sans autorisation de l'auteur ou de ses ayants droit comme, par exemple, les illustrations graphiques. En conséquence, il semble exister une opposition de deux droits légitimes : ceux de l'auteur et de ses ayants droits et ceux du consommateur. Il importe donc que les utilisateurs puissent trouver un mode en permettant la conciliation en ayant recours, notamment, aux liens hypertextes. **Les vendeurs pourraient ainsi renvoyer vers le site internet de l'éditeur où serait présenté, de manière plus complète et illustrée, l'ouvrage, le CD ou le DVD qu'il désire mettre en vente.**

### **L'information sur les conditions particulières de la vente**

L'article L. 113-3 du Code de la consommation impose au vendeur d'informer le consommateur sur les conditions particulières, s'il y en a, applicables à la vente. Ce principe fait miroir à celui existant pour les professionnels à l'article 1369-4 du Code civil, introduit par la loi pour la confiance dans l'économie numérique.

En pratique, chaque vendeur peut librement indiquer dans ses offres les conditions particulières applicables à la vente, certains sites leur offrant même des espaces dédiés à cette fin. En dehors de toute mention, la vente obéira aux principes minimums posés par le droit français, relativement protecteurs de l'acheteur.

## **La passation du contrat**

### **La condition de validité du contrat: le principe du double clic**

La loi du 21 juin 2004 pour la confiance dans l'économie numérique a créé au sein du Code civil un article 1369-5 instituant un formalisme *ad validatem* dans la conclu-

---

170. En ce qui concerne le mandataire, celui-ci ne pourra être tenu responsable de la diffusion d'informations erronées ou parcellaires que s'il est démontré qu'il en avait connaissance. En conséquence, si l'offreur remplit incorrectement son annonce, cela ne pourra être opposé à la plate-forme mandataire et ne pourra l'être qu'après de l'offreur.

sion du contrat électronique dans le but de protéger l'acheteur contre une prise de commande trop rapide. Le texte prévoit que *«pour que le contrat soit valablement conclu, le destinataire de l'offre doit avoir eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation»*.

**Le Code civil institue, à la charge du vendeur ou de son mandataire, un formalisme de nature technique (principe du double clic)** qui demeure étroitement lié à la conception et à la navigation dans le site de vente en ligne. Une exception est prévue à l'article 1369-6 du même code pour les contrats conclus par échange de courriers électroniques.

Dans le cas d'une vente conclue par l'intermédiaire d'une plate-forme, le vendeur n'a aucune maîtrise de l'architecture technique du site utilisé. Afin de concilier la règle sus-rappelée avec le désir d'une construction collective de la confiance dans le secteur du commerce électronique, il paraît opportun de faire participer le courtier en ligne au respect du formalisme imposé par le Code civil.

**En conséquence, le Forum invite les plates-formes qui ne seraient pas en conformité, à proposer à leurs utilisateurs un outil technique permettant de respecter les formalités imposées par l'article 1369-5 du Code civil.**

L'acheteur pourra ainsi se voir proposer le récapitulatif de sa commande avec la possibilité de le modifier, et ceci préalablement, à la conclusion définitive du contrat. Ce récapitulatif est d'autant plus utile que les différents éléments constitutifs de l'offre peuvent être indiqués dans plusieurs pages (annonce elle-même mais également les pages «boutiques», les «pages personnelles», etc.).

**En conséquence, le Forum des droits sur l'internet recommande aux plates-formes d'afficher le récapitulatif de la commande de manière à rassembler visuellement les principaux éléments constitutifs de l'offre.**

À noter que dans le modèle de vente sous forme d'enchères, le régime juridique applicable est susceptible de varier en fonction de la rédaction de l'offre par le vendeur. En effet, comme nous l'avons vu précédemment, soit le contrat sera considéré comme conclu sur la plate-forme lors de l'acceptation de l'offre par le vendeur, soit le contrat sera conclu postérieurement au recours à la plate-forme par l'intermédiaire d'un échange de courriels. Selon les situations, la vente pourra donc relever de l'article 1369-5 ou 1369-6 du Code civil.

En outre et contrairement à un contrat de vente classique où l'acheteur sélectionne l'offre faite par le vendeur, en matière de vente sous forme d'enchères, il peut revenir au vendeur, pour former le contrat, de choisir l'offre faite par l'acheteur. Le double-clic s'appliquerait alors vis-à-vis du choix opéré par le vendeur et non pas lors de la saisie de son offre par l'acheteur. Néanmoins, compte tenu des modalités plurielles de formation du contrat lors du recours à ces plates-formes et afin de préserver l'esprit du législateur qui souhaitait protéger l'acheteur de toute commande involontaire, le principe du double clic devrait, également, être mis en œuvre par ces plates-formes lors de l'indication d'une somme ou de la validation d'une commande par l'acheteur.

**Dans ces conditions, le Forum des droits sur l'internet recommande que les plates-formes de courtage sous forme d'enchères mettent en œuvre – quelque soit le type d'offre – un système de double clic lors de l'indication par l'acheteur de son offre d'achat.**

#### **La question de «l'erreur sur le prix»**

Cette problématique juridique, qui a fait l'objet de plusieurs cas concrets<sup>171</sup>, peut être rencontrée dans le cadre des relations commerciales entre particuliers. En effet, le vendeur – ou l'acheteur dans un système d'enchères – peuvent être amenés à commettre des erreurs en matière de fixation du prix de vente, erreurs qui pourraient ensuite leur être opposées.

L'erreur sur le prix commise par le vendeur consistera à proposer à la vente un produit à un prix dérisoire suite, par exemple, à une erreur de saisie. En principe, le droit français n'admet pas comme vice du consentement l'erreur sur le prix, pouvant entraîner une nullité du contrat. Néanmoins, la jurisprudence a pu aménager cette solution en permettant à un vendeur de revendiquer l'erreur sur le prix, et d'obtenir l'annulation de la vente, lorsqu'il apparaît que l'acheteur avait conscience qu'une erreur avait été commise. Cela vise en particulier les prix «manifestement» dérisoires. Dans le secteur des ventes entre particuliers, ce point est délicat et il est à nouveau nécessaire de distinguer selon que les ventes se font à prix fixe ou aux enchères.

Dans le cas d'une vente à prix fixe, le vendeur pourra revendiquer l'erreur de saisie commise dès lors qu'il démontre que l'acheteur avait conscience de «la coquille» – ce qui, en pratique, vise les erreurs importantes ou grossières (vente d'un appareil numérique à 2 euros au lieu de 200 euros).

À l'inverse, dans le cas d'une vente sous forme d'enchères, il sera difficile au vendeur de rapporter cette preuve. En effet, selon une pratique relativement courante (et parfois recommandée par les plates-formes elles-mêmes) les produits sont mis à prix à un montant relativement faible (1 euro par exemple) afin de créer un mécanisme d'entraînement qui permet au vendeur de recueillir un maximum d'enchères. Ainsi, un vendeur commercialisant, par exemple, un appareil photographique numérique avec une mise à prix initiale de 1 euro (au lieu de 100 euros) pourrait difficilement opposer à son acheteur ladite erreur dès lors que pour ce dernier, un prix de départ fixé de manière aussi basse peut correspondre à une pratique habituelle des utilisateurs du site.

**Il convient donc de recommander aux vendeurs la plus grande vigilance en matière de mise en vente de leurs produits dès lors, qu'en cas d'erreur, il leur serait difficile d'empêcher les acheteurs de s'en prévaloir.**

Un acheteur est également susceptible de commettre une erreur sur le prix. Cette hypothèse particulière provient de la spécificité des ventes sous forme d'enchères. En effet, dans ce mécanisme, le particulier est appelé à faire une offre d'achat matéria-

---

171. TGI Strasbourg, 24 juillet 2002, D. 2003, p.2434, obs. Cedric Manara; L'erreur sur le prix d'affichage dans le milieu du commerce électronique, 25 mars 2003.  
<http://www.foruminternet.org/actualites/lire.phtml?id=526>

lisée sous la forme d'un montant en euro saisi dans un formulaire de « proposition ». L'erreur de saisie commise peut avoir comme conséquence de faire une enchère très importante voire d'acheter un produit d'occasion à un montant supérieur à son prix de vente neuf. Il convient cependant de préciser que ce type d'erreur de la part de l'acheteur devrait être extrêmement rare dès lors qu'un système de confirmation du montant saisi (principe du double clic) est mis en place par la plate-forme.

Selon un raisonnement analogue et indépendamment des possibilités offertes par certaines plates-formes<sup>172</sup> afin de pouvoir invoquer l'erreur commise, l'acheteur devra prouver que le vendeur savait manifestement que le prix proposé n'était pas le bon. Or, cette preuve sera d'autant plus difficile à rapporter que l'acheteur doit « double-cliquer » avant que son offre définitive soit enregistrée par la plate-forme.

### **Le refus de vente par le vendeur ou la rupture des discussions par l'acheteur**

Le refus de vente<sup>173</sup> – et son pendant civiliste, la rupture abusive des pourparlers – sont deux mécanismes qui sont **destinés à sanctionner des comportements frauduleux ou abusifs en amont de la conclusion du contrat**.

Compte tenu de cette précision, la question du refus de vente ne peut être envisagée, en matière de ventes au travers des plates-formes, que dans le cas de la vente sous forme d'enchères. En effet, dans le mécanisme de vente à prix fixe et sauf exceptions, le vendeur et l'acheteur se retrouvent contractuellement liés dès la validation définitive du contrat. Aucune des deux parties ne peut donc – sauf décision conjointe – refuser d'exécuter les obligations mises à leur charge (livraison du bien, paiement du prix).

Dans les systèmes d'enchères, deux cas relativement proches dans les faits, mais aux qualifications juridiques différentes, doivent être envisagés: le **refus de vente par le vendeur** et la **rupture abusive des pourparlers par l'acheteur**.

Le **refus de vente par un vendeur** demeure une situation très rare et provient souvent d'une faculté laissée par la plate-forme à son utilisateur: celle de choisir l'acheteur avec lequel il souhaite contracter.

Dans certaines situations, le vendeur pourra être tenté de choisir un acheteur qui fait l'objet d'une bonne notation, avec lequel il a déjà entretenu de précédentes relations contractuelles plutôt que de choisir le meilleur enchérisseur. Ce choix du « second » offreur pourrait être perçu par le vainqueur de l'enchère comme un refus de vente. Néanmoins, l'article L. 122-1 du Code de la consommation admet une exception: lorsque le refus est justifié par un motif légitime.

---

172. A noter par exemple que eBay a mis en place le système double clic permettant à l'enchérisseur/acheteur de confirmer le montant saisi. eBay permet également aux enchérisseurs/acheteurs ayant commis une erreur de saisie de procéder à une « rétractation d'enchères ».

173. Le refus de vente est visé par l'article L. 122-1 du Code de la consommation: « *Il est interdit de refuser à un consommateur la vente d'un produit ou la prestation d'un service, sauf motif légitime, et de subordonner la vente d'un produit à l'achat d'une quantité imposée ou à l'achat concomitant d'un autre produit ou d'un autre service ainsi que de subordonner la prestation d'un service à celle d'un autre service ou à l'achat d'un produit* ».

Il en serait ainsi si le vendeur n'avait plus en sa possession le bien mis en vente (destruction du bien, vente antérieure par l'intermédiaire d'une autre plate-forme) ou si d'autres éléments objectifs pouvaient être invoqués: le meilleur enchérisseur n'a pas ou très peu d'évaluations, et/ou a fait l'objet d'une mauvaise notation par ses précédents cocontractants, il demeure dans un lieu rendant difficile la livraison du bien (par exemple, un acheteur basé à l'étranger et qui remporte la vente portant sur une voiture). À l'inverse, un refus qui proviendrait par exemple d'une discrimination fondée sur la nationalité, la race ou la religion (ces éléments peuvent en effet apparaître dans le pseudonyme de l'utilisateur) ne saurait être invoqué.

Concernant la rupture par l'acheteur, le droit permet à un **vendeur d'engager des poursuites à l'encontre d'un acheteur qui aurait réalisé une rupture abusive des pourparlers**, c'est-à-dire qui se serait engagé à acheter le bien mais qui déciderait au dernier moment de ne pas finaliser le contrat. Une telle situation se rencontre notamment lorsque l'acheteur, après réflexion, décide de ne pas finaliser le contrat avec le vendeur alors même qu'il a remporté l'enchère. Cela peut s'expliquer par le fait que l'achat en ligne demeure un achat d'impulsion et qu'en l'absence de paiement immédiat, certains acheteurs peuvent s'estimer non engagés dans un processus contractuel<sup>174</sup>.

Cette théorie, qui s'est principalement développée dans le monde des affaires, vise à indemniser la partie qui a été dans l'obligation – lors de la période précontractuelle – de procéder à certaines dépenses. La rupture abusive lui causant un préjudice, le droit l'autorise à en obtenir un dédommagement.

Dans les ventes entre particuliers, le préjudice subi par le vendeur peut avoir plusieurs sources. Cela peut correspondre au temps passé à tenter sans succès de finaliser le contrat ou, plus simplement, aux frais de mise en vente du produit qui ne lui seront pas remboursés par la plate-forme.

**Dans ces conditions, les utilisateurs des plates-formes de courtage sont invités à ne point rompre, sans motif légitime, la discussion devant aboutir à la conclusion du contrat, sous peine de s'exposer à des sanctions, civiles ou pénales.**

## L'exécution du contrat

### **La responsabilité de plein droit du vendeur vis-à-vis de la bonne exécution du contrat**

Introduit par l'article 15 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, le régime de responsabilité de plein droit du cyber-vendeur régit les contrats conclus par un particulier, y compris lorsque le vendeur est un non professionnel. En effet, l'article 15-I fait référence, quant à lui, à toute personne physique

---

174. « Les paiements sur l'internet », Deuxième rapport du Forum des droits sur l'internet sur la cyber-consommation, 19 mai 2005.  
<http://www.foruminternet.org/publications/lire.phtml?id=906>



ou morale exerçant une activité de commerce électronique – définition qui n’a pas souhaité intégrer les seules personnes exerçant cette activité à titre professionnel<sup>175</sup>.

Il en résulte que **tout vendeur ou mandataire assurant le service après-vente est responsable de plein droit de la bonne exécution du contrat conclu à distance**. Ce principe signifie qu’il devra s’assurer de la livraison du bien commandé, sans dommage ni absence de conformité aux caractéristiques précisées dans l’offre. Conformément à l’article 15-I, un vendeur ne pourra s’exonérer de sa responsabilité que dans trois situations : en cas de faute commise par l’acheteur – qu’il devra alors être en mesure de prouver, en cas de force majeure ou de faits irrésistibles et imprévisibles d’un tiers au contrat.

En matière de vente à distance, l’un des éléments sur lequel le vendeur a peu de maîtrise est l’expédition du bien qui fait intervenir un acteur supplémentaire.

**En conséquence, le Forum des droits sur l’internet recommande aux particuliers qui vendent par l’intermédiaire d’une plate-forme de soigner l’expédition de leurs objets et de recourir, pour les biens d’une valeur importante, à des produits postaux permettant un suivi de l’envoi.**

Cette recommandation fait écho au nouveau régime de responsabilité du transporteur postal, inséré par la loi du 20 mai 2005 relative à la régulation des activités postales<sup>176</sup>, aux articles L. 7 et suivants du Code des postes et communications électroniques prévoyant que «*la responsabilité des prestataires de services postaux au sens de l’article L. 1 est engagée dans les conditions prévues par les articles 1134 et suivants et 1382 et suivants du code civil à raison des pertes et avaries survenues lors de la prestation*». Ce régime s’il offre au vendeur la possibilité de se retourner contre le transporteur postal en cas de mauvaise exécution de son obligation<sup>177</sup>, ne lui permet pas de s’exonérer de sa propre responsabilité vis-à-vis de l’acheteur.

Ce régime de responsabilité de plein droit du cyber-vendeur demeure exceptionnel en droit français. Il n’existait auparavant que dans le cadre des contrats conclus par des consommateurs avec des agences de voyages et pour l’acquisition de voyage à forfait.

---

175. À l’occasion des débats parlementaires autour de la définition du commerce électronique, la Commission européenne est venue indiquer que la définition du commerce électronique prévue au sein de la directive du 8 juin 2000 ne pouvait exclure les activités non rémunérées de la société de l’information. Ainsi, la loi, qui transpose cette directive, ne distingue pas entre activité professionnelle et activité non professionnelle.

176. Loi n° 2005-516 du 20 mai 2005 relative à la régulation des activités postales, *JORF* 21 mai 2005, p. 8825, texte n° 1.  
<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=ECO0300058L>

177. Néanmoins, le vendeur devra se ménager des modes de preuve suffisants de la non exécution de ladite obligation d’où la nécessité de recourir à des outils permettant la traçabilité de la transaction.

Compte tenu du caractère novateur de la mesure et de ses conséquences importantes pour un vendeur<sup>178</sup> et afin d'avoir une construction collective de la confiance, le Forum invite les plates-formes, dans le cadre des messages d'information adressés aux vendeurs, à sensibiliser ceux-ci à ce régime spécifique de responsabilité et aux solutions qui leur sont proposées permettant de diminuer le risque encouru (produits postaux, système d'assurance ou d'indemnisation proposés par la plate-forme).

Enfin et en raison de leur rôle particulier comme mandataire, le Forum invite les plates-formes qui procèdent à une gestion intégrée des modalités d'envoi postal (modèle Priceminister) à imposer un mode d'envoi non ordinaire (lettre suivie, messagerie rapide, recommandé, etc.) lorsque le montant de la commande passée par l'utilisateur dépasse un certain montant (qu'il reviendra à la plate-forme de déterminer en fonction notamment du panier moyen).

### **La garantie des vices cachés**

Aux termes de l'article 1641 du Code civil, « *le vendeur est tenu de la garantie à raison des défauts cachés de la chose vendue qui la rendent impropre à l'usage auquel on la destine, ou qui diminuent tellement cet usage, que l'acheteur ne l'aurait pas acquise, ou n'en aurait donné qu'un moindre prix, s'il les avait connus* ».

Cette obligation de garantie s'impose à tout vendeur, professionnel ou non. Elle offre la possibilité à l'acheteur, soit de rendre la chose et de se faire restituer le prix, soit de la garder et de se faire rendre une partie du prix dont le montant doit, aux termes de l'article 1644 du Code civil être « *arbitrée par experts* ». Si le vendeur connaissait les vices de la chose, il est tenu, outre la restitution du prix qu'il en a reçu, de tous les dommages et intérêts envers l'acheteur. À l'inverse, si le vendeur ignorait les vices de la chose, il ne sera tenu qu'à la restitution du prix, et à rembourser à l'acquéreur les frais occasionnés par la vente.

Depuis l'ordonnance du 17 février 2005, il est à noter que cette action doit être intentée par l'acquéreur dans un délai de deux ans, délai qui court à compter de la découverte du vice et non pas à compter de la vente.

Compte tenu de ces éléments, le Forum des droits sur l'internet rappelle à tous les vendeurs qu'ils demeurent soumis à la garantie légale sur les vices cachés, **quand bien même le produit vendu serait un bien d'occasion**.

Enfin, les plates-formes sont invitées à diffuser, dans leur page d'aide, une information en la matière.

---

178. À défaut d'élément lui permettant de s'exonérer de sa responsabilité, le vendeur sera tenu soit de rembourser son client, soit de procéder à l'expédition d'un nouvel exemplaire du bien initialement commandé.

## Les règles spécifiques applicables au vendeur professionnel

Depuis le lancement des plates-formes de mise en relation sur le marché français, des professionnels ont souhaité recourir à ces outils afin de développer leur activité commerciale sur l'internet. En tant que vendeur, ils sont soumis à des obligations supplémentaires tirées, notamment, du droit de la vente à distance. A défaut de respecter ces règles, ils peuvent être considérés comme développant des activités paracommerciales «*qui consistent à se livrer à une activité commerciale sans supporter les charges correspondantes [et qui] sont une atteinte aux règles d'une saine concurrence*».

Ce phénomène existe sur l'internet. Un précédent rapport du Forum des droits sur l'internet dénombrait en France plusieurs milliers de particuliers devenus, grâce à ces outils, des professionnels de la vente à distance. Il n'est pas nouveau. Par une circulaire du 12 août 1987<sup>179</sup> relative à la lutte contre les pratiques paracommerciales, plusieurs ministres indiquaient qu'il ne pouvait être admis «*qu'avec une concurrence devenue plus intense certaines entreprises rencontrent des difficultés, non pas parce qu'elles sont insuffisamment efficaces, mais parce qu'elles perdent des clients au profit de concurrents dont la seule performance consiste à ne pas supporter les mêmes charges*».

Il faut noter que le développement de telles activités n'est, en général, pas l'expression d'une volonté d'échapper à un régime juridique. La circulaire du 12 août 1987 rappelait, d'ailleurs, que : «*le développement des pratiques paracommerciales est un mouvement spontané qui témoigne souvent moins d'un désir de fraude que d'initiatives naturelles de personnes ou d'organismes voulant développer leur activité sans prendre connaissance des règles qui leur sont applicables*».

Après avoir défini la notion de vendeur «*professionnel*», le rapport s'attachera à rappeler les principales règles spécifiques qui lui sont applicables en matière de vente à distance.

### **La notion de professionnel**

Le concept de «*professionnel de la vente à distance*», notion charnière en matière d'application du droit de la vente à distance, n'a jamais fait l'objet d'une définition par le Code de la consommation. Afin d'apprécier le statut d'un particulier opérant des ventes par l'intermédiaire de ces plates-formes, il est nécessaire dans un premier temps d'élaborer une définition du «*professionnel*» avant, dans un second temps, de l'appliquer à certaines situations actuellement rencontrées sur l'internet.

#### **Les critères posés par le droit positif**

Plusieurs textes font référence à la notion de «*professionnel*» sans jamais la définir. La jurisprudence, quant à elle, est venue apporter des précisions permettant de fixer quelques critères.

#### **Le droit commun**

Le droit commun fait référence à une notion centrale, le commerçant, et plus rarement à celle de professionnel. L'article L. 121-1 du Code du commerce précise que «*sont*

---

179. Circulaire du 12 août 1987 relative à la lutte contre les pratiques paracommerciales, *JORF* 25 août 1987, p.9704.

commerçants ceux qui exercent des actes de commerce et en font leur profession habituelle». Selon l'article L. 110-1 du même code, sont notamment des actes de commerce, «1° tout achat de biens meubles pour les revendre, soit en nature, soit après les avoir travaillés et mis en œuvre». Un double critère est donc appliqué: celui de la réalisation de certaines activités (actes de commerce, etc.) et celui de l'exercice de cette activité à titre habituel.

La jurisprudence a pu estimer que l'activité commerçante s'entend d'une «*occupation sérieuse de nature à produire des bénéfices et à subvenir aux besoins de l'existence*»<sup>180</sup>. Les juges ont donc apporté une précision complémentaire à savoir la nécessité, pour le commerçant, d'avoir une activité susceptible de lui procurer des revenus suffisants pour vivre.

Ces critères (activité, habitude, rémunération) sont repris par d'autres textes, par exemple, en matière de droit du sport<sup>181</sup>, en matière de protection sociale<sup>182</sup> ou en matière fiscale<sup>183</sup>.

### **Le droit de la consommation**

Le droit de la consommation et le droit commun n'ont pas le même champ d'application. En effet, si un commerçant peut être un professionnel au sens du droit de la consommation, tout commerçant ne l'est pas systématiquement (cas des non-professionnels) et tout professionnel n'est pas obligatoirement un commerçant, au sens du Code du commerce (cas des travailleurs indépendants, artisans, etc.).

Le droit de la consommation fait référence, selon les articles, à trois notions distinctes: le consommateur, le professionnel et le non-professionnel. Cette dernière catégorie vise les personnes physiques ou morales auxquelles le droit souhaite offrir une protection équivalente aux consommateurs<sup>184</sup>. Aucune de ces notions n'est définie par le Code de la consommation<sup>185</sup>; en particulier, celle du vendeur professionnel n'est pas explicitée.

---

180. CA Paris, 30 avril 1906, *DP* 1907, 5, p. 9.

181. Les textes font une distinction entre les sportifs amateurs et professionnels: le critère utilisé est celui de la régularité et de la fourniture d'un revenu permettant de vivre.

182. Les juges ont pu estimer, qu'en matière d'indemnisation d'un demandeur d'emploi par les ASSEDIC, qu'il n'y avait pas d'activité professionnelle en l'absence de rémunération (cas de l'exercice par le demandeur d'emploi d'une activité bénévole à temps plein).

183. Le droit fiscal a institué deux statuts de loueur meublé, l'un professionnel, l'autre non professionnel. La différence tient au montant des revenus retirés de cette activité (supérieur ou inférieur à 23 000 €).

184. Pour une application: Civ. 1<sup>o</sup>, 15 mars 2005, Syndicat départemental de contrôle laitier de la Mayenne, n° 02-13285: «*la notion distincte de non professionnel, utilisée par le législateur français, n'exclut pas les personnes morales de la protection contre les clauses abusives*».

185. À ce sujet, voir Rép. Min. Weber n° 54215, *JOANQ* 19 avril 2005, p. 4085: «*Aucune définition du consommateur n'a été insérée au sein du code de la consommation en raison de la nature de la codification qui en est à l'origine. En effet le code de la consommation, adopté en 1993, réunit des textes dont les objectifs sont très différents et dont les champs d'application diffèrent sensiblement. (...) L'absence d'une définition du consommateur, conforme à la tradition juridique française, ne constitue pas une véritable difficulté mais plutôt un élément de souplesse car elle permet à la jurisprudence d'appliquer avec discernement les règles du droit de la consommation au contexte de chaque espèce*».

En droit communautaire, les directives adoptées en matière de protection du consommateur définissent le professionnel au travers de deux critères : une habitude d'exercice de l'activité et la volonté d'en tirer des profits. La jurisprudence française a confirmé<sup>186</sup> ces premières pistes et a pu étendre le champ d'application du droit de la consommation en ayant recours à un nouveau critère : celui de l'exercice d'une activité sous une forme organisée.

### **Les critères permettant de qualifier un particulier de vendeur professionnel**

Plusieurs critères<sup>187</sup> permettent de qualifier de professionnel de la vente à distance un particulier qui vendrait des biens sur l'internet. Le changement de statut du particulier ne sera pas lié à l'application d'un seul de ces indices mais au constat que l'internaute en remplit plusieurs. C'est donc un faisceau d'indices qui déterminera le statut exact du vendeur.

#### **Le Forum des droits sur l'internet a pu établir la liste de critères suivante :**

– la **régularité de l'activité** : les juges rechercheront si le vendeur procède à son activité de manière fréquente et régulière et non pas de manière occasionnelle. La doctrine administrative a ainsi pu estimer que « *le particulier qui se livre à titre habituel à des actes de vente sur un site marchand est un commerçant de fait au sens de l'article L. 121-1 du Code de commerce* »<sup>188</sup>. La circulaire du 12 août 1987 avait adopté le même critère en estimant qu'en « *aucun cas, la vente d'objets mobiliers personnels par un particulier [qui ne souhaite pas devenir un professionnel], qu'elle soit réalisée dans des lieux publics ou privés, ne doit présenter un caractère habituel* ».

– le **caractère lucratif de l'activité** : les juges tenteront de déterminer si le vendeur souhaite tirer des revenus de son activité. L'absence de revenus suffisants pour vivre n'est pas pour autant un élément suffisant pour prouver le caractère non lucratif de l'activité.

– l'**intention d'avoir une activité professionnelle** : ce critère permet de déterminer la volonté réelle du vendeur. Pour démontrer cette intention, il est possible de recourir à plusieurs indices de commercialité :

- *la réalisation d'actes de commerce* au sens de l'article L. 110-1 du Code de commerce. Ainsi, un particulier réalisant à titre habituel des actes d'achats pour revendre pourra être considéré comme un professionnel ;
- *l'existence d'un système organisé de vente à distance* : il s'agira par exemple de la réalisation par le vendeur d'une page personnelle présentant les objets mis en vente, de l'ouverture d'une boutique virtuelle, de la rédaction de conditions générales de vente, de la réalisation de publicités, de l'utilisation d'outils professionnels d'expédi-

---

186. Cas d'un crédit à la consommation demandé par une association de guitare. Le juge refuse la qualification de crédit à la consommation car l'objet même de l'activité de l'association est de dispenser des cours et est rémunératrice : c'est un exercice professionnel (« *Une association qui a pour objet l'apprentissage de la guitare et dont les statuts prévoient la rémunération de cet enseignement exerce une activité professionnelle au sens de l'article L. 311-3.3° du Code de la consommation* ») : Civ. 1<sup>er</sup>, 23 mars 1999, n° 97-11392.

187. Philippe Le Tourneau, « Les critères de la qualité de professionnel », *LPA* n° 181, 12 septembre 2005, p. 4.

188. Rép. Min. Le Fur n° 53223, *JOANQ* 1<sup>er</sup> mars 2005, p. 2248.

tion des produits voire de l'aménagement de locaux destinés spécifiquement à cette activité marchande.

Cette liste ne fait intervenir aucun seuil de valeur à partir duquel le vendeur serait considéré comme un professionnel. En effet, les principes jurisprudentiels et issus des textes communautaires s'opposent à l'intégration d'un tel critère qui pourrait, en outre, être perçu comme arbitraire, voire artificiel.

### **Approche didactique de la notion de « professionnel de la vente à distance »**

Quelques exemples permettant de mieux comprendre le contour exact de la notion vendeur professionnel de la vente à distance peuvent être pris.

---

#### *Exemple 1 : un internaute mettant en vente sa collection*

*À l'occasion de cette activité, l'internaute devra procéder à de multiples actes de vente (une offre par timbre mis en vente par exemple). Cet internaute ne sera pas, néanmoins, un professionnel de la vente à distance dès lors qu'il apparaît que ces ventes ne constituent pas des actes de commerce puisque les achats initiaux n'ont pas été réalisés dans une finalité de revente.*

#### *Exemple 2 : un internaute vend sa propre production ou fabrication*

*La vente par un particulier de sa propre production ou fabrication peut être regardée comme une activité à caractère civil ou à caractère commercial dès lors qu'il a acquis des biens pour les transformer et pour les revendre. Par ailleurs, dès lors qu'il réalise cette activité de manière habituelle et récurrente ou s'il fait appel à un système organisé de vente à distance, il devra alors être regardé comme un professionnel.*

#### *Exemple 3 : un internaute revendant sur l'internet ses propres biens*

*De la même manière qu'un collectionneur ne procède pas à des actes d'achat pour revendre, le fait pour un internaute de procéder à la revente des biens qu'il a acquis ou qu'on lui a offert ne saurait le faire regarder comme un professionnel.*

#### *Exemple 4 : un internaute revendant sur l'internet des biens achetés à cette fin*

*À l'inverse de l'exemple précédent, l'internaute pourrait, dans cette situation, acquérir la qualification de vendeur professionnel dès lors qu'il choisit délibérément de procéder à des acquisitions de biens en vue de procéder à leur revente. Une telle qualification est d'autant plus probable que le vendeur recherche, par une telle activité, à en tirer des profits.*

#### *Exemple 5 : un internaute jouant le rôle d'intermédiaire dans la vente d'objets*

*Certaines plates-formes proposent à leurs utilisateurs de jouer le rôle d'intermédiaire entre l'acheteur et le véritable propriétaire du bien. Ils deviennent en quelque sorte un courtier supplémentaire qui s'ajoute à la chaîne d'acteurs présents dans la relation contractuelle. Dès lors qu'une telle activité nécessite pour l'intermédiaire de mettre en œuvre un système organisé afin d'assurer parfaitement ce rôle, il pourra relever du statut de professionnel, notamment s'il y a une régularité dans l'exercice de cette activité, voire si celle-ci est rémunérée.*

---

## **Les recommandations du Forum des droits sur l'internet aux plates-formes de mise en relation**

La notion de «vendeur professionnel» constitue une définition charnière qui déterminera le régime juridique applicable à la relation contractuelle qu'il va nouer avec un acheteur. Compte tenu de l'intérêt que son identification peut représenter pour les consommateurs, le Forum des droits sur l'internet invite les professionnels à s'identifier comme tels dans leurs annonces – même si aucune obligation légale n'existe en la matière.

Par ailleurs, dans l'optique d'une meilleure information du consommateur, le Forum des droits sur l'internet recommande aux plates-formes de mise en relation de permettre aux «vendeurs professionnels» de s'identifier comme tels auprès d'elles. Cette identification devrait ensuite être complétée par l'adoption d'une signalétique appropriée apparaissant en marge des offres diffusées par tout vendeur sur le site et permettant aux acheteurs d'identifier rapidement et simplement le statut de leur cocontractant, et en conséquence, le régime juridique applicable à la transaction commerciale.

Aucune obligation de surveillance et de recherche des utilisateurs «*professionnels*» ne peut, pour autant, être imposée aux plates-formes. En effet, celle-ci s'avère difficilement praticable et surtout partielle. Ainsi, un vendeur écoulant en petite quantité sa marchandise sur de très nombreux sites pourrait échapper à ces contrôles. De même, ne serait pas détecté un vendeur professionnel, ayant un magasin physique mais avec une activité dématérialisée relativement faible.

Il convient plutôt de soutenir les pratiques de certaines plates-formes qui encouragent les vendeurs professionnels à s'autodéclarer en leur faisant bénéficier d'offres ou de services particuliers (récupération de la TVA sur les commissions perçues, outils évolués de mise en ligne, etc.)

## **Les règles applicables au vendeur professionnel**

Dès lors qu'un particulier est qualifié de professionnel de la vente à distance, il est soumis à certaines obligations spécifiques, complémentaires des règles générales et principalement issues du Code de la consommation<sup>189</sup>.

---

189. Jérôme Passa, «Commerce électronique et protection du consommateur», *D.* 2002, p. 555. A noter également que lorsque les ventes d'un professionnel ont lieu par l'intermédiaire de plates-formes de ventes sous forme d'enchères, elles sont soumises aux dispositions du Code de la consommation malgré l'exclusion prévue par l'article L. 121-17 du Code de la consommation pour «les ventes aux enchères». En effet, les ventes ayant lieu par l'intermédiaire de ces sites ne sauraient être qualifiées de «*ventes aux enchères publiques*», conformément à la définition donnée par le Code de commerce mais de «*ventes sous forme d'enchère*». En conséquence, les dispositions des articles L. 121-18 et suivants sont pleinement applicables aux vendeurs utilisant ces sites. Pour de plus amples informations, voir à ce sujet les développements consacrés dans une précédente recommandation du Forum des droits sur l'internet: «Le courtage en ligne des biens culturels», 22 juillet 2004.

### **L'information sur les modalités de paiement et de livraison et sur la date de livraison**

Aux termes de l'article L. 121-18 du Code de la consommation, tout vendeur professionnel est tenu d'indiquer «*les modalités de paiement, de livraison ou d'exécution*» et, conformément à l'article L. 114-1 du même code, d'«*indiquer la date limite à laquelle il s'engage à livrer le bien ou à exécuter la prestation*». **Les vendeurs sont donc responsables de la bonne exécution de ces obligations.**

En pratique, sur les plates-formes de courtage en ligne, les vendeurs ont la liberté d'indiquer, ou non, les modalités de paiement et de livraison. Sur les plates-formes agissant comme mandataires du vendeur, l'offreur initial doit obligatoirement choisir les modalités de livraison applicables (normal, recommandé, messagerie), le site proposant lui-même un nombre prédéterminé de mode de paiement (carte bancaire, chèque, etc.)

Au regard notamment des auditions menées, l'information de l'acheteur sur les modalités de paiement et de livraison constitue un des éléments essentiels pouvant déterminer un consommateur à entrer dans une phase contractuelle avec un vendeur. En effet, et en particulier en ce qui concerne les modes de livraison, cette information peut avoir une incidence sur le prix dont devrait s'acquitter l'acheteur et surtout sur la possibilité pour celui-ci de prendre possession du bien commandé (un vendeur pouvant ainsi imposer pour un bien encombrant un retrait sur place).

**Dans ces conditions et même si ces obligations sont à la charge du vendeur, le Forum des droits sur l'internet recommande aux plates-formes d'inviter leurs utilisateurs – en particulier professionnels – à indiquer, lors de la saisie de l'offre, les modalités de paiement et de livraison. En tout état de cause, seul le vendeur sera responsable de la non exécution de cette obligation. Il pourrait notamment s'exposer à une demande d'annulation du contrat de la part du consommateur pour dol.**

De même, et en application de l'article L. 114-1 du Code de la consommation, le vendeur professionnel est tenu d'indiquer au consommateur une **date de livraison**. En pratique, certaines plates-formes imposent à leurs vendeurs l'envoi de la commande dans un délai déterminé (48 heures par exemple pour Priceminister).

Le respect de cette obligation demeure délicat pour le vendeur dès lors que la date de livraison peut dépendre à la fois du mode de paiement choisi (envoi à réception du chèque), mais également, d'un tiers (le transporteur) sur lequel le vendeur n'a pas forcément de maîtrise. Ces difficultés ont ainsi incité les cyber-marchands traditionnels à modifier les informations communiquées au consommateur, privilégiant l'indication d'une date d'expédition plutôt que de livraison.

Pour autant, cette information demeure primordiale pour les consommateurs. Dans le commerce électronique opéré sur les sites internet, c'est même souvent l'élément



déterminant du choix du vendeur<sup>190</sup>, l'internaute procédant en général à une comparaison des vendeurs sur ce point.

**En conséquence, le Forum des droits sur l'internet invite les vendeurs à informer leurs acheteurs, a minima, sur une date d'expédition voire sur une date de livraison approximative compte tenu des délais annoncés par le transporteur.**

### **Le processus contractuel**

#### ***L'information sur les différentes étapes à suivre et les conditions générales de vente***

Aux termes de l'article 1369-4 du Code civil, «*quiconque propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services [doit préciser] les différentes étapes à suivre pour conclure le contrat par voie électronique*».

**Cette obligation est à la charge du vendeur professionnel ou de son mandataire.** Seulement, celle-ci – comme pour le principe du double clic précédemment abordé – est étroitement liée à l'architecture du site auquel le vendeur a recours pour procéder à sa vente. Dans ces conditions les plates-formes sont les acteurs qui ont la meilleure connaissance de l'outil technique permettant de décrire aux utilisateurs les différentes étapes du processus contractuel. En conséquence, et afin de participer à la construction de la confiance sur le réseau, **le Forum invite les plates-formes non mandataires à assister le vendeur dans la bonne exécution de l'obligation posée par l'article 1369-4 du Code civil sur les plates-formes.**

D'ores et déjà, les courtiers en ligne sous formes d'enchères sont également tenus à une obligation similaire d'information en application de l'article 67 du décret n° 2001-650 du 19 juillet 2001 pris en application des articles L. 321-1 à L. 321-38 du code de commerce et relatif aux ventes volontaires de meubles aux enchères publiques qui précise qu'«*en cas de courtage aux enchères réalisé à distance par voie électronique, le courtier assure l'information en ligne du public sur la nature exacte des opérations de courtage, sur les obligations respectives des vendeurs et des acheteurs et sur les conditions de conclusion des ventes. Cette information reproduit, de manière apparente, les dispositions du deuxième alinéa de l'article L. 321-3 du code de commerce*».

---

190. TGI Lyon, jugement correctionnel, 3 février 2005, Procureur de la République et Association des nouveaux consommateurs du Rhône c/ Thomas C. Les magistrats indiquaient dans ce jugement que: «*le délai de livraison annoncé et vérifié par la consultation des pages internet du site de cette société est donné pour*»*extrêmement rapide, entre deux et dix jours*«*et avait bien pour objet de stimuler la décision d'achat à ce site de commerce électronique le délai apparaissant d'ailleurs un des éléments principaux et mis en avant pour recourir plus particulièrement à la vente en ligne*».  
<http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=878>

**En conséquence, le Forum des droits sur l'internet recommande aux plates-formes, mandataires ou non, de procéder à la création d'une rubrique «aide» expliquant à leurs utilisateurs les modalités de fonctionnement du site et en particulier le schéma contractuel dans lequel ceux-ci vont s'engager.**

***L'information sur les moyens de consulter les règles professionnelles***

Aux termes de l'article 1369-4 du Code civil, «*quiconque propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services [doit préciser] les moyens de consulter par voie électronique les règles professionnelles et commerciales auxquelles l'auteur de l'offre entend, le cas échéant, se soumettre*».

Cette obligation, instituée par les dispositions de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, vise les vendeurs professionnels qui appartiendraient à un ou plusieurs organisations professionnelles les soumettant ainsi à des règles déontologiques plus strictes et plus protectrices du consommateur en matière de vente à distance. Elle a donc vocation à s'appliquer aux vendeurs professionnels, membres de telles structures, ce qui n'est pas le cas de la majorité de ceux ayant recours aux plates-formes.

**Néanmoins et dans un souci de permettre l'extension de l'usage de ces plates-formes à tous les acteurs du commerce électronique, il apparaît opportun que les plates-formes n'interdisent pas<sup>191</sup> au vendeur professionnel de réaliser une telle mention dans son offre ou dans sa page de présentation avec notamment l'insertion d'un lien hypertexte pointant vers lesdites règles.**

***La revente à perte***

Conformément à l'article L. 442-2 du Code du commerce, «*le fait, pour tout commerçant, de revendre ou d'annoncer la revente d'un produit en l'état à un prix inférieur à son prix d'achat effectif est puni de 75 000 euros d'amende. Cette amende peut être portée à la moitié des dépenses de publicité dans le cas où une annonce publicitaire, quel qu'en soit le support, fait état d'un prix inférieur au prix d'achat effectif*». En pratique, le prix d'achat effectif est le prix unitaire figurant sur la facture majoré des taxes sur le chiffre d'affaires, des taxes spécifiques afférentes à cette revente et du prix du transport.

En pratique, cette disposition peut viser les vendeurs professionnels qui procéderaient à la revente d'un produit à un prix inférieur à son prix d'achat effectif, que le produit soit neuf ou d'occasion.

Tel est en particulier le cas pour les vendeurs utilisant les plates-formes de vente sous forme d'enchère et dont le prix final payé par l'internaute est inférieur à ce prix d'achat effectif.

---

191. Les conditions générales d'utilisation de certaines plates-formes interdisent en effet aux vendeurs de réaliser des liens hypertextes externes dans leurs offres.

**En la matière, il convient de recommander aux magistrats de considérer le montant de mise en vente d'un produit sur ces plates-formes particulières comme ne constituant pas l'annonce de la revente à perte d'un produit, infraction prohibée par les dispositions sus rappelées.**

En effet, comme nous avons eu l'occasion de le rappeler précédemment, la mise en vente d'un produit à un faible montant est une technique inhérente au mécanisme de l'enchère destinée à accroître le nombre d'enchères.

**En tout état de cause, et afin de diminuer tout risque juridique, il convient de recommander aux vendeurs professionnels utilisant ces plates-formes d'indiquer un prix de réserve – lorsqu'une telle faculté est permise – correspondant, au minimum, au prix d'achat effectif du bien.**

Enfin, les plates-formes, mandataires ou non, sont invitées à sensibiliser, dans leur page d'aide, leurs vendeurs professionnels sur cette règle particulière.

## **Exécution du contrat**

### ***L'information sur l'existence d'un droit de rétractation***

Le droit de rétractation, disposition centrale en matière de protection du consommateur dans le secteur de la vente à distance, n'est juridiquement applicable qu'aux relations commerciales conclues à distance entre un professionnel et un consommateur.

Aux termes de l'article L. 121-20 du Code de la consommation, «*le consommateur dispose d'un délai de sept jours francs pour exercer son droit de rétractation sans avoir à justifier de motifs ni à payer de pénalités, à l'exception, le cas échéant, des frais de retour*». Ce délai court à compter de la réception pour les biens ou de l'acceptation de l'offre pour les prestations de services. Lorsqu'il expire un samedi, un dimanche ou un jour férié ou chômé, il est prorogé jusqu'au premier jour ouvrable suivant. Lorsque le droit de rétractation est exercé, le professionnel est tenu de rembourser sans délai le consommateur et, au plus tard, dans les trente jours suivant la date à laquelle ce droit a été exercé. Au-delà, la somme due est, de plein droit, productive d'intérêts au taux légal en vigueur.

Afin de rendre effective cette disposition, les articles L. 121-18 et L. 121-19 imposent aux vendeurs professionnels d'informer le consommateur de l'existence d'un droit de rétractation et de lui indiquer les modalités d'exercice de ce droit.

À ce stade, trois précisions importantes doivent être apportées. Tout d'abord et conformément à la loi, le consommateur ne peut invoquer un droit de rétractation que lorsqu'il est en présence d'un vendeur professionnel au sens du droit de la consommation. Si le vendeur est un particulier «non professionnel», ce droit n'existe pas.

Ensuite, dans certaines situations, le consommateur ne bénéficie pas du droit de rétractation. Cela vise en particulier :

– les contrats de fourniture de services dont l'exécution a commencé, avec l'accord du consommateur, avant la fin du délai de sept jours francs

- les contrats de fourniture de biens ou de services dont le prix est fonction de fluctuations des taux du marché financier;
- les contrats de fourniture de biens confectionnés selon les spécifications du consommateur ou nettement personnalisés ou qui, du fait de leur nature, ne peuvent être réexpédiés ou sont susceptibles de se détériorer ou de se périmérer rapidement;
- les contrats de fourniture d'enregistrements audio ou vidéo ou de logiciels informatiques lorsqu'ils ont été descellés par le consommateur;
- les contrats de fourniture de journaux, de périodiques ou de magazines.

Si l'on rapporte ces règles à la pratique des utilisateurs des plates-formes, on constate qu'un secteur important des relations commerciales visées par la présente recommandation en est ainsi exclu: celui des ventes de certains produits culturels (CD, DVD, VHS) qui ont été descellés (cas des biens d'occasion).

Enfin, tout vendeur, professionnel ou non, peut aller au-delà des textes et octroyer contractuellement au consommateur un régime de protection supplémentaire comme par exemple, reconnaître un droit de rétractation à l'acheteur alors même que le Code de la consommation ne lui accorderait pas cette faculté.

En la matière, les pratiques des utilisateurs et des plates-formes varient. Certains vendeurs indiquent clairement dans leurs offres une politique de retour. Des plates-formes peuvent également inciter leurs utilisateurs à faire de même.

En l'état actuel, il apparaît que certaines difficultés ont vu le jour:

- des consommateurs peuvent demander à bénéficier d'un droit de rétractation lors d'un achat auprès d'un vendeur non professionnel alors que le Code de la consommation ne leur ouvre pas une telle faculté;
- des vendeurs professionnels peuvent refuser l'application de ce principe par méconnaissance – volontaire ou non – des règles applicables.

Deux réponses pouvaient être apportées à ces constats: l'une reposant sur le vendeur, l'autre sur la plate-forme.

La première consisterait à recommander aux vendeurs d'indiquer l'existence éventuelle et les modalités d'un droit de rétractation dans leur annonce. Il s'agirait d'une application littérale du droit puisque le Code de la consommation fait peser sur eux le respect de cette obligation. Néanmoins, cela pourrait s'avérer insuffisant dès lors que les « nouveaux professionnels » pourraient ignorer les règles applicables voire, dans certains cas, refuser volontairement au consommateur un tel droit. Or, cette information – en matière de vente à distance, est essentielle pour le consommateur.

**La seconde, s'appuie sur les plates-formes de mise en relations qui détiennent la maîtrise technique de la présentation de l'offre. Il s'agit de leur recommander, afin de les faire participer à la construction de la confiance sur le réseau, de procéder à un affichage « en dur » soit sous la forme d'un message explicite, soit sous la forme d'un logotype d'une information de base sur le droit de rétractation ou encore un lien hypertexte dans la page de l'annonce. Cette information préciserait ainsi les conditions permettant à un consommateur d'invoquer un droit de rétractation et les limites apportées par la loi.**

Nonobstant cette information, il n'est pas actuellement possible de demander aux plates-formes d'afficher un message personnalisé en fonction du vendeur et des produits mis en vente, celles-ci n'opérant pas de vérification ou d'analyse systématique des annonces publiées par leurs vendeurs (et ainsi ne peuvent déterminer si les biens mis en vente bénéficient ou non d'un droit de rétractation).

En tout état de cause, **seul le vendeur ou son mandataire** (si un mandat a été donné en matière de droit de retour) **sont responsables de l'absence des mentions imposées par le Code de la consommation en matière de droit de rétractation, et a fortiori du refus d'exercice opposé par un professionnel à un consommateur**. Les courtiers en ligne sont, en outre, invités à informer leurs utilisateurs sur cette règle centrale du droit de la vente à distance.

### ***L'extension de l'application du droit de rétractation aux relations commerciales conclues entre deux particuliers***

À ce jour, la majorité des contrats formés par l'intermédiaire d'une plate-forme de mise en relation demeure encore le fait de deux consommateurs. Le droit de rétractation, disposition centrale du régime protecteur prévu en matière de vente à distance, quant à lui, ne s'applique pas puisque le vendeur n'est pas un professionnel<sup>192</sup>. Cette application stricte de la loi a pu être contestée. En effet, même si les relations commerciales font intervenir deux acteurs de même force économique, il n'en demeure pas moins qu'il s'agit toujours d'un contrat conclu à distance. Au cours des réflexions du groupe de travail, plusieurs arguments à la fois favorables et défavorables à ce choix ont pu être émis.

### **Les arguments favorables à une évolution du droit**

Deux principaux arguments ont pu être développés en faveur d'une extension aux vendeurs particuliers du régime protecteur applicable aux ventes à distance réalisées par un professionnel.

Le droit de la vente à distance tend à renforcer la protection du consommateur à l'occasion d'une activité commerciale au cours de laquelle, comme le précise l'article L. 121-16 du Code de la consommation, a lieu une vente conclue sans «*la présence physique simultanée des parties, entre un consommateur et un professionnel qui, pour la conclusion de ce contrat, utilisent exclusivement une ou plusieurs techniques de communication à distance*».

En matière de ventes conclues sur l'internet, le contrat est toujours conclu «*sans la présence physique simultanée des parties*» en utilisant «*exclusivement une ou plusieurs techniques de communication à distance*». C'est ce qui avait notamment incité le Conseil d'État, dans son rapport 'Internet et les réseaux numériques', à afficher comme objectif prioritaire, celui «*d'assurer aux consommateurs une protection d'un degré comparable, lors de transactions dématérialisées, à celle dont ils jouissent*

---

192. Il faut relever qu'avant la réforme d'août 2001, une ambiguïté demeurerait laissant penser que le régime de la vente à distance était susceptible de s'appliquer également aux relations commerciales entre particuliers. Voir à ce sujet: Jean BEAUCHARD, Droit de la distribution et de la consommation, PUF, Thémis, 1996, p.372. Cette interrogation est aujourd'hui levée avec la nouvelle formulation de l'article L. 121-16 du Code de la consommation.

à l'occasion de ventes à distance classiques »<sup>193</sup>. Il a été en cela largement suivi par la doctrine ainsi que la jurisprudence. Mais si l'on s'en tient à cette volonté d'appliquer à toutes les ventes à distance le même régime juridique, les relations commerciales entre deux particuliers auraient naturellement vocation à relever de ce régime spécifique.

D'une part, il s'agit de faire bénéficier le commerce en ligne sous toutes ses formes, des mêmes garanties que la vente à distance classique. D'autre part, il s'agit de protéger le consommateur par rapport à un vendeur non professionnel qui, contrairement à un vendeur professionnel, ne connaît pas forcément toutes les caractéristiques essentielles de son bien et peut en faire une description partielle. Reconnaître alors à l'acheteur un droit de rétractation permettrait ainsi d'atténuer l'impact d'une mauvaise information de la part du vendeur.

### **Les arguments défavorables à une évolution du droit**

À ces quelques thèses en faveur d'une extension du régime protecteur de la vente à distance, s'opposent d'autres arguments défavorables à toute modification du champ d'application du Code de la consommation.

Tout d'abord, le droit de la consommation cherche par nature à rééquilibrer une relation commerciale associant un acteur économiquement fort et informé (le vendeur professionnel) et un être faible, facilement influençable (le consommateur). Or, dans les relations commerciales entre deux particuliers, aucun déséquilibre ne peut être constaté, les deux parties étant de nature et de poids économique équivalents, ayant les mêmes connaissances et compétences.

Ensuite, l'application des dispositions relative au droit de rétractation pourrait avoir des conséquences dommageables pour le vendeur. Si ce droit est utile à l'acheteur qui n'a pas la possibilité de voir le bien préalablement à la conclusion du contrat, il constitue pour le vendeur une contrainte en terme de logistique (assurer le retour du bien, le remettre en vente) avec un impact financier non négligeable (remboursement des sommes versées par l'acheteur, montant qui peut ne plus être en sa possession, obligation de s'acquitter de nouveaux frais pour la remise en vente de l'objet). En pratique, l'application de ce droit aux relations commerciales entre deux particuliers pourrait porter préjudice à la vente (découragement du vendeur, refus « de bonne foi » du vendeur de faire application de cette règle en raison des contraintes, etc.)

En outre, les auditions ont également montré qu'il n'apparaît pas de demande clairement identifiée de la part des acheteurs en faveur d'une extension du champ d'application du droit de rétractation. Cela s'explique principalement par le fait que le montant des transactions demeure relativement faible (quelques dizaines d'euros en moyenne). En outre, dès lors qu'un consommateur est déçu par le bien reçu, il le remet généralement assez vite en vente, pouvant – dans certains cas – en tirer un revenu supérieur au montant dépensé pour son acquisition.

S'appuyant sur ces éléments, le Forum des droits sur l'internet n'a pas souhaité proposer une modification des dispositions du Code de la consommation en faveur

---

193. Conseil d'État, « Internet et les réseaux numériques », *La Doc. fr.*, 1998, p. 55.

de la prise en compte, dans le champ du régime applicable au droit de rétractation, des relations commerciales entre particuliers.

**Le Forum estime que le régime juridique existant encadrant les relations commerciales entre particuliers est suffisamment protecteur des parties; il doit cependant être connu et mis en œuvre par les parties.**

#### ***La responsabilité du fait des produits défectueux***

Conformément aux dispositions de l'article 1386-7 du Code civil et à l'article L. 221-1 du Code de la consommation<sup>194</sup>, le vendeur professionnel peut être responsable de plein droit du défaut de sécurité d'un produit dès lors que le producteur de ce produit demeure inconnu.

Il est donc rappelé aux vendeurs professionnels qu'ils peuvent être soumis à un tel régime de responsabilité en cas de défectuosité du produit vendu.

#### ***L'obligation de délivrance conforme***

Aux termes d'une ordonnance du 17 février 2005, un régime de garantie légale de conformité du bien livré s'applique à tout vendeur professionnel – pour les contrats conclus postérieurement au 19 février 2005. Ainsi, le nouvel article L. 211-4 du Code de la consommation prévoit que *«le vendeur est tenu de livrer un bien conforme au contrat et répond des défauts de conformité existant lors de la délivrance»*. Il répond également des défauts de conformité *«résultant de l'emballage, des instructions de montage ou de l'installation lorsque celle-ci a été mise à sa charge par le contrat ou a été réalisée sous sa responsabilité»*.

Afin de donner une portée plus forte à ce principe, l'article L. 211-5 du Code de la consommation définit ce qu'il faut entendre par conformité au contrat. Le bien devrait soit *«être propre à l'usage habituellement attendu d'un bien semblable et, le cas échéant: correspondre à la description donnée par le vendeur et posséder les qualités que celui-ci a présentées à l'acheteur sous forme d'échantillon ou de modèle [ou] présenter les qualités qu'un acheteur peut légitimement attendre eu égard aux déclarations publiques faites par le vendeur, par le producteur ou par son représentant, notamment dans la publicité ou l'étiquetage»*, soit *«présenter les caractéristiques définies d'un commun accord par les parties ou être propre à tout usage spécial recherché par l'acheteur, porté à la connaissance du vendeur et que ce dernier a accepté»*.

En application de l'article L. 211-7, les défauts de conformité *«qui apparaissent dans un délai de six mois à partir de la délivrance du bien»* sont présumés exister au moment de la délivrance, sauf preuve contraire. Cet élément permet donc à l'acheteur d'agir sur ce terrain même postérieurement à la réception du bien dès lors qu'un défaut apparaît dans un délai de 6 mois. Il devra néanmoins faire valoir son action dans un délai de deux ans à compter de la réception du bien.

---

194. *«Les produits et les services doivent, dans des conditions normales d'utilisation ou dans d'autres conditions raisonnablement prévisibles par le professionnel, présenter la sécurité à laquelle on peut légitimement s'attendre et ne pas porter atteinte à la santé des personnes»*.

Cependant, l'acheteur ne peut invoquer un défaut qu'il connaissait ou ne pouvait ignorer lorsqu'il a contracté. Les articles L. 211-9 et L. 211-10 ajoutent des précisions. En effet, en cas de défaut de conformité, l'acheteur peut choisir entre la réparation et le remplacement du bien. Le vendeur peut ne pas procéder selon le choix de l'acheteur si ce choix entraîne un coût manifestement disproportionné, compte tenu de la valeur du bien ou de l'importance du défaut.

Par ailleurs, si la réparation et le remplacement du bien sont impossibles, l'acheteur peut rendre le bien et se faire restituer le prix ou garder le bien et se faire rembourser une partie du prix. La même faculté lui est ouverte si la solution demandée, proposée ou convenue ne peut être mise en œuvre dans le délai d'un mois suivant la réclamation de l'acheteur ou si cette solution ne peut l'être sans inconvénient majeur pour celui-ci compte tenu de la nature du bien et de l'usage qu'il recherche.

L'annulation de la vente ne pourra, en tout état de cause, jamais être prononcée si le défaut de conformité est mineur. À noter, que le remplacement et la réparation du bien doivent avoir lieu sans aucun frais pour l'acheteur.

Ces règles s'appliquent à tout bien commercialisé par des professionnels, qu'ils soient neufs ou d'occasion.

Compte tenu de ces règles nouvelles, **le Forum invite les plates-formes à informer, dans leurs pages d'aide, leurs vendeurs professionnels sur le régime applicable au titre de la garantie de la conformité des biens livrés.**

## Le régime fiscal et social

### **Le régime social applicable aux vendeurs**

Lorsqu'un particulier exerce une activité économique même à titre accessoire, non salarié et non agricole, il relève du régime social des travailleurs indépendants. Ce régime implique un contact avec trois interlocuteurs: l'Organic pour son régime de retraite, la CANAM pour son régime d'assurance maladie et l'URSSAF pour la cotisation à la CAF, CSG et CRDS.

#### **La définition du travailleur indépendant**

Le travailleur indépendant se définit par opposition à la notion de travailleur salarié. Est travailleur indépendant, la personne physique qui exerce une activité professionnelle, même à titre accessoire, sans lien de subordination, sans intégration dans un service organisé et qui supporte un risque économique.

La notion d'activité professionnelle n'est pas définie clairement. C'est à la fois la jurisprudence et l'interprétation au cas par cas par l'URSSAF qui fixent cette définition.

Ainsi, n'est pas constitutive d'une activité professionnelle, une activité liée à la gestion du propre patrimoine de la personne (gestion d'un portefeuille d'action, vente de sa propre collection avec une plus-value, etc.). D'autres exemples peuvent être cités. Pour les chambres d'hôtes, l'administration fiscale a adopté un critère simple à savoir un montant au-dessus duquel l'exploitant est considéré comme un professionnel. À l'inverse, la jurisprudence sociale est frileuse et a plutôt choisi un faisceau de critères



(maîtrise de l'accueil des hôtes, partage de la maison familiale, partage des repas à la table du maître de maison).

En matière d'activités exercées sur l'internet, l'URSSAF a été amenée à prendre position sur le cas d'internautes possédant des sites internet et affichant des bannières publicitaires.

Une double réponse a été apportée :

– si le créateur du site est mineur, il n'exerce pas forcément une activité professionnelle même si les revenus sont importants ;

– à l'inverse si l'exploitant du site, majeur, met à jour fréquemment son site dans l'intention d'en tirer des revenus complémentaires, il devient travailleur indépendant.

En pratique, l'assujettissement au régime des travailleurs indépendants est dicté par les éléments suivants :

– l'activité doit être exercée de manière régulière ;

– elle doit être exercée à des fins lucratives (volonté de réaliser certaines opérations afin d'en tirer des revenus).

Par ailleurs, un autre critère peut également être utilisé : l'assujettissement fiscal. En effet, l'assiette sociale étant calquée sur l'assiette fiscale, un particulier déclarant des revenus en bénéfiques industriels et commerciaux (BIC) sera considéré comme ayant des revenus professionnels et donc devant s'inscrire au régime des travailleurs indépendants.

**Afin d'unifier le régime applicable aux vendeurs professionnels, le Forum des droits sur l'internet propose à l'URSSAF, à l'Organic et la CANAM d'adopter une définition commune de la notion de travailleur indépendant – en matière de ventes par un particulier sur l'internet – qui s'inspirerait de celle établie pour la notion de « professionnel de la vente à distance » dans la présente recommandation.**

#### **Les conséquences de l'assujettissement**

Un particulier devra s'acquitter de plusieurs types de cotisations : à l'URSSAF, à la CANAM et à l'Organic. Contrairement à l'URSSAF, l'Organic et la CANAM ne prévoient pas de mécanisme de dispense.

En pratique, l'URSSAF peut admettre que lorsque le particulier ne génère pas de revenus importants, seule une déclaration de ses revenus au titre des BIC est nécessaire. Mais, cette position n'est pas systématiquement suivie par les autres organismes dès lors que ces derniers n'ont pas inséré de mécanisme de dispense.

#### **Le régime fiscal applicable aux vendeurs**

Dès lors qu'il exerce une activité professionnelle, un vendeur est tenu de déclarer les sommes perçues auprès de l'administration fiscale.

### **L'assujettissement à l'impôt sur le revenu**

Les bénéfices réalisés par des **personnes physiques** et provenant de l'exercice d'une profession commerciale, industrielle ou artisanale sont considérés comme bénéfices industriels et commerciaux, pour l'application de l'impôt sur le revenu. Selon la doctrine administrative, «*l'exercice d'une profession industrielle et commerciale s'entend de l'accomplissement habituel, par des personnes agissant pour leur propre compte et poursuivant un but lucratif, d'opérations de caractère industriel ou commercial*».

Le droit fiscal a donc recours à plusieurs critères : l'habitude d'exercice de l'activité, le caractère lucratif de l'activité et l'exercice d'opérations commerciales.

**Afin d'adopter un champ d'application commun aux dispositions visant la notion de professionnel, le Forum des droits sur l'internet invite l'administration fiscale à retenir, comme critères d'assujettissement, ceux préalablement établis pour la définition du «vendeur professionnel».**

De même, les bénéfices réalisés par des personnes morales seront, quant à eux, imposés dans la catégorie de l'impôt sur les sociétés.

### **L'assujettissement à la taxe sur la valeur ajoutée**

Par ailleurs, un professionnel n'est pas redevable de la taxe sur la valeur ajoutée (TVA) dès lors que le montant annuel des sommes perçues au titre de son activité n'excède pas certains plafonds fixés en application de l'article 293 B du code général des impôts.

En franchise de TVA, le vendeur qui émet une facture doit préciser explicitement que «*la TVA n'est pas applicable conformément à l'article 293 B du CGI*».

## **Conclusion**

Comme indiqué précédemment, le commerce entre particuliers constitue une nouvelle forme d'achat. Selon l'étude FEVAD – Mediamétrie/Netrating de juin 2005, 39,4 % des internautes déclaraient avoir utilisé des sites permettant une mise en relation directe des acheteurs avec des vendeurs pour l'achat ou la vente de produits neufs ou d'occasion. Les principaux produits échangés sur ces plates-formes demeuraient les produits culturels (18,1 %), les produits techniques (13,9 %), l'habillement et les jouets (8,3 % chacun) et les produits liés à l'univers de la maison (6,1 %).

Nonobstant le fait que les plates-formes de mise en relation soient ou non mandataires du vendeur, elles jouent un rôle central dans la conclusion d'une transaction entre deux de leurs utilisateurs. En offrant un lieu d'échange et de rencontre, elles permettent à une relation économique de se nouer entre un vendeur, professionnel ou non, et un acheteur.

Ainsi, et au-delà des obligations juridiques particulières que l'on peut leur reconnaître, elles constituent indéniablement des intermédiaires commerciaux. À ce titre, les

plates-formes se doivent de participer à la construction de la confiance sur le réseau au travers notamment du développement d'une information pédagogique sur leur site.

En effet, si le cadre juridique existant pour les relations commerciales entre particuliers est protecteur, il demeure peu connu des utilisateurs. Ainsi, et malgré les pages d'information élaborées par certaines plates-formes, il apparaît que les consommateurs français – contrairement aux consommateurs allemands comme l'ont montré les auditions – se renseignent rarement en amont d'une transaction mais uniquement lorsqu'un différend ou un problème naît.

Il est donc nécessaire d'avoir une démarche pédagogique à destination des acheteurs et vendeurs, utilisateurs des plates-formes de mises en relation.

**Le Forum des droits sur l'internet invite les plates-formes à mettre en place une page destinée à informer leurs utilisateurs des règles principales applicables dans le secteur des ventes entre particuliers ou entre un professionnel et un consommateur.**

À cette page devraient être associés des liens hypertextes pointant vers des sites d'information (le site de la DGCCRF ou le site d'information du Forum des droits sur l'internet: DroitDuNet.fr) permettant ainsi à l'utilisateur d'obtenir de plus amples renseignements. En tout état de cause, la plate-forme ne serait pas tenue de procéder à une diffusion exhaustive de toutes les règles applicables.

**Cette page d'information devrait être facilement accessible et compréhensible** afin de permettre à un non juriste de saisir rapidement les principes de base encadrant la transaction commerciale ainsi conclue.

Des actions d'information et de sensibilisation similaires pourraient également être menées notamment dans le cadre des **opérations menées par les pouvoirs publics.**

## Annexe 1

### **Composition du groupe de travail**

**Jean-Luc DANIEL**, bureau Droit de la consommation, Direction générale à la concurrence, à la consommation et à la répression des fraudes (DGCCRF)

**Bénédicte DELEPORTE**, directrice juridique, eBay France

**Véronique DONNADIEU**, juriste, association CLCV

**Patricia FOUCHER**, juriste, Institut national de la consommation

**Jérôme HUET**, professeur de droit à l'université de Paris II

**Pierre KOSCIUSKO-MORIZET**, président-directeur général et **Pierre KRINGS**, directeur général, Priceminister

**Bertrand PINEAU**, responsable des nouvelles technologies et du système d'information, Fédération de la vente à distance (FEVAD)

La coordination des travaux était assurée par **Benoît TABAKA**, chargé de mission au Forum, rapporteur du groupe

## Annexe 2

### **Auditions réalisées par le groupe de travail**

Le groupe de travail a procédé aux auditions de :

**Anne AURIANT**, internaute

**Grégory BOUTTE**, directeur général, eBay France

**Aymeric CHOTARD**, président-directeur général, 2xMoinsCher

**Carola CISTERNAS**, internaute

**Philippe COMMEROT**, internaute

**Bénédicte DELEPORTE**, directrice juridique, eBay France

**Véronique DONNADIEU**, juriste, association CLCV

**Jérôme FRITEAU**, sous-direction juridique et réglementaire, ACOSS

**Pierre KOSCIUSKO-MORIZET**, président-directeur général, Priceminister

**Martine MERIGEAU**, directrice, Centre européen des consommateurs de Kehl

**Jean-Pierre PIZZIO**, professeur à l'université de Bourgogne

**Christine RIEFA**, *Lecturer in Law*, université de Brunel (Royaume-Uni)

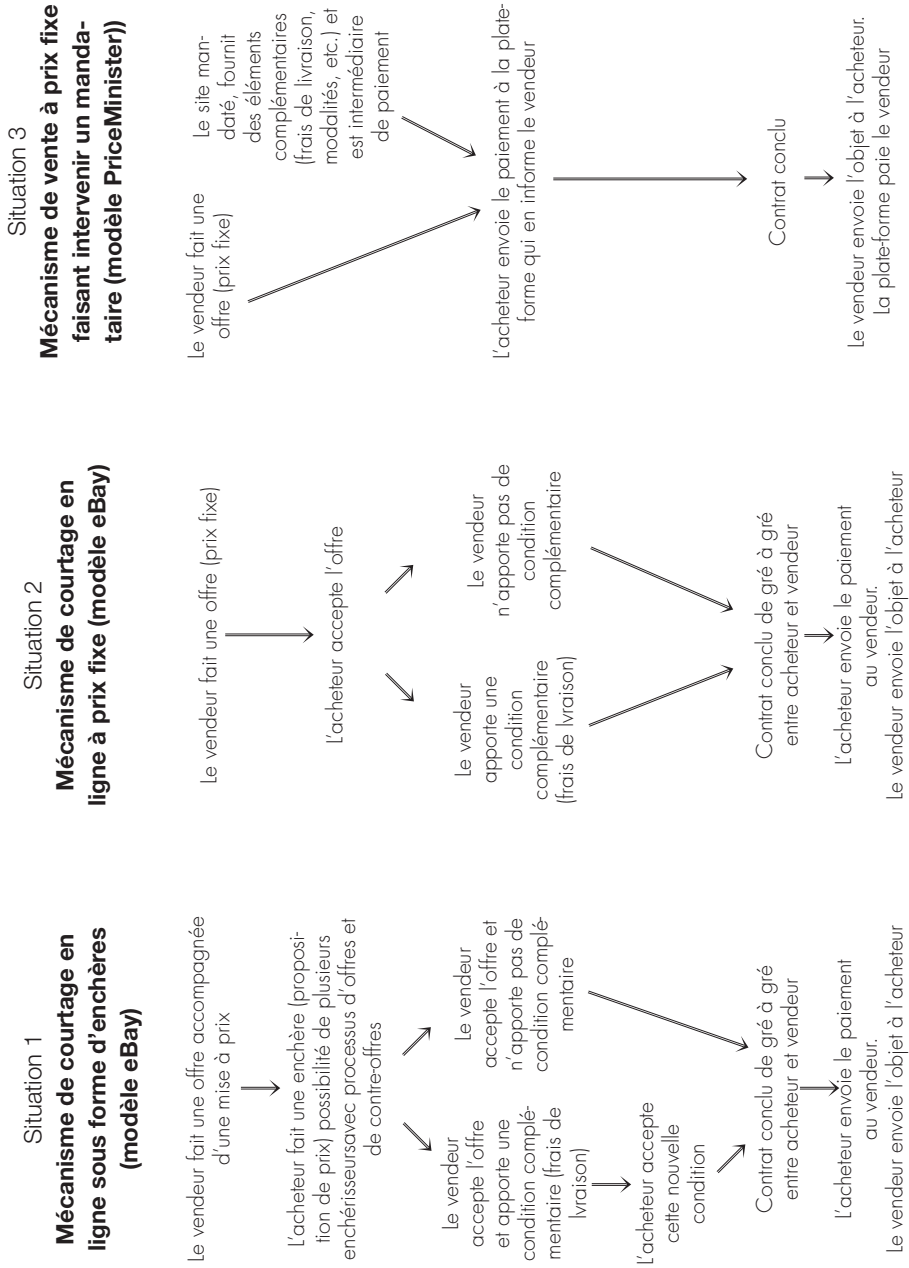
**Stéphane SCHMIDT**, juriste, Centre européen des consommateurs de Kehl

**Philippe STOFFEL-MUNCK**, professeur à la faculté de droit de Paris Saint-Maur

Enfin, le groupe de travail tient à remercier **Cédric MANARA**, professeur à l'*Edhec Business School* de Nice pour les précieuses réponses apportées à ses interrogations.

## Annexe 3

# Schémas synthétiques du processus contractuel



# La conservation électronique des documents

*Recommandation publiée le 1<sup>er</sup> décembre 2005*

## Introduction

La dématérialisation des documents tend à se généraliser au sein des entreprises. Les échanges internes, avec les fournisseurs et les clients se font de plus en plus souvent sans recours au support papier. De ce fait, se pose la question de la conservation électronique des documents, de ses modalités et de son cadre juridique.

La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique a amorcé une réforme en profondeur du droit de la preuve. En reconnaissant une existence juridique à l'écrit sous forme électronique et en lui attribuant une force probante équivalente à l'écrit sur support papier, le législateur a engagé la dématérialisation des écrits.

Cependant, si les textes juridiques concernant l'écrit sous forme électronique font de la conservation du document électronique l'une des conditions essentielles de sa valeur juridique, aucun n'évoque les modalités légales de cette conservation<sup>195</sup>. On voit ainsi qu'un aspect primordial du cycle de vie du document électronique n'a pas encore été appréhendé.

Or, il est nécessaire de s'assurer que les documents électroniques constitueront une preuve valable (recevable en justice et ayant force probante) au même titre que les documents sur support papier, et ceci, plusieurs années après leur versement dans les systèmes de conservation. Cette garantie de préservation du statut d'origine du document constitue un enjeu majeur de la conservation. Il convient également de s'assurer que les documents et les informations qu'ils contiennent restent accessibles et exploitables dans le temps.

À cela s'ajoutent des considérations d'ordre technique. L'actuel processus de dématérialisation des documents conduit bien souvent à faire émerger des questions qui ne se posaient pas dans l'environnement traditionnel. Un certain nombre d'entreprises, par souci de «sécuriser» leur chaîne de production et de stockage des documents électroniques, se dotent d'outils ou de procédures complexes qui loin d'apporter les résultats escomptés risquent, à terme, de s'avérer inutiles, voire de produire des effets néfastes sur les documents conservés.

---

195. La seule exception étant les dispositions du Code Général des Impôts et leurs textes d'application concernant un domaine très spécifique: les factures transmises par voie électronique (art. 289 du CGI, décret n° 2003-659 du 18 juillet 2003, instruction de la DGI du 7 août 2003).

Les obligations de conservation qui pèsent désormais sur les entreprises nécessitent que soient précisés les conditions et les moyens de la conservation sans pour autant atténuer la dynamique du secteur. Pour cela il faut instaurer un climat de confiance encadrant ces nouvelles pratiques.

C'est à partir de ce constat et dans cet objectif que le Forum des droits sur l'internet et la Mission Économie Numérique du Ministère de l'Économie et des Finances et de l'Industrie ont souhaité mettre en place un groupe de travail sur le sujet. Ce groupe interdisciplinaire, constitué de juristes, d'informaticiens, de praticiens de l'archivage au sein des entreprises et de représentants des administrations a été formé durant l'année 2004<sup>196</sup>.

Le groupe s'est attaché à faire émerger des solutions pratiques et juridiquement acceptables pour guider l'ensemble des acteurs et favoriser la confiance dans ce domaine.

Cette orientation est apparue d'autant plus utile que les auditions menées par le groupe de travail ont montré que peu d'entreprises disposent d'une politique définie concernant l'archivage.

Le groupe a procédé, en complément de ses séances de travail collectif, à des auditions de personnalités, reconnues pour leurs expériences et leurs connaissances des enjeux relatifs à la conservation des documents, mais aussi d'entreprises ou encore d'organismes publics ayant ou souhaitant mettre en place et gérer la conservation électronique de leurs documents.

Les travaux du groupe n'ont porté que sur le secteur privé mais, afin de préserver la cohérence globale du traitement de la question de la conservation électronique, se sont largement intéressés aux éléments existant dans le secteur public. Les intérêts spécifiques des particuliers et des consommateurs n'ont pas été négligés.

La présente recommandation a un double objectif: d'une part, caractériser l'intégrité des documents électroniques, cette notion apparaissant comme centrale dans l'architecture juridique mise en place par la loi du 13 mars 2000; d'autre part, instaurer la confiance dans ce domaine en fournissant aux acteurs les moyens de mettre en place des processus de conservation garantissant l'intégrité des documents.

Dans le cadre de la présente recommandation, le terme de conservation a été préféré à celui d'archivage. Le groupe a estimé que ce terme plus précis correspondait mieux à ses réflexions. En outre, la loi précitée désigne l'opération de stockage de l'écrit par le terme de « *conservation* ». Il apparaît que ce choix de langage est dicté par une volonté de neutralité du législateur. Pour toutes ces raisons, ce terme a été retenu par le groupe.

Enfin, il convient de noter que la démarche des travaux du groupe s'est inscrite dans le cadre des réflexions internationales menées dans ce domaine. En effet, de nombreux pays tentent également de gérer la dématérialisation des écrits et le problème de la conservation électronique des documents. Cependant, aucun

---

196. Voir en annexe la composition du groupe de travail.



consensus international ne paraît exister et les approches privilégient des solutions diverses même si le recours au « métadonnées »<sup>197</sup> est largement partagé par la plupart des pays.

Le présent rapport a été soumis à l'ensemble des membres du Forum des droits sur l'internet et adopté par le Conseil d'orientation du Forum dans sa séance du 21 novembre 2005.

## Plan du rapport

La première partie de la présente recommandation présente un état des lieux des principaux éléments juridiques et techniques qui doivent être pris en compte dans la démarche de conservation des documents sous forme électronique.

La seconde partie se propose de fournir des recommandations pratiques permettant de satisfaire à l'objectif de conservation d'un document intègre.

## **La conservation électronique des documents : état des lieux**

### Le cadre juridique de la conservation des documents

#### **La conservation : un élément de la valeur probatoire de l'écrit électronique**

Du seul point de vue juridique, la finalité principale de la conservation réside dans la possibilité de pouvoir restituer à un temps donné un document pour répondre à un besoin de preuve.

Ainsi, en matière civile, depuis la loi du 13 mars 2000 relative à la preuve et à la signature électronique et l'adoption du nouvel article 1316 du Code civil « *la preuve littérale ou preuve par écrit résulte d'une suite de lettres, de caractères, de chiffres, ou de tout autres signes ou symboles dotés d'une signification intelligibles, quels que soient leur support et leur modalité de transmission* ».

La définition de la preuve par écrit est donc extensive, ce qui valide toutes formes d'écrits, y compris mais non exclusivement ceux sous forme électronique.

Selon le nouvel article 1316-1 du Code civil, tel que créé par la loi du 13 mars 2000, « *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

Alors que la loi et plusieurs textes réglementaires précisent les notions d'identification et d'établissement de l'écrit sous forme électronique, aucun texte ne précise

---

197. Le terme est expliqué en page 198.

les critères permettant de conserver électroniquement un écrit dans des conditions garantissant son intégrité<sup>198</sup>.

Ce constat est préoccupant car même si toutes les prétentions ne se prouvent pas de la même façon, certaines supposent la production d'un écrit. Dans ce cadre, la conservation de l'écrit intègre et sa restitution déterminent l'issue d'un litige.

La prise en considération de ces éléments permet de délimiter le champ d'application de la présente recommandation du point de vue du droit probatoire: celle-ci ne vise pas la conservation des actes authentiques mais uniquement celle des écrits sous forme électronique.

Les actes authentiques électroniques<sup>199</sup>, quant à eux, font l'objet de deux décrets<sup>200</sup> traitant de la question de leur établissement et de leur conservation.

L'écrit sous seing privé<sup>201</sup>, en tant que manifestation de la volonté, n'exige en principe aucun support matériel pour exister. Par exception toutefois, la formalisation d'un écrit constatant l'acte juridique peut être nécessaire, soit pour assurer la validité de l'acte lui-même, soit pour en permettre la preuve.

• **En matière civile**, les actes juridiques dont l'objet est supérieur à 1500 euros<sup>202</sup> ne peuvent être prouvés que par certains moyens. Il s'agit essentiellement de l'écrit<sup>203</sup>. Les actes juridiques dont l'objet est inférieur à ce montant échappent à cette règle et la preuve de leur contenu ou de leur existence peut être apportée par tous moyens.

• **En matière commerciale**, l'article L. 110-3 du Code de commerce pose le principe de la liberté de la preuve: «*À l'égard des commerçants, les actes de commerce peuvent se prouver par tous moyens à moins qu'il n'en soit autrement disposé par la loi*». Sauf cas spéciaux, les commerçants disposent donc d'une liberté de preuve pour les actes de commerce.

• **Entre un commerçant et un consommateur**, le régime de preuve est dit «mixte»: le consommateur peut bénéficier d'un régime de la liberté de la preuve, alors que le

---

198. Voir page 203.

199. L'acte authentique est, en droit français, au sommet de la hiérarchie probatoire mise en place par le Code civil, donc au-dessus de la preuve littérale. C'est un moyen de preuve quasi absolu car sa validité ne peut être contestée que dans le cadre d'une procédure particulièrement exigeante, l'inscription de faux, réglementée par les articles 303 et suivants du nouveau Code de procédure civile. L'acte authentique est rédigé par un officier public (un notaire ou un huissier de justice).

200. Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires et décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice.

201. L'acte juridique a pour origine la volonté d'une ou plusieurs personnes. Il a pour objectif de produire des effets juridiques. Par exemple, un contrat de travail est un acte juridique résultant de la volonté d'un employeur et d'un salarié.

202. Décret n° 2004-836 du 20 août 2004, art. 56 modifiant le décret n° 80-533 du 15 juillet 1980 pris pour l'application de l'article 1341 du Code civil.

203. Les preuves sont rapportées par l'écrit, l'aveu ou le serment (art. 1356 et s., 1361 et s. du Code civil).

commerçant est tenu aux dispositions plus strictes du Code civil et donc à la preuve par écrit lorsque celle-ci est exigée.

Enfin, en l'absence de dispositions légales expressément applicables à la conservation électronique de documents et de jurisprudence sur l'applicabilité du régime juridique des copies de document à la conservation électronique, il est possible de recourir, dans une certaine mesure, à des conventions de preuve pour faciliter la preuve et les échanges. Une convention de preuve permet aux parties de décider contractuellement d'accepter certains modes de preuve et de reconnaître la valeur probatoire des écrits électroniques qu'elles échangent et par là même les modalités de conservation de ces actes pour leur attribuer une force probante. La jurisprudence puis la loi ont admis l'utilisation de telles conventions de preuve<sup>204</sup>.

Cependant, il convient de rappeler que le rapport du Conseil d'État *Internet et les réseaux numériques*<sup>205</sup> a considéré que «*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*». Ces conventions n'ayant d'effet qu'entre les parties qui les concluent, elles ne sauraient résoudre le problème de l'efficacité d'un système de conservation électronique opposable à tous.

## **Les textes spécifiques à la conservation électronique des documents**

La conservation d'un document électronique est précisée, voire imposée dans plusieurs textes législatifs ou réglementaires. Ces textes ont trait à des domaines très variés et sont de diverses origines. S'ils précisent des dispositions applicables dans des cas particuliers (factures, actes authentiques), aucun ne donne d'indications générales sur les modalités devant entourer la conservation d'un document électronique.

---

204. La validité de ces conventions a été reconnue depuis plusieurs années par la jurisprudence (Cass. civ. 1<sup>re</sup>, Sté Crédicas, 8 nov. 1989) et la loi n° 2000-230 du 13 mars 2000 a consacré leur existence par le biais de l'article 1316-2 du Code civil (art. 1316-2 Code civil : «*Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable, quel qu'en soit le support*»), sans toutefois en fixer les conditions de validité. Le juge reste ainsi seul compétent pour apprécier la validité de la convention.

205. Rapport du Conseil d'État, «*Internet et les réseaux numériques*». La Documentation française, 1998.

## **Deux textes législatifs prévoient la fonction de conservation mais ils restent lacunaires**

Un premier dispositif faisant référence à la conservation des documents se trouve dans l'article 25<sup>206</sup> de la loi du 21 juin 2004 pour la confiance dans l'économie numérique<sup>207</sup> qui complète l'article 1369-1 du Code civil en prévoyant l'obligation, pour le vendeur, de mentionner dans ses conditions générales de vente: «*En cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre*». Ce même article 25 insère un nouvel article 1108-1 dans le Code civil qui dispose que «*Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4*». On se rend compte que, tant que les modalités de conservation du 1316-1 ne sont pas clairement précisées, cet article risque d'être, dans les faits, source de difficultés d'application.

Plus spécifiquement, l'article 27 de la loi crée, dans le Code de la consommation, un nouvel article L. 134-2 qui dispose que «*Lorsque le contrat est conclu par voie électronique et qu'il porte sur une somme égale ou supérieure à un montant fixé par décret<sup>208</sup>, le contractant professionnel assure la conservation de l'écrit qui le constate pendant un délai déterminé par ce même décret<sup>209</sup> et en garantit à tout moment l'accès à son cocontractant si celui-ci en fait la demande*». Or, une nouvelle fois, rien ne précise la façon dont le professionnel doit assurer la conservation de cet écrit.

Des conditions de conservation des archives électroniques ont néanmoins pu être précisées en matière de facture électronique<sup>210</sup>. Le nouveau dispositif légal et réglementaire<sup>211</sup> assure la transposition de la directive européenne du 20 décembre 2001 prise «*en vue de simplifier et moderniser les conditions imposées à la facturation en matière de T.V.A.*». Cependant, le caractère limité et particulièrement précis de ces conditions de conservation empêche de les retenir comme principes généraux de conservation des documents électroniques.

---

206. Chapitre VII, Des contrats sous forme électronique. Art. 1369-1: «*Quiconque propose, à titre professionnel, par voie électronique, la fourniture de biens ou la prestation de services, met à disposition les conditions contractuelles applicables d'une manière qui permette leur conservation et leur reproduction. Sans préjudice des conditions de validité mentionnées dans l'offre, son auteur reste engagé par elle tant qu'elle est accessible par voie électronique de son fait. L'offre énonce en outre (...) 4° En cas d'archivage du contrat, les modalités de cet archivage par l'auteur de l'offre et les conditions d'accès au contrat archivé.*»

207. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

208. Décret n° 2005-137 du 16 février 2005 qui fixe dans son article 1 à 120 euros le montant à partir duquel l'archivage du contrat doit avoir lieu.

209. Décret n° 2005-137 du 16 février 2005: l'article 2 précise que le délai de conservation «*est fixé à 10 ans à compter de la conclusion du contrat lorsque la livraison du bien ou l'exécution de la prestation est immédiate. Dans le cas contraire, le délai court à compter de la conclusion du contrat jusqu'à la date de livraison du bien ou de l'exécution de la prestation et pendant une durée de dix ans à compter de celle-ci.*»

210. Code général des impôts, annexe 3, article 96F «*I. -1. a. Les factures émises dans les conditions visées au premier alinéa du V de l'article 289 du Code général des impôts tiennent lieu de factures d'origine lorsque l'authenticité de leur origine et l'intégrité de leur contenu sont garanties au moyen d'une signature électronique.*» [extrait].

211. Loi de finances rectificative pour 2002 n° 2002-1576 du 30 décembre 2002, décret n° 2003-659 du 18 juillet 2003, instruction fiscale n° 136 du 7 août 2003.

C'est ensuite l'ordonnance du 6 juin 2005 relative à la commercialisation à distance de services financiers auprès des consommateurs qui transpose la directive 2002/65/CE.

Les articles<sup>212</sup> nouveaux précisent que «*Le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition et auquel il a accès en temps utile et avant tout engagement, les conditions contractuelles ainsi que les informations mentionnées à l'article L. 121-20-10*» [extrait].

Cette notion de support durable est issue de la directive concernant la commercialisation à distance de services financiers auprès des consommateurs<sup>213</sup>. Elle y est définie comme étant «*tout instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées*»<sup>214</sup>.

De ce fait, le consommateur doit être mis en mesure de conserver pour s'y référer pendant un laps de temps adapté, les informations qui lui sont transmises.

### **Des textes spécifiques portent sur la conservation des certificats électroniques**

Il s'agit pour l'essentiel de la directive européenne du 13 décembre 1999<sup>215</sup>, de la loi du 13 mars 2000 et son décret d'application du 30 mars 2001<sup>216</sup> et enfin de l'arrêté du 26 juillet 2004<sup>217</sup>.

La directive européenne du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques dans son annexe II, relative aux «*Exigences concernant les prestataires de services de certification délivrant des certificats qualifiés*», dispose que les prestataires de services doivent «*enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par voie électronique*» et «*utiliser des systèmes fiables pour stocker les certificats*»; aucune information n'étant donnée sur la fiabilité exigée pour le stockage des certificats.

---

212. Ordonnance n° 2005-648 du 6 juin 2005 relative à la commercialisation à distance de services financiers auprès des consommateurs, art. 2 créant l'article L. 121-20-11 du Code de la consommation.

213. Directive 2002/65/CE du Parlement Européen et du Conseil du 23 septembre 2002.

214. Art. 2 de la directive précitée.

215. Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques: *JOCE* n° L 013 du 19/01/2000 p. 12-20.

216. Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique.

217. Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation.

L'article 6-II, k) du décret d'application du 30 mars 2001 énonce qu'un prestataire de services de certification électronique (PSCE) doit « *Conserver, éventuellement sous forme électronique, toutes les informations relatives au certificat électronique qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique* », mais n'indique pas précisément quels types d'informations doivent être conservés et les façons dont elles doivent l'être.

De même, la clause a), II, de l'article 6 de ce même décret prévoit, d'une manière générale, que le PSCE « *doit faire preuve de la fiabilité des services de certification électronique qu'il fournit* ». Il en résulte que les PSCE doivent pouvoir démontrer que les systèmes d'archivage concourant aux services de certification fournis sont fiables.

Enfin, il faut mentionner la loi type de la Commission des Nations Unies pour le Droit Commercial International sur le commerce électronique de 1996<sup>218</sup>. Cette loi a pour objectif d'offrir aux législateurs nationaux un ensemble de règles internationalement acceptables sur la manière de créer un environnement juridique plus sûr pour contribuer au développement du commerce électronique. Les principes énoncés dans la loi type se veulent également utiles pour les particuliers qui pratiquent aussi le commerce électronique.

#### **La délibération de la Commission nationale de l'informatique et des libertés**

Enfin, il convient de mentionner un texte qui traite de l'enjeu important de l'archivage électronique dans les entreprises.

La Commission nationale de l'informatique et des libertés a adopté en octobre 2005 une délibération sur l'archivage électronique dans les entreprises<sup>219</sup>.

Dans sa recommandation, la CNIL rappelle que les informations faisant l'objet d'un archivage peuvent comporter des données à caractère personnel et sont, dès lors, protégées par les dispositions de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 relative aux fichiers, à l'informatique et aux libertés.

Face à la mémoire de l'informatique, la CNIL considère que seul le principe du « droit » à l'oubli consacré par l'article 6-5° de la loi du 6 janvier 1978 peut garantir que les données collectées sur les individus ne soient pas conservées, dans les entreprises, pour des durées qui pourraient apparaître comme manifestation excessives. La CNIL préconise que la conservation soit divisée en trois périodes de temps (archives courantes, intermédiaires et définitives). La CNIL recommande également que le responsable du traitement établisse des procédures aptes à gérer des durées de conservation distinctes selon les catégories de données qu'il collecte.

S'agissant des archives intermédiaires, la CNIL recommande que l'accès à celles-ci soit limité à un service spécifique (par exemple un service du contentieux). S'agissant

---

218. Loi type de la CNUDCI sur le commerce électronique, résolution 51/162 de l'assemblée générale du 16 décembre 1996, voir article 10, <http://www.uncitral.org/pdf/french/texts/electcom/ML-EC-F.pdf>

219. Délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel.

des archives définitives, celles-ci doivent être conservées sur un support indépendant avec accès limité au seul service habilité (par exemple la direction des archives de l'entreprise).

\*  
\* \*

On se rend compte que les textes se réfèrent de plus en plus souvent à la nécessité de conserver et font dans la plupart des cas de cette conservation une des conditions de la confiance et de la valeur probante du document numérique. Cependant, et à la différence de ce qui a été opéré pour la reconnaissance de la signature électronique, aucun texte ne donne d'indication ou ne propose de critères juridiques précis concernant la qualification de « conservation intègre » nécessaire pour un nombre de plus en plus élevé de documents électroniques.

Dès lors, tant que les modalités de conservation de l'article 1316-1 du Code civil ne seront pas clairement précisées, ces textes risquent de poser des difficultés lors de leur mise en œuvre

## Le cadre technique entourant la conservation électronique des documents

Le cadre technique entourant la conservation électronique des documents peut être décrit par les outils auxquels recourent les systèmes informatisés, les procédures mises en place mais aussi, à un niveau plus général, par des normes.

### **Les outils techniques de la conservation**

En fonction des objectifs assignés, des outils techniques doivent être combinés pour atteindre un résultat déterminé. L'intégrité des documents électroniques conservés dépend, pour partie, de l'association cohérente de ces différents outils. Il est donc important de connaître leurs caractéristiques principales.

#### **Les formats**

Tout processus informatisé et notamment celui entourant la conservation électronique, repose sur l'emploi d'un format de codage. Le codage exprime la manière dont l'information est structurée au sein du fichier de façon à pouvoir être conservée, transmise et échangée.

En considérant la notion juridique de « *lisibilité* »<sup>220</sup> dans le contexte des documents électroniques, il convient de rappeler que tout codage est inclus dans une chaîne d'autres codages<sup>221</sup> et qu'il fait également partie d'une chaîne d'éléments qui le rendent intelligible (par exemple, un fichier *Word* est lié au logiciel *Word*, lui-même

---

220. Voir page 203.

221. Le simple affichage d'une lettre à l'écran est le fruit d'une interaction de ces codages : codage des caractères (ASCII, *Unicode*), polices de caractères (*PostScript*, *TrueType*), structuration de l'information sous forme d'un document (*Word*, *Wordperfect*), structuration de l'information (XML).

mis en œuvre sur un certain modèle d'ordinateur et par un certain système d'exploitation): la notion de lisibilité d'un document électronique ne peut par conséquent être comprise en dehors de l'interaction de l'ensemble de ces encodages avec le logiciel et le matériel informatique conçus pour les interpréter.

On peut classer les formats suivant le caractère ouvert ou fermé de leurs spécifications, c'est-à-dire dont la « fabrication » est connue ou non. Des formats sont dits :

- « ouverts » quand les spécifications sont publiques<sup>222</sup>,
- « fermés » quand les spécifications sont tenues secrètes par le propriétaire,
- « propriétaires » lorsqu'ils sont définis par un organisme propriétaire et leur utilisation soumise à des droits,
- « standards » lorsqu'ils sont définis et adoptés par un organisme de normalisation, et que leur utilisation est libre.

Il convient donc de mesurer à quel point les choix techniques opérés *a priori* peuvent retentir sur la restitution du document *a posteriori*. Les choix relatifs à l'environnement de production du document (notamment en termes d'architecture matérielle, de système d'exploitation, d'applicatif et de format) affecteront son processus de conservation.

Il est donc indispensable de choisir, dès l'origine, des formats considérés comme pérennes et d'effectuer, en temps voulu, les conversions nécessaires pour maintenir la lisibilité des données.

C'est pour ces raisons que l'Agence pour le développement de l'administration électronique (ADAE) a édicté un cadre commun d'interopérabilité précisant les standards et normes qui doivent être utilisés par l'administration. Ce cadre concerne notamment les formats de documents (version publiée en septembre 2003). Son application sera renforcée dans le cadre du prochain référentiel interministériel d'interopérabilité<sup>223</sup>.

### **Les supports**

Les principales caractéristiques que l'on attend d'un support d'archivage sont la pérennité et la fiabilité. Dans le choix d'un support, il conviendra de tenir compte de l'infrastructure logicielle et matérielle qui permettra d'en exploiter son contenu. Tout processus de conservation électronique restant dans la dépendance des supports de stockage utilisés, il conviendra de veiller à ce que les choix opérés soient compatibles avec les exigences assignées aux systèmes de conservation.

La pérennité des enregistrements qui pourrait être apportée par un type de support ne doit pas faire oublier la nécessité (comme dans tout système d'information) de disposer de sauvegardes.

---

222. La loi du 21 juin 2004 définit le *standard ouvert* comme « tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérable et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre ».

223. [http://www.adae.gouv.fr/article.php3?id\\_article=219](http://www.adae.gouv.fr/article.php3?id_article=219)



Les supports actuellement utilisés pour l'archivage sont les suivants :

**Les supports optiques**, à savoir :

- les disques optiques de technologie WORM (*Write Once Read Many*) qui ont la propriété d'interdire toute modification des données enregistrées. C'est actuellement le support le plus utilisé pour archiver des volumes relativement réduits. Ce type de support est privilégié dans les systèmes de conservation qui se réfèrent à la norme NF Z 42-013 ;
- les disques optiques réinscriptibles. Plusieurs technologies sont disponibles. À des fins d'archivage, on utilise principalement des supports dont la réécriture est protégée par un procédé logiciel.

**Les supports magnétiques**, à savoir :

- les différents types de supports magnétiques (cartouches, bandes, disques) ;
- les disques magnétiques peuvent être intégrés dans des solutions logicielles protégeant leur réécriture.

**Les supports analogiques**, à savoir :

- les microformes COM (*Computer Output Microform*) dans la mesure où il s'agit d'un support durable au sens de la copie fidèle et durable. L'usage de ce support suppose une rematérialisation en fin de chaîne du document électronique. Il s'agit des supports utilisés dans le cadre de la norme NF Z 43-400.

**Les métadonnées**

Le terme de « métadonnées » est utilisé pour définir l'ensemble des informations techniques et descriptives ajoutées au document pour mieux le qualifier. Ces informations décrivent le contexte, la structure et le contenu des documents, ainsi que sa gestion dans le temps. Les métadonnées<sup>224</sup> sont indispensables pour retrouver et accéder aux informations tout au long du cycle de vie des documents.

Plusieurs normes les évoquent, notamment la norme sur le « *records management* » et la norme OAIS<sup>225</sup> (*Open Archival Information System*).

L'utilisation des métadonnées est l'un des éléments permettant de documenter et de suivre le processus de conservation. C'est notamment le cas des migrations de documents signés par un procédé de signature cryptographique à clef publique où il sera nécessaire d'inscrire dans les métadonnées associées au document les informations issues des procédures de vérification de signature<sup>226</sup>. Cette place fondamentale des métadonnées est reconnue au niveau international. L'utilisation des métadonnées

---

224. Elles peuvent être classées :– selon le contenu avec des métadonnées descriptives : titre, auteur, date, mots-clés ; métadonnées contextuelles (provenance, contexte d'établissement, de création, fonds d'appartenance)– selon la forme qui peut être structurelle : structure logique ou physique (pagination d'un livre, structure d'un inventaire) ; technique : support, taille, format, langue, signature électronique, type de compression, plate-forme utilisée ;– selon l'usage : utilisateurs finaux, droits d'accès ; informations de gestion quant à l'archivage (identifiant, date de versement..) ; fréquence d'accès... Enfin, il convient de noter qu'il existe différents formats de métadonnées.

225. Voir page 200.

226. Voir page 209.

permet également de participer à l'intégrité de la conservation. Les métadonnées participent, par les informations qu'elles contiennent, à la vérification de certains critères permettant de s'assurer de l'intégrité du document (spécialement la traçabilité).

### **La signature cryptographique à clef publique**

Les procédés de signature cryptographique (ou « signatures à clef publique ») sont des techniques qui permettent de garantir l'intégrité et l'origine d'un document électronique au sens où la signature qui en résulte dépend à la fois de l'identité du signataire et du contenu du document signé et qu'elle ne peut être établie qu'au moyen de la clef privée du signataire. Ces procédés peuvent donc être utilisés pour remplir les fonctions de signature électronique au sens de l'article 1316-4 du Code civil.

Toutefois, le terme « intégrité » est à prendre ici au sens technique puisqu'il ne s'agit pas de l'intégrité de l'information contenue dans le document, mais de l'intégrité du document numérique représenté sous un format de codage donné (une suite de symboles binaires). Ainsi, un même texte représenté sous deux formats différents, par exemple en « .doc » et en « .pdf »<sup>227</sup>, aura deux signatures cryptographiques complètement différentes, même si ces deux documents numériques correspondent exactement à la même information et produisent des documents papier strictement identiques.

Le fait que la signature cryptographique s'applique au document numérique et non seulement à l'information qu'il contient (au sens de ce qui apparaît à l'écran ou à l'impression) a deux conséquences importantes :

- le signataire n'a pas toujours connaissance de l'ensemble des données qu'il signe en particulier quand le document est encodé dans un format fermé. Le document formaté peut en effet contenir un certain nombre d'informations techniques issues de l'environnement de production du document ;
- la signature perd entièrement sa validité dès que l'on change le format de codage du document (ou la version d'un même format). La conservation de la signature cryptographique interdit donc toute migration de format de codage, opération généralement nécessaire pour assurer la lisibilité du document sur le long terme.

Enfin, la conservation des documents signés par un procédé cryptographique nécessite également la conservation de plusieurs informations nécessaires à la vérification de la signature au cours du temps. En effet, une signature cryptographique garantit uniquement qu'elle a été apposée par une personne ayant connaissance d'une certaine clef cryptographique. Mais le lien entre cette clef et l'identité de son propriétaire, assuré par un certificat de clef, doit aussi être conservé. Par ailleurs, la signature cryptographique est un procédé qui reste relativement vulnérable dans la durée : la clef propre à un utilisateur peut lui être subtilisée, le procédé cryptographique de signature peut perdre sa fiabilité du fait d'évolutions techniques. Ces éléments

---

227. « doc » : format propriétaire lisible à l'aide du logiciel de traitement de texte *Word*. « pdf » : format propriétaire de présentation de document indépendant des systèmes d'exploitation, lisible à l'aide du logiciel *Acrobat Reader*.

devront être pris en compte pour établir les conditions de la conservation des documents signés au moyen d'un procédé de signature cryptographique à clef publique.

## **La normalisation dans le domaine de la conservation électronique des documents**

Une norme est un « *document, établi par consensus et approuvé par un organisme reconnu* »<sup>228</sup>.

Actuellement, de nombreux processus de conservation électronique des documents font référence à une norme, qu'elle soit d'application internationale ou locale. Ces normes n'ont pas de caractère obligatoire mais peuvent être utilisées comme base technique. Ainsi, la jurisprudence a pu estimer qu'elles permettent de représenter un « *état de l'art* » dans le domaine auquel elles se rapportent<sup>229</sup>.

Dans le cadre de la présente recommandation, il est apparu utile de présenter les principales normes développées dans ce domaine.

Le choix de neutralité technologique et organisationnelle qui a guidé les travaux du groupe implique cependant qu'aucune norme n'est recommandée en tant que telle. Les recommandations de la seconde partie du rapport sont donc, par principe, applicables à toute situation sans référence à l'utilisation d'une norme quelconque.

Les principaux organismes de normalisation sont, au niveau international, l'ISO (*International Standard Organisation / Organisation internationale de normalisation*), la CEI (Commission électrotechnique internationale), l'UIT (Union internationale des télécommunications) avec leur équivalent européen, CEN (Comité européen de normalisation), CENELEC (Comité européen de normalisation en électronique et en électrotechnique), ETSI (*European Telecommunications Standards Institute*) et nationaux, l'AFNOR (Association française de normalisation) pour la France.

Ces organismes ont, à des titres divers, élaboré des documents traitant des procédures d'organisation qui permettent, dans une certaine mesure, d'encadrer le processus d'archivage.

Au niveau international, on peut retenir trois normes : la norme ISO 14721 (ou norme OAIS – *Open Archival Information System*), la norme ISO 15489-1 sur le « *records management* » et la norme ISO 19005-1 sur l'utilisation du format PDF pour l'archivage (PDF/A-1).

La norme OAIS définit un vocabulaire et un ensemble de concepts permettant d'appréhender, de façon globale et complète, la question de l'archivage électronique sur le long terme. Elle définit un modèle d'information et un modèle fonctionnel dont les fonctions de base sont le versement, la gestion des données, le stockage et l'accès. Elle propose également une classification des types de migration et des différents

---

228. La norme est définie par l'Organisation internationale de normalisation comme un « *document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné* ».

229. Cass. civ. 3<sup>e</sup> ch., 4 février 1976, *Bull. civ. III*, n° 49.

modes de coopération possibles entre archives. La mise en œuvre de cette norme permettra de s'assurer de la fiabilité de leur exploitation.

La norme sur le «*records management*» ne concerne pas exclusivement la conservation électronique des documents mais s'intéresse à l'ensemble du cycle de vie du document électronique. À ce titre, elle propose des procédures d'organisation et de gestion du document, depuis sa création jusqu'à la fin de son intérêt pour l'entreprise. Son utilisation est recommandée dans de nombreux pays. Ainsi l'Australie a adapté cette norme pour en faire un standard utilisé par toutes les autorités publiques en charge de l'archivage<sup>230</sup>. La norme «*record management*» est mise en œuvre, au niveau européen, par le biais du modèle MoReq<sup>231</sup> (*Model Requirements for the Management of Electronic*: modèle d'exigences pour l'organisation de l'archivage électronique). Il vise à mettre en place «*un système en mesure de gérer les documents électroniques aux degrés de confidentialité et d'intégrité voulus en combinant les avantages de la gestion électronique et ceux de la théorie classique de l'archivage*».

Le format PDF est devenu un format standard d'échange et de stockage de données car il est indépendant des outils et des systèmes de création et d'exploitation.

La description du format PDF/A est maintenant une norme internationale sous la référence ISO 19 005-1 «*Format de fichier des documents électroniques pour une conservation à long terme – Utilisation du PDF 1.4 (PDF/A-1)*».

Le format PDF/A-1 est conforme aux spécifications PDF version 1.4, mais n'en utilise pas toutes les possibilités, de manière à permettre une meilleure conservation et une restitution plus fidèle des documents. Il s'applique aux documents contenant du texte et des images (matricielles ou vectorielles); les séquences de son et de vidéo sont exclues.

La norme ISO 19 005-1 détaille les fonctionnalités du PDF à utiliser obligatoirement (référence au format de caractères Unicode par exemple), celles à utiliser avec des restrictions (sur la manière de saisir des métadonnées par exemple) et celles à ne pas utiliser (par exemple, le chiffrement, la compression LZW, la transparence des images...).

D'autres modèles existent en Europe, certains pays ayant même initié des programmes adaptés aux besoins de l'archivage électronique. L'Allemagne s'est ainsi dotée d'un programme intitulé DOMEA<sup>232</sup> (*Document Management and Electronic Archiving*) et la Finlande d'un programme appelé SAHKE<sup>233</sup>.

Au niveau français, on peut retenir les normes NF Z 42-013 et NF Z 43-400.

---

230. AS ISO 15489, Australian standard for record management.

231. Le Royaume-Uni et le Portugal y font expressément référence.

232. DOMEA: norme de l'administration fédérale allemande pour la gestion électronique des processus. Elle préconise l'usage de certains formats et supports et établit des recommandations en matière d'intégrité et d'authenticité pour les archives électroniques.

233. SAHKE: préconise l'usage de certains formats ou supports comme le XML ou l'ASCII.

La norme Z 42-013<sup>234</sup> a été homologuée en juillet 1999 et révisée en décembre 2001. Elle a pour objet de spécifier les conditions dans lesquelles les systèmes de gestion électroniques doivent assurer, de manière fiable, la conservation électronique des documents.

La norme Z 43-400 a été homologuée en septembre 2005. Elle a pour objet de spécifier les conditions dans lesquelles la conservation de documents électroniques peut être assurée avec l'emploi de supports micrographiques. Les procédés et les technologies recommandés ne peuvent être employés que si le document électronique à conserver possède une représentation visuelle imprimable.

Les normes nationales comme locales constituent des instruments indispensables au déploiement des technologies de la conservation électronique; elles assurent par leur adoption par les industriels des outils d'unification. La normalisation présente l'avantage d'offrir aux opérateurs économiques des cadres communs négociés et donc adaptés à leur activité. Elles sont en ce sens un facteur de dynamisme et de compétitivité.

## **Mettre en place un environnement de confiance**

Le cadre entourant la conservation électronique des documents reste en grande partie à préciser. Les obligations légales de conservation qui pèsent sur les entreprises nécessitent que soient indiqués les conditions et les moyens pour parvenir à une conservation juridiquement satisfaisante. La confiance dans l'environnement numérique se renforcera par le biais notamment de précisions sur les règles existantes et par la mise en place d'éléments pratiques permettant une conservation propre à répondre aux exigences des différents textes.

À titre préalable, le Forum des droits sur l'internet et la Mission Économie Numérique estiment que la mise en place d'un processus de conservation électronique d'un document ne doit pas modifier son statut juridique d'origine (principe d'équivalence juridique).

De plus, cette conservation ne doit pas privilégier des techniques spécifiques (principe de neutralité technique). Il est en effet important que le cadre de la conservation électronique des documents reste technologiquement neutre.

Enfin, il importe que la conservation électronique d'un document ne fasse pas référence à un mode d'organisation particulier. L'archivage peut être mis en œuvre, soit par le recours à un tiers archiveur (conservation externe), soit par un service d'archivage interne (conservation interne), par l'un ou l'autre des modes d'organisation alternativement ou encore de façon mixte (principe de neutralité organisationnelle).

---

234. Norme AFNOR (Association Française de NORmalisation) de décembre 2001 NF Z 42-013: «*Archivage électronique – Spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes.*»

**Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent que toute réflexion sur le cadre réglementaire de la conservation électronique des documents respecte les principes de neutralité technologique et organisationnelle et que le statut juridique des documents ne soit pas modifié du fait de leur conservation électronique.**

Le Forum des droits sur l'internet et la Mission Économie Numérique entendent favoriser l'émergence d'un environnement de confiance bâti sur le respect de principes et de bonnes pratiques garantissant la valeur des documents conservés. La poursuite de cet objectif s'accompagnera de recommandations permettant d'accompagner la démarche de conservation dans l'entreprise et d'ouvrir des pistes de prospective pour l'évolution du cadre juridique de la conservation.

## Les modalités d'une conservation de l'écrit électronique

Jusqu'à présent, l'essentiel des réflexions sur le document électronique a porté sur le procédé relatif à sa signature, mais très peu sur la conservation et la restitution de l'écrit électronique. À l'heure actuelle, il ne semble pas y avoir de consensus clair sur ce qu'il convient de conserver parmi l'ensemble des éléments (document, données relatives au créateur, à l'environnement de création...) qui procèdent de la création du document électronique.

L'intégrité du document et la possibilité de conserver un document intègre sont cependant au centre du dispositif mis en place par la loi du 13 mars 2000 sans que les critères ou les moyens permettant de garantir cette intégrité soient précisés.

## **Les critères d'une conservation électronique garantissant l'intégrité des documents**

Devant le juge se posent les questions de la recevabilité et de la force probante des documents électroniques archivés.

L'article 1316-1 du Code civil précise que l'écrit sous forme électronique doit, pour être *« admis en preuve au même titre que l'écrit sur support papier »*, être *« établi et conservé dans des conditions de nature à en garantir l'intégrité »*. Comme il a été dit précédemment, aucun texte ne précise les critères permettant de juger de cette intégrité.

Dès lors, il est nécessaire de garantir que celui à qui incombe la preuve disposera bien, au moment opportun, des moyens requis pour accéder à un document archivé plusieurs années auparavant et qu'il pourra prouver l'intégrité de celui-ci devant le juge.

Pour cela, les critères de l'intégrité des documents doivent être édictés. Ils permettront de définir les conditions dans lesquelles un document conservé pourra avoir force probante.

Pour faciliter la mise en place des processus de conservation électronique des documents et leur efficacité du point de vue juridique, il est apparu nécessaire de choisir

des critères issus de la pratique des professionnels de l'archivage et pris en considération par les juristes.

Le Forum et la Mission estiment en effet que le choix de ces critères doit se fonder sur les notions existantes. Deux des critères retenus se retrouvent dans le décret n° 2005-973 du 10 août 2005 relatif aux actes établis par les notaires<sup>235</sup> et dans le décret 2005-972 du 10 août 2005 relatif au statut des huissiers de justice<sup>236</sup>.

Ces critères sont en outre partagés par les professionnels de l'archivage qui estiment qu'ils permettent de garantir la fiabilité du processus de conservation. Le respect de ces critères doit guider les acteurs de l'archivage tout au long du processus d'archivage et permettre au juge de vérifier l'intégrité de la conservation.

En définitive, pour garantir l'intégrité d'un écrit, le Forum et la Mission estiment que trois critères doivent être cumulativement réunis par le processus de conservation :

- la **lisibilité** du document ;
- la **stabilité** du contenu informationnel ;
- la **traçabilité** des opérations sur le document.

La lisibilité désigne la possibilité d'avoir accès, au moment de la restitution du document, à l'ensemble des informations qu'il comporte. Cette démarche est facilitée par les métadonnées associées au document.

La stabilité du contenu informationnel désigne la nécessité de pouvoir garantir que les informations véhiculées par le document restent les mêmes depuis l'origine et qu'aucune n'est omise ou rajoutée au cours du processus de conservation. Le contenu informationnel s'entend de l'ensemble des informations, quelle que soit leur nature ou leur origine, issues du document et, le cas échéant, de sa mise en forme<sup>237</sup>.

La traçabilité désigne la faculté de présenter et de vérifier l'ensemble des traitements, opérés sur le document lors du processus de conservation.

**Le Forum des droits sur l'internet et la mission économie numérique recommandent que la notion d'intégrité du document telle que prévue par l'article 1316-1 du Code civil soit assurée par le respect cumulé des trois critères suivants :**

- lisibilité du document ;**
- stabilité du contenu informationnel ;**
- traçabilité des opérations sur le document.**

---

235. Décret n° 2005-973 du 10 août 2005 modifiant le décret n° 71-941 du 26 novembre 1971 relatif aux actes établis par les notaires.

236. Décret n° 2005-972 du 10 août 2005 modifiant le décret n° 56-222 du 29 février 1956 pris pour l'application de l'ordonnance du 2 novembre 1945 relative au statut des huissiers de justice.

237. À titre d'exemple, sont visés comme pouvant faire partie, le cas échéant, du contenu informationnel d'un document : la taille des polices de caractères utilisées, les mises en évidence résultant du recours aux caractères gras etc.

## **Les bonnes pratiques d'une politique de conservation électronique des documents**

L'objectif de restitution d'un document intègre sous-tend, du point de vue de la preuve, la mise en place d'un processus de conservation électronique. Il impose que les acteurs puissent fonder leur confiance dans le respect de bonnes pratiques.

La mise en œuvre de bonnes pratiques permettra d'aboutir au respect des critères définissant l'intégrité. Les travaux menés pour l'adoption de cette recommandation ont permis de définir ces bonnes pratiques au travers de quatre étapes dans le processus de conservation.

Chacune de ces étapes précise les opérations qui concourent à l'obtention de l'intégrité. L'emploi de ces bonnes pratiques tout au long du processus de conservation contribuera à établir que l'intégrité du document conservé a bien été préservée.

**Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent aux acteurs souhaitant conserver des documents électroniques l'emploi de bonnes pratiques en vue de satisfaire aux conditions de l'article 1316-1 du Code civil. L'usage de ces bonnes pratiques doit se poursuivre tout au long des quatre étapes du processus de conservation: le versement, l'enregistrement, la gestion et la restitution des documents.**

### **Première étape: le versement des documents**

Le versement est la première étape du processus de conservation électronique du document.

Le document peut provenir d'origines variées. Il peut avoir été créé par l'entité concernée directement (format natif électronique), avoir été reçu par un tiers ou encore provenir d'une opération de transformation à partir d'un autre document (notamment d'un document papier).

Le terme de «versement» recouvre l'ensemble des opérations qui permettent de transférer un document de son environnement de création ou de réception à son environnement de conservation. On peut employer des termes différents selon les métiers, les activités ou les environnements (dépôt, transfert, remise, etc.).

Il convient de rappeler que l'environnement de conservation et le versement peuvent être internes ou externes à l'entreprise (cf. *infra*). Dans ces conditions, une même personne (physique ou morale) peut jouer à la fois le rôle de déposant et celui d'archiviste.

Cette étape doit inclure suivant les cas et le type d'organisme souhaitant archiver (administrations, entreprises...), les opérations suivantes :

- identifier la partie (organisme, personne, programme, serveur,...) qui verse le document et, le cas échéant, vérifier qu'elle y est habilitée ;
- vérifier que le document n'a pas été altéré lors de sa transmission entre la partie qui verse et le système d'archivage. Cette vérification suppose que soient préalablement établies les règles de la transmission et que les procédés de vérification soient adaptés aux modalités de transmission ;



– contrôler que la structure des documents, le nombre, la taille, le format des documents et des métadonnées définies et la codification (format du fichier informatique) sont conformes aux règles définies préalablement et conjointement par la partie versante et l'entité qui va assurer la conservation.

Il conviendra également de garantir la chronologie des opérations successives effectuées sur l'objet archivé. Pour les éventuels cas où, en plus de la chronologie, la date d'une opération doit être mentionnée de manière fiable, il pourrait être envisagé de recourir à un système d'horodatage fiable, à l'exemple de celui mentionné aux articles 1369-7 et 1369-8 du Code civil<sup>238</sup>.

### **Deuxième étape : l'enregistrement des documents**

Cette étape a pour but d'insérer les nouveaux documents dans le système de gestion des documents.

L'insertion se fait sur deux niveaux, qui correspondent à autant d'opérations différentes et que la pratique des professionnels de l'archivage électronique lie fortement<sup>239</sup> :

#### **Le référencement des nouveaux documents pour en permettre la gestion**

Il s'agit en pratique d'enregistrer (par exemple dans une base de données) les caractéristiques des documents (identifiants, date d'arrivée, durée de conservation, protections particulières...). Cet enregistrement doit être aussi automatique que possible et exploiter si possible les métadonnées présentes dans les documents versés. Le référencement permet la vérification des éléments de traçabilité et de stabilité du contenu informationnel.

#### **L'écriture des documents sur des supports de stockage**

Le choix inadéquat de dispositifs de stockage peut avoir une incidence sur le processus de conservation. Il en résulte que le choix des supports implique de prendre en compte de nombreux paramètres<sup>240</sup>.

**Des contrôles sont opérés par la personne ou l'organisme chargé de la conservation.** Si les résultats des contrôles sur les opérations précédentes sont corrects, le document électronique peut être considéré comme inséré dans le système de conservation. Indépendamment de l'inscription de cet événement dans l'historique des opérations, l'envoi d'une notification de prise en charge à la partie versante est fortement recommandé.

---

238. Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.

239. Cette exigence implique d'ailleurs pour beaucoup de ne considérer que la prise en charge de nouveaux documents n'est complète et valide que si les deux opérations sont effectuées avec succès.

240. Il s'agira notamment d'évaluer le volume à stocker, la stabilité intrinsèque du support, sa robustesse, le niveau de sécurité souhaité, la plus ou moins large diffusion de la technologie, la présence sur le marché d'une offre multi-constructeurs ou reposant sur des normes publiques, l'existence d'outils de contrôle des supports, l'existence d'un chemin d'accès aux données protégées, la simplicité des opérations de recopie, la protection contre l'effacement accidentel...

On recommandera au minimum, sans que cela soit nécessaire à l'obtention de l'intégrité mais pour des raisons de bonne gestion et de sécurité, l'utilisation de supports multiples conservés dans des lieux distincts.

En ce qui concerne la datation de cette étape : l'enregistrement de la date peut faire appel à un procédé d'horodatage fiable<sup>241</sup>.

### **Troisième étape : la gestion des documents conservés**

Cette étape est, sur la durée, la plus longue du processus de conservation, et les opérations qui la composent sont importantes pour la bonne gestion des documents conservés.

Elle comprend notamment la réalisation d'opérations de migration qui sont, en pratique, souvent indispensables à l'obtention d'une conservation intègre dès lors que la conservation est envisagée pour une durée importante.

Les opérations qui interviennent au cours de cette étape sont les suivantes :

#### **Contrôles de lisibilité des documents**

Ces contrôles doivent prendre en compte plusieurs données (ancienneté et volume global des documents, caractéristiques des supports, taux d'activité).

L'interprétation des résultats de ce contrôle conduira à des actions préventives (recopie, migration, maintenance,...) visant à garantir la lisibilité.

#### **Vérifications périodiques de la cohérence entre les référentiels du système d'information et le stockage des documents**

Cette opération a pour finalité le maintien de l'intégrité globale des archives et l'accès à celles-ci. La plate-forme matérielle doit pouvoir évoluer sans conséquence sur l'organisation logique des documents archivés. Il est recommandé de pouvoir reconstituer un référentiel d'accès minimum à partir des métadonnées des documents archivés.

#### **Régénération**

Il s'agit d'une copie des documents de leur support actuel sur un nouveau support ayant les mêmes caractéristiques ou de la recopie des documents sur leur support actuel.

#### **Opérations de migrations**

Deux types de migration peuvent être effectuées selon les besoins :

- migration de support – copie des documents de leur support actuel vers un nouveau support ayant des caractéristiques différentes ;
- migration de format – copie des documents, accompagnée d'une recodification, c'est-à-dire d'un changement de format informatique.

#### **Contrôle des opérations de migrations (avant, pendant, après)**

- contrôle préalable de l'opération sur un échantillon ;

---

241. Voir étape précédente.

- contrôle et validation de la migration ;
- contrôle de l'absence d'altération du contenu informationnel en cas de recodification (en principe opéré par la partie versante).

### **Opérations de suppression**

Cette opération est réalisée lorsque les documents ont atteint le terme de la durée souhaitée de conservation et conformément aux procédures établies préalablement avec la partie déposante (suppression logique ou physique).

### **Éventuellement, opérations globales sur le système de gestion des documents électroniques**

Ces opérations, naturelles pour tout système informatique, doivent impérativement être documentées à un niveau global. Elles concernent notamment la maintenance d'un composant, le changement de système d'exploitation etc.

### **Quatrième étape: la restitution et la communication des documents conservés**

Pour son organisation et sa mise en œuvre, on retiendra qu'il s'agit de l'étape complémentaire ou symétrique du versement.

On distingue deux types de restitutions :

#### **La restitution définitive à la partie versante**

Cette opération, qui n'est pas la plus fréquente, correspond en général à un changement de solution d'archivage électronique à l'initiative de la partie versante. Sa mise en œuvre suppose que des choix de standard de réversibilité ont été faits à l'origine. La restitution définitive s'accompagne de la suppression logique et/ou physique de tous les enregistrements dans le système d'archivage.

#### **La restitution pour des besoins de production de preuve ou de contrôle**

En fonction de la finalité, la restitution pourra prendre plusieurs formes :

- fourniture du document ou d'une copie sur un support amovible ;
- impression du document ;
- affichage du document sur écran.

La restitution s'effectue selon la procédure suivante :

- contrôle de l'habilitation du demandeur à effectuer la requête de restitution ;
- contrôle de la disponibilité et de la maîtrise de l'ensemble des procédés externes de restitution par le demandeur. Cette étape vise à s'assurer de l'absence d'altération entre la sortie du système d'archivage et la réception par le destinataire final ;
- sélection du document dans le référentiel ;
- lecture sur son support de stockage et transcription conformément au mode de restitution choisi ;
- accusé de réception.

Dans une perspective de bonne gestion, il est souhaitable que le demandeur accuse réception du document communiqué et puisse notifier la bonne fin des opérations.

## L'impact des migrations, notamment sur les documents signés au moyen d'un procédé cryptographique

La conservation dans le temps ne peut, le plus souvent, se faire qu'au prix d'une évolution de l'objet conservé<sup>242</sup>. Sauf à imaginer l'arrêt de toute évolution technologique, il faut accepter une certaine mutation des environnements informatiques. Cette évolution, qui concerne bien évidemment les matériels, les logiciels et systèmes d'exploitation, affecte nécessairement la lisibilité des documents.

Les évolutions que l'on fait subir aux documents en vue de leur conservation sont appelées migrations. Elles s'intègrent au processus de conservation et font partie des bonnes pratiques que nécessite une conservation préservant l'intégrité des documents (voir *supra*).

Les migrations sont classées en deux grandes familles: les migrations de support et les migrations de format:

- les migrations de support consistent en un simple déplacement de données d'un environnement physique à un autre. Les migrations de support ont peu de conséquences si elles s'effectuent entre des supports de caractéristiques similaires et répondant à de strictes exigences de sécurité (voir étape 3);
- les migrations de format sont des modifications qui affectent la nature même du document. Elles peuvent être réalisées avec ou sans migration de support. Ce type de migration va entraîner des conséquences sur le fichier qui représente le document puisque sa représentation numérique va être modifiée. Cependant, en dépit de ces modifications, le contenu informationnel du document doit être préservé au cours de la migration. Ces migrations de format sont souvent nécessaires pour préserver la lisibilité du document. Toutefois, leur nombre et leur fréquence peuvent être considérablement réduits par l'emploi d'un format ouvert ou standard dès l'établissement du document.

De façon générale, il conviendra donc, quel que soit le type de migration opéré, de s'assurer que ces migrations sont effectuées dans des conditions<sup>243</sup> qui permettent de préserver l'intégrité des documents. En particulier, les migrations de format doivent être réalisées dans des conditions telles qu'elles ne puissent être suspectées d'altérer le contenu informationnel du document (voir étape 3).

À cet égard, il convient de préciser le cas particulier de la migration des documents signés au moyen d'un procédé cryptographique au sens de l'article 1316-4 du Code civil.

Au niveau de sa fonction probatoire, un document signé peut être utilisé pour établir différentes preuves:

- identité des parties;
- expression de la volonté des parties;
- lien entre l'expression de la volonté et le contenu de l'acte;
- contenu de l'acte;
- garantie d'intégrité de l'acte.

---

242. Voir *supra*, troisième étape.

243. Voir page 205.

Un document signé présente donc comme particularité que sa valeur au titre de la preuve n'est pas seulement liée à son contenu mais également à des informations attachées à celui-ci par l'utilisation de la signature.

De plus, lorsqu'elle est réalisée au moyen d'un procédé cryptographique (signature cryptographique à clef publique), la fonction de signature résulte d'un processus appliqué au document sous sa forme numérique comme cela a été précisé dans la première partie de la recommandation<sup>244</sup>. C'est l'association de la signature, expression d'un consentement émané d'une personne, et de la forme binaire initiale du document qui apportera à celui-ci sa valeur propre.

L'utilisation d'un procédé de signature cryptographique implique donc que le document signé soit représenté par une forme binaire unique. C'est en effet grâce à ce caractère propre que l'on peut vérifier et connaître les éléments composant le document et s'assurer de l'absence d'altération. Il résulte de cela que la nécessité d'un procédé de vérification fige nécessairement le document à l'instant de sa signature.

Ainsi, toute vérification à terme de la signature d'un document signé au moyen d'un procédé cryptographique suppose la préservation de la forme binaire d'origine alors même que l'accès au contenu du document ne peut s'opérer que sous réserve de migrations de format<sup>245</sup> rendues nécessaires pour la lisibilité du document dans le temps.

Il convient ainsi de noter une contradiction propre à l'utilisation de la signature cryptographique à clef publique. Cette contradiction réside dans le fait que la migration de format entraîne une impossibilité de vérifier la signature électronique alors que cette migration est pourtant nécessaire pour des raisons archivistiques (voir traçabilité, lisibilité). Il faut souligner que le fait que les documents signés soient établis dans des formats ouverts ou standards est particulièrement souhaitable dans ce contexte, puisque l'on réduit ainsi les risques à court terme qu'une migration de format soit nécessaire pour assurer la lisibilité du document.

Dans tous les cas, il est indispensable d'anticiper la vérification de signature.

Pratiquement, les vérifications de signature opérées à des fins probatoires n'intéressent que les cas où la preuve par écrit est exigée par la loi (art. 1341 du Code civil) ou que cette exigence résulte d'une convention de preuve ou d'actes qui doivent être constatés par écrit pour être valables. Dans les autres cas, les parties sont libres des moyens de preuve, soit que la loi les y autorise, soit qu'elles en sont convenues par avance.

La restitution devra permettre d'établir l'identité du signataire du document, la validité de la signature et le lien de cette signature au contenu signé. Ces éléments seront, en fonction des choix techniques opérés, inscrits dans les métadonnées associées au document.

---

244. Voir page 199.

245. Voir page 206.

L'ensemble des vérifications de signatures interviendra nécessairement dans un temps où les éléments le permettant seront disponibles et valides. En particulier, la vérification interviendra nécessairement dans la période de validité du ou des certificats impliqués.

Les vérifications de signatures qui seront opérées pourront l'être soit :

- par un **tiers indépendant** des parties ;
- par les **parties elles-mêmes**.

Toute vérification de la signature, qui s'inscrit dans l'exigence de traçabilité du document, devra s'accompagner de la restitution du résultat de cette opération. Cette procédure conduit à l'inscription dans les métadonnées du document de tous les éléments vérifiés ou issus de la vérification ainsi que le résultat de cette vérification éventuellement assortie de mesures techniques complémentaires.

Sous réserve du respect des critères définissant l'intégrité du document conservé, il est possible de considérer, comme c'est le cas pour les actes authentiques électroniques<sup>246</sup> dressés par des officiers publics, que « *les opérations successives justifiées par sa conservation, notamment les migrations dont il peut faire l'objet, ne retirent pas à l'acte sa nature d'original* »<sup>247</sup>.

**Le Forum des droits sur l'internet et la Mission pour l'Économie Numérique recommandent que, sous réserve de la possibilité de vérifier l'intégrité des documents conservés, les opérations successives justifiées par cette conservation, notamment les migrations, ne retirent pas au document son statut juridique d'origine.**

## Les moyens complémentaires de garantir la mise en place d'un environnement de confiance

La mise en œuvre de solutions de conservation de documents électroniques peut prendre plusieurs formes. Les deux plus importantes sont :

- l'appel à des prestataires de service externes ;
- l'utilisation de services internes spécialisés dans ces fonctions.

Dans les deux cas, une formalisation s'impose afin de fixer les obligations des intervenants et les modalités de mise en œuvre des services. Il est recommandé, en cas de conservation externe, d'établir un contrat de service et en cas de conservation interne, un document définissant la politique d'archivage.

---

246. Voir décret n° 2005-972 et décret n° 2005-973 précités.

247. Décret n° 2005-973, art. 28 al. 5 et décret n° 2005-972, art. 29 ; précités.

## **Le contrat de service d'archivage (conservation externe)**

En cas d'archivage externe, le contrat de service est conclu avec un tiers archiveur, c'est-à-dire une «*personne physique ou morale qui se charge pour le compte de tiers d'assurer et de garantir la conservation et l'intégrité des documents électroniques*»<sup>248</sup>.

La relation contractuelle qui unit les parties ne peut s'envisager que dans la durée puisqu'il s'agit d'assurer, dans le temps, le stockage des documents confiés. D'ailleurs, les effets attendus d'une conservation par un tiers archiveur n'apparaîtront le plus souvent que longtemps après le versement du premier document. C'est dans la restitution ou la communication d'un document intègre que la conservation prendra alors tout son sens et déploiera son plein effet juridique.

Il apparaît donc important que, dès le début de la relation contractuelle, les parties puissent fonder leur confiance mutuelle sur un engagement clair incluant notamment les bonnes pratiques définies dans la présente recommandation.

Si le contenu du contrat de service relève de la liberté contractuelle des parties, il paraît nécessaire de prévoir certaines «*clauses types*». Le Forum et la Mission estiment ainsi important que les partenaires soient particulièrement vigilants sur la présence des clauses suivantes au sein de leur contrat :

### **Clause de sécurité et de protection des données**

Le tiers archiveur doit conserver l'intégralité des éléments électroniques qui lui sont transmis par le client.

Le tiers archiveur doit permettre un accès direct pour consultation ou extraction des documents dont il est dépositaire. Cet accès doit être sécurisé.

Le tiers archiveur doit faire procéder, par un prestataire indépendant, à des audits de vérification des dispositions qu'il a prises pour garantir le niveau de service contractuellement défini. Les rapports d'audit peuvent être communiqués au client à titre confidentiel.

Le tiers archiveur devra prendre toute mesure technique propre à garantir que les données à caractère personnel figurant dans les documents archivés ne soient accessibles qu'aux personnes habilitées et que celles-ci ne soient pas modifiées ou endommagées<sup>249</sup>. À cet effet, il convient de se reporter aux récentes recommandations de la CNIL dans ce domaine<sup>250</sup>.

### **Clause d'information et de conseil**

Le tiers archiveur doit informer son client de la nécessité de préserver la compatibilité entre ses propres systèmes et les objets électroniques qui lui ont été confiés.

---

248. Définition retenue par le guide de l'archivage électronique sécurisé (12 juillet 2000) – EDIFICAS et IALTA et la norme NF Z 42-013.

249. Dispositions de l'article 226-17 du Code pénal.

250. Délibération n° 2005-213 du 11 octobre 2005 portant adoption d'une recommandation concernant les modalités d'archivage électronique, dans le secteur privé, de données à caractère personnel (*supra* page 195)

Le tiers archiveur pourra, à cette fin, proposer une prestation complémentaire.

Le tiers archiveur doit informer le client des opérations de migrations ou des modifications techniques intervenues sur ses systèmes et des conséquences sur la disponibilité ou la compatibilité des matériels du client ou sur le mode d'échange et de conservation des données confiées.

#### **Clause de reprise et de continuité**

En cas de reprise d'un fond documentaire par un tiers archiveur (sortie de contrat, faillite, disparition du tiers, transfert d'archives), le nouveau prestataire doit pouvoir, au cours et à l'issue de l'opération de migration, assurer aux documents le maintien de leurs caractéristiques fondamentales. À cet égard :

- il convient de prévoir l'interopérabilité des formats et des versions entre tiers archiveurs (pour éviter le risque de rupture d'intégrité ou de perte de données);
- le tiers archiveur doit assurer le transfert de l'intégralité des données qui lui sont confiées en garantissant leur intégrité;

- dans tous les cas, le tiers archiveur doit consigner dans un lieu ou par un moyen accessible à son client, ou à toute personne désignée par lui, les informations et données techniques permettant la récupération des données et prendre toutes dispositions garantissant au client un délai raisonnable permettant la récupération des données dont il est dépositaire.

#### **Clause de confidentialité**

Le tiers archiveur doit garantir la confidentialité des informations qui lui sont confiées ou dont il peut avoir eu connaissance à l'occasion de la relation contractuelle avec son client.

Ces informations, couvertes par le secret des affaires, peuvent provenir de l'accès ou des opérations effectuées sur les documents qu'il a la charge de conserver, ou provenir de sa connaissance des systèmes d'information de l'entreprise, que cette connaissance résulte de ses constatations ou qu'elle lui soit apportée par son client.

À ce titre, les informations ne pourront être communiquées qu'aux personnes désignées par le client, à l'exception des cas où il est légalement tenu de communiquer ces informations à des tiers.

#### **Clause d'assurance professionnelle**

Le tiers archiveur devra contracter une assurance le couvrant dans le domaine de la «*responsabilité civile professionnelle*». Cette assurance donne une protection financière de l'activité de tiers archivage en cas de mise en cause de sa responsabilité suite à l'indisponibilité du service.

Le tiers archiveur doit de plus s'engager à maintenir en vigueur le contenu de l'assurance tout au long du contrat de service.



Afin de protéger sa responsabilité civile en cas par exemple de dysfonctionnement de ses systèmes informatiques, le tiers archiver pourra également contracter une assurance dite de « *dommages pour compte* »<sup>251</sup>.

D'une manière générale, il convient de noter que la nouvelle profession de tiers archiver s'organise<sup>252</sup> mais ne dispose pas d'un statut propre comme peuvent en avoir désormais les prestataires de services de certification électronique<sup>253</sup>. Une garantie liée à une accréditation et au respect d'un cahier des charges précis ou de normes *ad hoc*, identiques pour tous, pourrait être mise en place. Les clauses mentionnées précédemment pourraient utilement être retenues au titre des éléments figurant au cahier des charges.

## **Les chartes ou politiques d'archivage (conservation interne)**

Les objectifs d'une conservation opérée en interne ne diffèrent guère de ceux qui sont assignés aux tiers archiveurs. Symétriquement à la conservation externe, il est souhaitable que des bonnes pratiques guident la mise en place d'une conservation interne.

Ces bonnes pratiques pourront se concrétiser dans la rédaction d'un document, appelé charte ou politique, dont l'objet sera de décrire le processus de conservation et la démarche qualité qui doit l'accompagner.

Ce document permettra à chacun, au sein de l'entreprise ou de l'administration qui opère sa conservation en interne, d'inscrire son action dans un processus commun de nature à aboutir à une conservation garantissant l'intégrité des documents.

---

251. Une évolution récente du concept d'assurance des risques immatériels informatiques permet en effet d'envisager la couverture des clients du tiers archiver : – sur des bases contractuelles dites de « *dommages pour compte* », le tiers archiver ayant transféré à l'assurance pour financement, les risques encourus par l'ensemble de ses clients dans le cadre d'une rupture de services ; – en dehors de toute nécessité immédiate de rechercher en responsabilité le tiers archiver ou tout autre prestataire à l'origine des préjudices subis ; – dans des délais rapides ; – en combinaison avec les couvertures Responsabilité Civile pour augmenter la capacité indemnitaire en cas de faute avérée.

252. Création de la Fédération Nationale des Tiers de Confiance (FNTC).

253. Voir le statut des prestataires de services de certification électronique (PSCE) et notamment leur régime de responsabilité spécifique instituée par la loi pour la confiance dans l'économie numérique du 21 juin 2004 en son article 33 : « *Sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants : 1° Les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ; 2° Les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ; 3° La délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ; 4° Les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers. Les prestataires ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs. Ils doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'ils pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qualifiés qu'ils délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.* »

Les rédacteurs de ces documents pourront se référer aux bonnes pratiques visées précédemment. Le contenu précis de la charte sera fonction des statuts et des modes d'organisation propres à chaque organisme. En outre, les fonctions identifiées au titre des clauses principales des contrats d'archivage externe (voir *supra*) pourront être reprises par les rédacteurs.

Il importe que la charte ou la politique d'archivage retenue produise son plein effet dans l'entreprise. C'est pourquoi il est impératif qu'elle soit connue et respectée par les personnes intervenant à un titre ou un autre dans le processus de conservation. Les moyens ou la voie choisie par l'organisme pour l'appliquer relèvent des modes d'organisation de l'entreprise.

Pour parachever le dispositif interne mis en place, une procédure de contrôle-qualité pourrait être mise en œuvre. Cette procédure devra évaluer, de façon indépendante, la mise en œuvre des prescriptions de la charte ou de la politique d'archivage dans ses différents éléments.

**Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent, dans le cas d'une conservation externe, que soient mis en place des contrats de services se référant aux bonnes pratiques édictées. Ce contrat de service contiendra certaines « clauses types » :**

- Clause de sécurité
- Clause d'information et de conseil
- Clause de reprise et de continuité
- Clause de confidentialité
- Clause d'assurance professionnelle

**Dans le cas d'une conservation interne, il convient de mettre en place un document interne (charte ou politique d'archivage), se référant aux bonnes pratiques édictées, et accompagné d'un contrôle-qualité.**

## Pistes de prospective pour la confiance dans l'environnement électronique

Le Forum des droits sur l'internet et la Mission Économie Numérique entendent poursuivre la réflexion sur des points portant sur la transition et la coexistence entre les environnements papier et les environnements numériques.

## **Harmoniser les durées de conservation et de prescription au niveau européen**

D'une manière générale, on peut constater qu'il existe une grande hétérogénéité des durées de prescription ou de conservation des documents, tant civils que commerciaux. Cette hétérogénéité constitue assurément un facteur de complexité pour la gestion dans le temps des documents conservés.

Ce constat n'est en aucun cas propre à la conservation électronique des documents mais concerne bien évidemment l'archivage traditionnel des supports papiers. Il

apparaît que cette absence d'homogénéité n'est pas sans conséquences financières, organisationnelles ou opérationnelles.

Compte tenu de ces éléments et afin également de limiter les volumes de données électroniques ou de papiers dus à la conservation souvent inutile des documents pour des raisons de respect de la prescription, il convient de mener une réflexion sur une éventuelle harmonisation des délais.

À l'échelle de l'Union européenne, une importante étude sur le droit des contrats conduite à la demande de la Commission de l'Union européenne offre un aperçu des principales durées de prescription pour les actions liées aux contrats<sup>254</sup>.

Il ressort de l'examen de cette étude que les situations en matière de prescription sont diverses et que les durées sont très variées. Cette situation pose des questions en matière d'égalité dans les conditions de la compétition économique entre les acteurs opérant au sein du marché de l'Union.

Des initiatives étrangères de réduction des délais de prescription ont déjà été conduites dans certains pays.

Dans ce domaine, l'expérience allemande est significative : il y a été instauré le 1<sup>er</sup> janvier 2002 un régime qui ramène la prescription de droit commun de 30 à 3 ans (§ 195 BGB<sup>255</sup>). Cette forte diminution est compensée par un nouveau système de calcul des délais de prescription qui semble avoir satisfait à la fois les praticiens du droit et la doctrine<sup>256</sup>. Valable pour presque toutes les actions dont le fondement est contractuel, ce régime ne connaît dorénavant que peu d'exceptions, en matière de vente ou de contrat d'entreprise.

De telles mesures permettant d'aboutir à une simplification doivent être encouragées. Il est donc nécessaire que ces initiatives soient envisagées à l'échelle de l'Union européenne.

**Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent que les délais de conservation soient harmonisés pour tous les documents quels que soient leurs supports. À cet égard, le Forum et la Mission considèrent qu'il est nécessaire de mener, à une échelle européenne, une réflexion portant sur la réduction des délais de prescription et de conservation.**

---

254. Étude sur l'intersection entre le droit des contrats et le droit de la responsabilité extra-contractuelle et le droit de la propriété pages 193 à 196  
[www.europa.eu.int/comm/consumers/cons\\_int/safe\\_shop/fair\\_bus\\_pract/cont\\_law/studies\\_fr.htm](http://www.europa.eu.int/comm/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/studies_fr.htm)

255. Bürgerliches Gesetzbuch, l'équivalent de notre Code civil en Allemagne.

256. Voir Michael Schley, La grande réforme du droit des obligations en Allemagne, D. 2002., chron., p. 738; Jochen Bauerreis, Le nouveau droit de la prescription, *RIDC* 4-2002, p. 1023; Claus Burckardt et Estelle Chassard, La réforme du droit des obligations allemand, la refonte du Bürgerliches Gesetzbuch, *RDAI* 2002, p. 211. [www.schuldrechtsmodernisierung.com](http://www.schuldrechtsmodernisierung.com)

## **Poursuivre la réflexion sur la notion de «support durable» dans le cadre du commerce électronique**

La dématérialisation des échanges et notamment de ceux ayant trait au commerce électronique nécessite des adaptations du cadre juridique existant. Les consommateurs comme les entreprises sont amenés à recevoir et à émettre des documents.

La transmission par voie électronique d'un nombre croissant de documents à caractère commercial entre les professionnels et les consommateurs oblige à raisonner sur la conservation de ces documents par les consommateurs et aux modalités de transmission par les commerçants.

L'ordonnance<sup>257</sup> du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique complète les dispositions du Code civil en ce qui concerne les contrats conclus par voie électronique<sup>258</sup>.

Par ailleurs des dispositions spéciales à certains services commercialisés par voie électronique imposent aux professionnels des obligations de transmission d'informations qui doivent être envisagées en considération des nouveaux articles 1369-1 et 1369-2 du Code civil.

L'ordonnance n° 2005-648 du 6 juin 2005 relative à la commercialisation à distance de services financiers auprès des consommateurs qui transpose la directive 2002/65/CE modifie respectivement les codes de la consommation, des assurances, de la mutualité, de la sécurité sociale et le code monétaire et financier en insérant 5 articles nouveaux.

Les articles nouveaux précisent :

*« Art. L. 121-20-11. – Le consommateur doit recevoir, par écrit ou sur un autre support durable à sa disposition et auquel il a accès en temps utile et avant tout engagement, les conditions contractuelles ainsi que les informations mentionnées à l'article L. 121-20-10. Le fournisseur peut remplir ses obligations au titre de l'article L. 121-20-10 et du présent article par l'envoi au consommateur d'un document unique, à la condition qu'il s'agisse d'un support écrit ou d'un autre support durable et que les informations mentionnées ne varient pas jusqu'à et y compris la conclusion du contrat.*

*Le fournisseur exécute ses obligations de communication immédiatement après la conclusion du contrat, lorsque celui-ci a été conclu à la demande du consommateur en utilisant une technique de communication à distance ne permettant pas la transmission des informations précontractuelles et contractuelles sur un support papier ou sur un autre support durable. » [troisième alinéa non reproduit]*

---

257. Ordonnance n° 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique.

258. Art. 1369-1 du Code civil : « La voie électronique peut être utilisée pour mettre à disposition des conditions contractuelles ou des informations sur des biens ou services. » Art. 1369-2 du Code civil : « Les informations qui sont demandées en vue de la conclusion d'un contrat ou celles qui sont adressées au cours de son exécution peuvent être transmises par courrier électronique si leur destinataire a accepté l'usage de ce moyen. »

Cette notion de support durable est issue de la directive concernant la commercialisation à distance de services financiers auprès des consommateurs<sup>259</sup>. Elle y est définie comme étant «*tout instrument permettant au consommateur de stocker des informations qui lui sont adressées personnellement d'une manière permettant de s'y reporter aisément à l'avenir pendant un laps de temps adapté aux fins auxquelles les informations sont destinées et qui permet la reproduction à l'identique des informations stockées*»<sup>260</sup>.

À cet égard la directive précise que «*les supports durables incluent notamment les disquettes informatiques, les CD-ROM, les DVD et le disque dur de l'ordinateur du consommateur sur lequel le courrier électronique est stocké, mais ils ne comprennent pas les sites Internet, sauf ceux qui satisfont aux critères spécifiés dans la définition des supports durables*»<sup>261</sup>.

Cette même approche de la notion de support durable est retenue par la directive 2002/92 CE du Parlement européen et du Conseil du 9 décembre 2002 sur l'intermédiation en assurance<sup>262</sup> qui donne une définition du support durable dans les termes de la directive 2002/65/CE.

Cette approche, si elle est critiquée au plan technique comme n'offrant pas une sécurité suffisante, est considérée par la Commission européenne comme un moyen d'aborder la problématique du stockage des informations sous forme électronique de manière pragmatique et de prendre en compte le point de vue des consommateurs qui doivent disposer d'instruments simples permettant de se reporter dans le temps aux documents transmis.

Dans le droit positif français et avant la transposition de la directive précitée, il convient de noter que le terme «durable» est utilisé par l'article 1348 alinéa 2 du Code civil en matière de copie fidèle et durable.

L'article 1348 alinéa 2 du Code civil<sup>263</sup> prévoit, depuis la loi du 12 juillet 1980, la notion de «*copie fidèle et durable*», lorsque l'original n'a pas été conservé. Il prévoit ainsi la faculté de présenter, à titre de commencement de preuve par écrit, une copie qui soit une reproduction fidèle et durable de l'original. La reproduction doit être indélébile et

---

259. Directive 2002/65/CE du Parlement Européen et du Conseil du 23 septembre 2002.

260. Art. 2 de la directive 2002/65/CE précitée.

261. Considérant 20 de la directive 2002/65/CE précitée.

262. Journal officiel n° L 9 du 15/01/2003, p. 3-10.

263. Article 1348 alinéa 2 du Code civil: «*Elles reçoivent aussi exception lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. Est réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support.*»

entraîner une modification irréversible du support. Plusieurs décisions permettent de cerner la notion de copie fidèle et durable et la valeur probatoire de ces copies<sup>264</sup>.

En 1980, la question était celle de la durabilité des supports dans le sens d'irréversibilité et d'intangibilité. Aujourd'hui, c'est la pérennisation de l'information, son accessibilité et son intégrité qui doivent être assurées.

Si l'article 1348 alinéa 2 rend possible la pratique de la copie sur microfilms, il limite aussi, dans une certaine mesure, l'utilisation de copies électroniques étant donné qu'est «réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support». En effet, les supports électroniques habituellement utilisés (disques durs, disquettes, disques numériques réinscriptibles, mémoires flash...) ne répondent pas à ce critère de durabilité.

C'est pourquoi il serait souhaitable de préciser la définition légale du «support durable». Il convient néanmoins de noter que la Commission européenne<sup>265</sup> a abordé ce sujet et souhaite traiter des difficultés soulevées précédemment au niveau du droit européen des contrats. La réflexion entourant la notion de support durable doit donc être traitée en fonction de l'avancement des travaux de la Commission.

**Le Forum des droits sur l'internet et la Mission Économie Numérique estiment qu'il est important de préciser la notion de support durable afin de faciliter le développement des échanges du commerce électronique. La réflexion entourant la notion de support durable doit être traitée en fonction de l'avancement des travaux de la Commission de l'Union européenne.**

## **Accompagner l'équivalence fonctionnelle du papier et de l'électronique**

La loi du 13 mars 2000 a pour la première fois en France reconnu une équivalence fonctionnelle entre les écrits sur support papier ou électronique. Il résulte de ce principe que les deux supports disposent de la même force probante. Les écrits sur papier et sur support électronique sont donc mis sur un pied d'égalité.

---

264. Une cour d'appel appréciant souverainement la valeur et la portée de la photocopie qui lui était soumise, a jugé que celle-ci, qui ne révélait aucune trace de falsification par montage de plusieurs documents et permettait de constater que les caractéristiques d'ordre général de l'écriture du bulletin complémentaire de 1992 présentaient de grandes similitudes avec celles de l'écriture du bulletin d'adhésion de 1990, constituait une copie sincère et fidèle du document, au sens de l'article 1348, alinéa 2, du Code civil (Cass. civ., 30 mai 2000: *Bull. civ.* 2000, I, n° 164, p. 106). Une cour d'appel, saisie d'une demande en paiement, ne peut se fonder sur la copie d'un acte certifié conforme à l'original, dès lors que celui à qui la copie est opposée soutient que cette copie n'est pas conforme à l'original dont il demande la production, et à défaut d'un tel acte, dont il lui appartient d'ordonner au demandeur de le produire, elle doit rechercher si la copie versée aux débats par ce dernier est une reproduction fidèle et durable de l'original ou si celui-ci a disparu par suite d'un cas fortuit ou d'une force majeure (Cass. civ., 6 octobre 1998: *Bull. civ.* 1998, I, n° 271, p. 189).

265. Rapport de la Commission sur l'état d'avancement du droit européen des contrats et de la révision de l'acquis, 29 septembre 2005: [http://europa.eu.int/comm/consumers/cons\\_int/safe\\_shop/fair\\_bus\\_pract/cont\\_law/progress05\\_fr.pdf](http://europa.eu.int/comm/consumers/cons_int/safe_shop/fair_bus_pract/cont_law/progress05_fr.pdf)

L'un des intérêts de la conservation électronique peut être, à terme et dans certains contextes, de substituer le document électronique au document «*papier*». Une telle évolution permettrait, selon certains, des économies et des facilités de gestion des documents. Ils s'interrogent donc sur la possibilité de détruire légalement un document originairement sur support papier et constituant une preuve au profit d'un document conservé sur support électronique.

En l'état actuel du droit privé, il convient de noter que cette possibilité n'est pas prévue en France. Les seuls textes précisant ce point concernent les actes authentiques.

Les décrets n° 2005-972 et n° 2005-973 du 10 août 2005 prévoient pour les notaires et les huissiers de justice la possibilité de réaliser des copies électroniques de documents papier<sup>266</sup> sans pour autant prévoir la destruction des documents papier numérisés. Ces numérisations réalisées dans des conditions garantissant «*la reproduction à l'identique*» par un officier public ne sont pas considérées comme des originaux mais bien comme des copies.

À l'étranger certains ont déjà engagé la réflexion ou adopté des solutions.

Le Québec autorise, au travers de la «*loi concernant le cadre juridique des technologies de l'information*», la destruction du document original ou de la copie et son remplacement «*par les documents résultant du transfert*»<sup>267</sup>. Cette disposition vise le cas spécifique du transfert de l'information d'un document qui doit être conservé afin de constituer une preuve; la loi québécoise indique les conditions<sup>268</sup> à satisfaire pour obtenir un tel résultat. Il convient de souligner que cet article est rédigé en termes d'objectifs à atteindre et non de technologies à utiliser. Il existe cependant des exceptions pour certaines catégories de documents. En effet, la conservation sur le support

---

266. Décret n° 2005-972 du 10 août 2005, art. 6 al. 2 et 3: «*Art. 29-4. – Lorsqu'ils sont établis sur support électronique, la conservation des premiers originaux est assurée dans un minutier central établi et contrôlé par la Chambre nationale des huissiers de justice sans préjudice de l'application de l'article 2 du décret du 3 décembre 1979 déjà mentionné. Les premiers originaux sont adressés à ce minutier par l'huissier de justice au plus tard dans les quatre mois de leur établissement. Dans l'attente de leur transfert vers ce minutier, leur conservation devra être assurée par cet huissier de justice au moyen du système prévu à l'article 26. L'huissier de justice qui a dressé l'acte ou qui le détient en conserve l'accès exclusif dans des conditions garantissant sa lisibilité et permettant d'en faire des copies. Art. 29-5. – Les opérations successives justifiées par sa conservation, notamment les migrations dont il peut faire l'objet, ne retirent pas à l'acte sa nature d'original.*» Décret n° 2005-973 du 10 août 2005, art. 37 al. 1 et 2: «*Le notaire peut procéder à la copie sur support électronique d'un acte établi sur support papier après avoir utilisé un système de numérisation dans des conditions garantissant sa reproduction à l'identique. Le notaire qui délivre une copie sur support électronique y mentionne la date et y appose sa signature électronique sécurisée. La copie authentique comporte en outre l'image de son sceau. Mention est portée sur la copie délivrée de sa conformité à l'original.*»

267. Article 20 de la loi concernant le cadre juridique des technologies de l'information: «*Les documents dont la loi exige la conservation et qui ont fait l'objet d'un transfert peuvent être détruits et remplacés par les documents résultant du transfert.*»

268. Il est en effet notamment précisé: «*pour que le document source puisse être détruit et remplacé par le document qui résulte du transfert tout en conservant sa valeur probatoire, le transfert doit être documenté de sorte qu'il puisse être démontré, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée*» (art. 17).

d'origine reste obligatoire pour les documents qui présentent une valeur archivistique, historique ou patrimoniale eu égard aux critères élaborés par la législation québécoise<sup>269</sup>.

En France, il est impossible de considérer que les originaux papier peuvent au travers de la numérisation se voir substituer des « originaux » électroniques. Malgré cela et afin d'éviter, sur le long terme, l'existence d'un document original papier et de sa « copie » électronique, certains envisagent la substitution et la destruction du document sur support papier.

Cette démarche implique que soient soigneusement évalués les coûts respectifs d'une conservation de support papier et une conservation de supports électroniques et que le cadre juridique le permette.

À ce titre, deux hypothèses seraient envisageables :

- soit les deux documents sont considérés comme équivalents ;
- soit une règle de preuve sera substituée à une autre.

Dans la première hypothèse, le mode de preuve reste inchangé et c'est la valeur du document qui sera jugée comme équivalente, et ce quel que soit son support.

Dans la seconde hypothèse, il s'agira de considérer le document résultant du transfert comme une copie et de l'accepter à titre de preuve.

La première solution ne nécessite pas d'adaptation de la législation mais suppose que l'on puisse accorder une confiance parfaite au processus permettant la réalisation du document de transfert qui est tenu pour un original.

Dans le cas où le titre originaire et le document résultant du transfert ont une force probante équivalente, le juge ne peut les refuser et ne devra trancher entre les deux documents qui si les deux subsistent et s'ils présentent une différence. Cette situation existant déjà dans l'environnement des actes sur support papier, elle ne nécessitera pas ou peu d'adaptation.

La seconde hypothèse repose sur un mécanisme juridique tel que celui prévu à l'article 1348 alinéa 2 du Code civil. Elle permet de recourir à la production d'une copie fidèle et durable en lieu et place d'un titre original lorsque celui-ci est détruit et qu'il n'est établi qu'à titre probatoire (*ad probationem*). Dans ce cas, le juge peut apprécier les caractères de la copie et l'accepter comme preuve, celle-ci pouvant être contestée par tout moyen à disposition des parties.

Il convient cependant de préciser que la seconde solution ne pourrait s'appliquer aux écrits établis à titre de validité (*ad validitatem*) ainsi que dans le domaine de la facturation électronique où l'administration fiscale impose la conservation de l'original (ou dans d'autres hypothèses où le terme « original » ou « document d'origine » peut être utilisé). En effet, les pièces justificatives relatives à des opérations ouvrant droit,

---

269. Art. 20 loi susmentionnée : « Toutefois, doit être conservé sur son support d'origine le document qui, sur celui-ci, présente une valeur archivistique, historique ou patrimoniale eu égard aux critères élaborés en vertu du paragraphe 1<sup>er</sup> de l'article 69, même s'il a fait l'objet d'un transfert ».



du point de vue fiscal, à une déduction en matière de taxes sur le chiffre d'affaires doivent être conservées en original pendant 6 ans<sup>270</sup>.

Toutefois, il convient de bien réfléchir aux conséquences induites sur les notions d'original et de copie (notamment sur le maintien de ces deux notions et sur la pertinence de leur distinction).

**Le Forum des droits sur l'internet et la Mission Économie Numérique considèrent qu'il est nécessaire de mener une réflexion approfondie, tant économique que juridique, sur la possibilité de substituer un document sur support électronique à un document sur support papier et de détruire, sous certaines conditions, le document d'origine. Cette réflexion pourra être conduite sous l'égide du Ministère de la Justice.**

---

270. La conservation de l'original pendant 6 ans s'effectue de la façon suivante :  
– conservation d'un original pour les pièces justificatives d'un droit à déduction en matière de taxes sur le chiffre d'affaires et notamment pour les factures d'achat ;  
– conservation d'un original ou d'une copie qui en est la reproduction fidèle et durable pour les autres documents justificatifs, notamment les copies des factures de vente

## Annexe 1

### **Synthèse des recommandations**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent que toute réflexion sur le cadre réglementaire de la conservation électronique des documents respecte les principes de neutralité technologique et organisationnelle et que le statut juridique des documents ne soit pas modifié du fait de leur conservation électronique.

#### Modalités d'une conservation électronique des documents

##### **Les critères d'une conservation électronique garantissant l'intégrité des documents**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent que la notion d'intégrité du document de l'article 1316-1 du Code civil soit assurée par le respect cumulé des trois critères suivants :

- lisibilité du document ;
- stabilité du contenu informationnel ;
- traçabilité des opérations sur le document.

##### **Les bonnes pratiques d'une politique de conservation électronique des documents**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent :

- Aux acteurs souhaitant conserver des documents sous forme électronique l'emploi de bonnes pratiques en vue de satisfaire aux conditions de l'article 1316-1 du Code civil.
- L'usage de ces bonnes pratiques doit se poursuivre tout au long des quatre étapes du processus de conservation : le versement, l'enregistrement, la gestion et la restitution des documents.

##### **L'impact des migrations, notamment sur les documents signés au moyen d'un procédé cryptographique**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent que sous réserve de la possibilité de vérifier l'intégrité des documents conservés, les opérations successives justifiées par cette conservation, notamment les migrations, ne retirent pas au document son statut juridique d'origine.

## Les moyens complémentaires de garantir la mise en place d'un environnement de confiance

### **Le contrat de service d'archivage (conservation externe)**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent l'emploi de contrats de services se référant aux bonnes pratiques édictées. Il convient également que ce contrat de service soit accompagné de certaines « clauses types » :

- clause de sécurité;
- clause d'information et de conseil;
- clause de reprise et de continuité;
- clause de confidentialité;
- clause d'assurance professionnelle;

### **Les chartes ou politiques d'archivage (conservation interne)**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent la mise en place d'un document interne (charte ou politique d'archivage) se référant aux bonnes pratiques édictées et accompagné d'un contrôle-qualité.

## Pistes de prospective pour la confiance dans l'économie numérique

### **Harmoniser les durées de conservation et de prescription au niveau européen**

Le Forum des droits sur l'internet et la Mission Économie Numérique recommandent que les délais de conservation soient harmonisés pour tous les documents quels que soient leurs supports. À cet égard, le Forum et la Mission considèrent qu'il est nécessaire de mener, à une échelle européenne, une réflexion portant sur la réduction des délais de prescription et de conservation.

### **Poursuivre la réflexion sur la notion de « support durable » dans le cadre du commerce électronique**

Le Forum des droits sur l'internet et la Mission Économie Numérique estiment qu'il est important que soit précisée la notion de support durable afin de faciliter le développement des échanges du commerce électronique. La réflexion entourant la notion de support durable doit être traitée en fonction de l'avancement des travaux de la Commission de l'Union européenne sur le contrat européen.

### **Accompagner l'équivalence fonctionnelle du papier et de l'électronique**

Le Forum des droits sur l'internet et la Mission Économie Numérique estiment qu'il est nécessaire de mener une réflexion approfondie, tant économique que juridique, sur la possibilité de substituer un document sur support électronique à un document sur support papier et de détruire, sous certaines conditions, le document d'origine. Cette réflexion permettra d'accompagner l'équivalence fonctionnelle telle qu'elle est envisagée dans le cadre de la loi du 13 mars 2000.

## Annexe 2

### Composition du groupe de travail

*La composition du groupe de travail était la suivante :*

**Françoise BANAT-BERGER**, direction des Archives de France

**Philippe BAZIN**, avocat, association pour le Développement de l'informatique juridique

**Arnaud BELLEIL**, directeur associé, Cecurity.com

**Nicolas BOUTIN**, Fédération bancaire française

**Mireille CAMPANA**, sous-directrice et **Antoine TARDIVO**, chef de bureau société de l'information, direction générale de l'industrie, des technologies de l'information et des Postes, ministère de l'Économie des Finances et de l'Industrie

**Anne CANTEAUT**, chargée de recherche, Institut national de recherche en informatique et en automatique (INRIA)

**Éric CAPRIOLI**, avocat, vice-président Fédération nationale des Tiers de confiance

**Gérard CATHALY-PRETOU**, président de la Commission de normalisation 171 « Applications en gestion documentaire », Association française de normalisation (AFNOR)

**Frédéric COUCHET**, président, Free SoftWare Foundation France

**Bruno COUDERC**, président, Association des professionnels de la gestion électronique des documents (APROGED)

**François COUPEZ**, juriste, Société générale

**Didier COURTAUD**, président de l'association Aristote, ingénieur au Commissariat à l'énergie atomique (CEA)

**Guillaume DESGENS-PASANAU**, responsable du contentieux et des sanctions, Commission nationale de l'informatique et des libertés (CNIL)

**Seif ELHOUTI**, juriste, direction des Affaires civiles et du Sceau, ministère de la Justice

**Marie-Laure LAFFAIRE**, avocate, cabinet Lexvia

**Isabelle de LAMBERTERIE**, directeur de recherche, Centre national de la recherche scientifique (CNRS)

**Marie-José PALASZ**, chef de service de la direction des affaires juridiques, ministère de l'Économie des Finances et de l'Industrie

**Jean-Marc RIETSCH**, expert au CoDiL, organe de labellisation des métiers de la confiance

**Pascal SOUHARD et Gabriel RAMANANTSOAVINA**, Agence pour le développement de l'administration électronique (ADAE)

**Gérard WEISZ**, secrétaire général, Fédération nationale des Tiers de confiance

*Rapporteurs des travaux du groupe :*

**Gilles d'ANCHALD**, chargé de mission à la Mission Économie Numérique

**Jean GONIÉ**, juriste, chargé de mission au Forum des droits sur l'internet

**Stéphane GRÉGOIRE**, juriste, chargé de mission au Forum des droits sur l'internet

## Annexe 3

### Auditions

*Le groupe de travail a procédé aux auditions suivantes :*

**Pascal AGOSTI**, avocat, cabinet Caprioli

**Laura AHO**, Access International Consulting, Finlande

**Christiaan ALBERDINGK THIJM**, avocat, SOLV Law firm, Pays Bas

**Christophe ALVISET**, sous-directeur de l'informatique, ministère de l'Économie des Finances et de l'Industrie

**Valentin ANDERS**, avocat, Johan, Schluter Law Firm, Danemark

**Jean-Claude ASSELBORN**, professeur, Faculty of Law, Economics and Finance, Luxembourg

**Françoise BANAT-BERGER**, ministère de la Culture, direction des Archives de France, responsable du Département de l'innovation technologique et de l'innovation (DITN)

**Serge BERAUD**, directeur Partenaires Services, XEROX France

**June BESEK**, Executive Director, Kernochan Center for Law, États-Unis

**Jean-Marc BING**, Fédération bancaire française

**Jean-François BLANCHETTE**, professeur, université de Californie, Los Angeles

**Olivier BLONDEAU**, sociologue

**Nicolas BOUTIN**, Fédération bancaire française

**Liette BOULAY**, notaire, directrice des services de certification, Notarius, Canada

**Charles du BOULLAY**, directeur général, société CDC Zantaz, filiale de la Caisse des dépôts et consignations

**Monique BROWN**, Certiposte, Belgique

**Anne CANTEAUT**, chargée de recherche, INRIA

**Gérard CATHALY-PRETOU**, président de la commission d'applications en gestion documentaire – CN 171, AFNOR

**Éric CAPRIOLI**, avocat, vice-président Fédération nationale des Tiers de confiance

**Emmanuel CAUVIN**, juriste, Arcelor

**Agneta CEDERBERG**, manager, Ernst & Young Suède

**Cynthia CHASSIGNEUX**, Lex Electronica (université de Montréal), Canada

**Majella CRENNAN**, avocat, Irlande

**Frédéric COUCHET**, président, Free SoftWare Foundation France

**Bruno COUDERC**, président, Association des professionnels de la gestion électronique des documents (APROGED)

**François COUPEZ**, juriste, Société générale

**Didier COURTAUD**, président de l'association Aristote, ingénieur, CEA

**Adrian CUNNINGHAM**, Archives Nationales d'Australie

**Guillaume DESGENS-PASANAU**, Commission nationale de l'informatique et des libertés

**Jean DEVEZE**, professeur de droit à l'Université des sciences sociales de Toulouse, avocat au barreau de Toulouse

**Jean DONIO**, expert judiciaire

**Geneviève DROUHET**, responsable du service des Archives, Groupe Médéric

**Jos DUMORTIER**, Lawfort, professeur de droit, K.U. Leuven, Belgique

**Olivier DUNANT**, avocat, Ernst & Young, Suisse

**Thomas ELM**, juriste, Cabinet Lexvia

**Louis FAIVRE d'ARCIER**, responsable des archives électroniques, Archives de Paris

**Bernard FLOTTER**, secrétaire général EuroExpert, Allemagne

**Jean-Pierre GINGUENAUD**, responsable Assurance Qualité, Biomérieux

**Jane GINSBURG**, professeur, *Literary and Artistic Property Law*, Columbia Law School, États-Unis

**Jean-Jacques GOMEZ**, magistrat, Cour de cassation

**Alain HALVICK**, Groupe Aspheria

**Andrea HÄNGER**, Archives nationales de Coblenz, Allemagne

**Else HELLAND**, avocat, Johan, Schluter Law Firm, Danemark

**Thomas HESSLER**, avocat, Ernst & Young Law, Allemagne

**Torbjörn HÖRNFELDT**, Archives nationales, Suède

**Claude HUC**, ingénieur au CNES, président du groupe de travail « pérennisation des informations numériques », Association ARISTOTE

**Kristine KANEKO**, avocat, Thelen Reid & Priest LLP, États-Unis

**Peter KARTOUS**, directeur de la Direction des Archives, Slovaquie

**Greg KOZAK**, University of British Columbia, Canada

**Marie-Laure LAFFAIRE**, avocate, cabinet Lexvia

**Isabelle DE LAMBERTERIE**, directeur de recherche, Centre national de la recherche scientifique (CNRS)

**Pierre LECLERCQ**, conseiller honoraire à la Cour de cassation et ancien commissaire à la CNIL

**Michel LESOURD**, directeur adjoint des études techniques, Conseil supérieur de l'Ordre des experts-comptables

**Marc LEWIS**, avocat, Tite & Lewis, Royaume-Uni

**Stéphane LIPSKI**, expert-comptable et commissaire aux comptes, Compagnie nationale des commissaires aux comptes

**Manuel LOPES ROCHA**, avocat, Barrocas & Alves Pereira, Portugal

**Francisco LOPEZ**, ministère de la Fonction publique, Espagne

**Vincent LORET**, Directeur informatique, Société CDC Zantaz, filiale de la Caisse des Dépôts et Consignations

**Philippe MANTEAU**, avocat, Thelen Reid & Priest LLP, États-Unis

**Claude MARSEILLE**, avocat, Fasken Martineau Dumoulin, Canada

**Jérôme MENDIELA**, directeur du développement, Cecurity.com

**Alexandre MESNAIS**, directeur Juridique, XEROX France

**Rauer MEYER**, avocat, Thelen Reid & Priest LLP, États-Unis

**Alain MICHARD**, président AM<sup>2</sup> Systems, Active Memory Management

**Annie MOREL**, services audit et sécurité, Ernst & Young France  
**Erik MOTELAY**, Business Manager SONERA Source, Finlande  
**Janne MYKRÄ**, Archives nationales, Finlande  
**Elena ÖRTHOLN**, Manager, Ernst & Young Suède  
**Gauthier OSSELAND**, responsable archives Pinault-Printemps-La Redoute  
**Radouane OUDRHIRI**, Systonomy, Royaume-Uni  
**Lucien PAULIAC**, président de l'association «Preuve & Micrographie», président de la Commission de normalisation, CN 43 «Archivage des données électroniques» à l'AFNOR  
**Thierry PIETTE-COUDOL**, avocat  
**Corinne PIRLOT**, avocat, Ernst & Young, Suisse  
**Sonia QUEIROZ VAZ**, avocat, Barrocas & Alves Pereira, Portugal  
**Claude RAPOPORT**, Portima, Belgique  
**Martine RAYNAUD**, chargée de mission Europe, CFCE  
**Arnaud RAYNOUARD**, professeur, Université de Toulouse I  
**Claude RECORDON**, Certiswiss, Suisse  
**Chris REED**, Professor of Electronic Commerce Law at CCLS – London, Royaume-Uni  
**Bernard REYNIS**, notaire, Conseil Supérieur du Notariat  
**Jean-Marc RIETSCH**, expert au CoDiL, organe de labellisation des métiers de la confiance  
**Eric RUIZ**, Société générale  
**Urbana SANCHEZ QUINTANILLA**, Agencia Tributaria, Espagne  
**Jean-laurent SANTONI**, société MARSH  
**Leena SAVE**, Business Manager SONERA Source, Finlande  
**Valérie SEDALLIAN**, avocate  
**Silke VON LEWINSKY**, Docteur, Head of department on international law at the Max Planck Institute, Munich, Allemagne  
**Jukka TAPANINEM**, General Manager, BasWare, Finlande  
**Michel TILLOY**, directeur administratif et financier, Ligne Roset-Cinna  
**Christian TREMLET**, directeur de la communication, Astérior-Crédit Agricole  
**Jarkko TUOMINEN**, FinnFacts, Finlande  
**Olivier de SOLAN**, direction des archives de France, responsable du département de l'innovation technologique et de l'innovation (DITN).  
**Gérard WEISZ**, secrétaire général, FNTC  
**Jacques DE WERRA**, avocat, Chargé de cours à l'université de Genève, Suisse  
**Susan WILDEY**, avocat, Tite & Lewis, Royaume-Uni  
**Jean-Michel YOLIN**, membre du Conseil général des Mines, président de la section Innovation et entreprise

Deuxième partie

# **L'information et la sensibilisation**



# **Rapport sur le projet de carte nationale d'identité électronique (CNIE)**

*Rapport publié le 16 juin 2005*

## **Introduction**

Le projet de création d'une carte nationale d'identité électronique (CNIE) est un projet majeur. Il a pour objectif de renforcer la qualité et la sécurisation des titres d'identité, mais aussi d'offrir de nouveaux services aux citoyens en leur donnant les moyens de prouver leur identité sur internet et de signer électroniquement. Ce faisant, il devient un projet qui va changer une partie de la vie des Français. Le ministère de l'Intérieur a souhaité recourir à un projet de loi pour le mettre en œuvre.

Le Forum des droits sur l'internet a pris l'initiative de proposer au ministère de l'intérieur d'organiser un débat public sur ce projet afin de donner à toutes les sensibilités et à tous les points de vue la possibilité de s'exprimer. Le ministère de l'intérieur a ainsi officiellement mandaté le Forum à ce sujet en janvier 2005 (voir lettre de mission en annexe).

Pour répondre à cette mission, le Forum des droits sur l'internet a mis en place trois outils : un débat en ligne et un débat en régions qui ont duré quatre mois (début février à début juin 2005) ; plus de 3 000 messages ont été postés et des manifestations publiques se sont tenues dans six villes ; par ailleurs, le Forum a invité des personnalités expertes à participer aux débats, soit dans les régions, soit en envoyant des contributions dans le débat en ligne.

Le Forum a souhaité également organiser un sondage sur le sujet. Avec l'institut IPSOS, il a ainsi recueilli l'opinion de 950 personnes, correspondant à un échantillon représentatif de la population et ces résultats orientent également les conclusions (voir sondage en annexe).

À partir de l'ensemble de ces contributions, le Forum des droits sur l'internet a élaboré le présent rapport. Le rapport a été adopté par le Conseil d'orientation du Forum dans sa séance du 14 juin 2005.

Ce rapport a pour objectif d'alimenter la réflexion des pouvoirs publics sur le sujet, dans la perspective du débat parlementaire.

## Les points forts du débat public

Sur les questions centrales

### Sur la justification du projet

Les enjeux et les changements induits par le projet de carte nationale d'identité électronique (caractère obligatoire et payant, base centralisée, biométrie, délivrance dans quelques mairies...) sont de la première importance. Les motivations d'un tel projet se doivent d'être clairement expliquées et convaincantes, les garanties largement développées, les aspects techniques et de sécurité fondés sur des travaux fiables et des études nombreuses. En effet, comme le précise Patrice Flichy, professeur de sociologie, *«en matière d'atteinte aux libertés publiques, les fantasmes peuvent parfois devenir réalité. Aussi est-il important de donner au citoyen le maximum de garanties et même plus que ce que les techniciens estiment sans doute nécessaire.»*<sup>271</sup>

Tout le débat tourne en effet autour de l'équilibre à trouver entre protection des libertés individuelles et sécurité de l'identité et sur la façon dont le ministère de l'intérieur a pu faire comprendre aux Français participant aux débats sa vision et ses projets dans le domaine de l'identité nationale électronique sécurisée.

Or, comme le note Michel Elie, président de l'Observatoire des Usages de l'Internet, *«nous demandons encore à être convaincus par votre solution»*<sup>272</sup>. Ces propos reflètent bien le sentiment qui s'est constamment exprimé tant en ligne qu'en régions. Alors que d'un côté les changements annoncés semblent bien réels, de l'autre, le projet semble lancé avec *«précipitation»*<sup>273</sup> et avancé pour des raisons trop légères sans justification convaincante.

Le ministère de l'Intérieur justifiait la mise en place d'une CNIE par le biais de quatre arguments :

#### Lutter contre la fraude à l'identité

La lutte contre la fraude à l'identité semble être une préoccupation majeure des Français puisqu'à la question *«dans le cadre de la lutte contre la fraude à l'identité, le ministère de l'intérieur envisage de remplacer la carte d'identité actuelle par une carte d'identité électronique comportant des données personnelles numérisées telles que empreintes digitales, photographie, voire iris de l'œil»*, 74 % des sondés répondent favorablement et 25 % défavorablement.

Pour autant, et alors que cet argument semble fondamental voire justifier en lui-même la mise en place d'une carte nationale d'identité électronique, le ministère de l'intérieur ne dispose d'aucune donnée chiffrée précise à l'appui de cet argument ; aucune étude systématique n'a été conduite en France. Les chiffres avancés dans

---

271. Contribution sur internet de Patrice Flichy, 13 avril 2005.

272. Message sur internet de Michel Elie, 17 avril 2005.

273. Contribution de Martial Gabillard, débat de Rennes, 11 mai 2005.

le débat par le ministère sur la fraude à l'identité ne s'appuient que sur des études étrangères (principalement américaines ou britanniques). À cet égard, beaucoup se sont demandé s'il est possible de se référer à des chiffres avancés dans des pays étrangers alors que les instruments et dispositifs d'identification qui y sont employés ne sont pas du tout les mêmes que ceux mobilisés en France (par exemple, pour les États-Unis, surtout le numéro de sécurité sociale et le permis de conduire et pour le Royaume-Uni, l'inexistence de carte nationale d'identité depuis 1952).

À cela le ministère de l'intérieur a répondu tout au long du débat que seuls les ministères des finances et des affaires sociales seraient à même d'établir le coût de la fraude et il a précisé que le Sénat a justement mis en place une mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire afin notamment de pouvoir établir des données chiffrées sur la fraude. Le ministère a cependant admis qu'il convenait de travailler sur ce point.

### **Lutter contre le terrorisme**

De même, cet argument a peu convaincu et les questions ont été nombreuses : un tel dispositif permettra-t-il vraiment de repérer un primo-terroriste ? En quoi cela empêchera-t-il quelqu'un qui souhaite commettre un acte terroriste de ne pas obtenir, en toute légalité, une CNIE ? À cet égard, certains se demandent si l'on ne se sert pas des contraintes internationales sur le projet passeport (Règlement européen du 13 décembre 2004<sup>274</sup> adopté dans un contexte de lutte contre le terrorisme afin d'améliorer le contrôle des passages aux frontières et de répondre aux exigences américaines) pour faire adopter la CNIE. Or, le débat a montré que si la France doit appliquer le règlement sur le passeport dans un bref délai, cette obligation ne concerne pas la carte d'identité nationale<sup>275</sup>. De plus, l'argument du terrorisme a surtout donné l'impression que la France subissait des pressions étrangères, européennes et surtout américaines.

Le ministère de l'intérieur a précisé que la fausse identité (ou l'usurpation) est souvent à la base du phénomène terroriste et qu'en ce sens, toute action destinée à rendre plus fiable l'identité des citoyens est un moyen de lutter contre les atteintes à la sécurité publique. En ce qui concerne l'articulation avec le projet passeport, le ministère a reconnu qu'aucune obligation ne concernait effectivement la CNI, même si le fait de coupler les deux procédures pouvait être utile et opportun au regard notamment de la compatibilité de la carte avec celles des autres États européens.

---

274. Règlement (CE) n° 2252/2004 du Conseil européen du 13 décembre 2004 «*établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres*».

275. L'article 1 alinéa 3 du règlement exclut la carte d'identité de son champ d'application : «*Le présent règlement s'applique aux passeports et aux documents de voyage délivrés par les États membres. Il ne s'applique pas aux cartes d'identité délivrées par les États membres à leurs ressortissants*».

### **Simplifier la vie du citoyen: une seule procédure pour la demande de deux titres (CNIE et passeport) et une accélération des renouvellements**

Cet argument est le seul où il a pu être reconnu un intérêt: mais cet intérêt a été estimé très réduit par rapport aux enjeux du projet.

### **Offrir aux citoyens les moyens de signer électroniquement ses transactions sur internet**

Cet argument n'a finalement que peu intéressé les participants qui ne voyaient pas son utilité, voire ont exprimé des réticences à avoir accès, sur un même support, à des usages administratifs et à des usages commerciaux ou encore de pouvoir faire une transaction sur internet, réseau ouvert et pouvant présenter de nombreuses failles de sécurité.

À l'issue du débat, on peut estimer, que le ministère de l'intérieur n'a pas convaincu dans les arguments avancés pour justifier le projet de carte nationale d'identité électronique. C'est d'ailleurs ce que résume l'internaute Algair, qui estime que «*dans l'équilibre fondamental entre protection des libertés individuelles et sécurité de l'identité, actuellement rien ne me convainc de la nécessité d'accepter d'abandonner un peu de liberté au profit de plus de sécurité*».

Ce déficit d'explication a par ailleurs contribué à nourrir des craintes et à brouiller les enjeux. Ainsi, pour certains comme les internautes Minas et Zébulon, la mise en place de la CNIE émane d'une volonté de «*flicage*» du gouvernement ou fait suite aux peurs «*sécuritaires développées par les Américains*» depuis les attentats du 11 septembre 2001. D'autres, n'y voient qu'une question d'argent et une pression des industriels (fabrication des puces, des cartes, des lecteurs, marché de la biométrie etc.). Ce déficit d'explication a également entraîné des confusions ou des erreurs. En effet, beaucoup ont estimé que la présentation du projet entraîne la confusion par le mélange des genres (projet destiné à la lutte contre le terrorisme, contre la fraude à l'identité, à développer la signature électronique, à des utilisations individualisées au moyen d'un «*portfolio personnel*»...). D'autres ont confondu les étiquettes RFID de la grande distribution avec l'interface radio de la carte d'identité ou ont cru que la carte servirait de moyen de paiement.

Cette impression générale de confusion est renforcée par le manque de coordination qui a été noté entre différents projets qui semblent néanmoins liés: CNIE, carte de vie quotidienne, dématérialisation de l'état civil.

### **Sur la protection de la vie privée**

À titre liminaire il convient de préciser que l'aspect «*vie privée*» est celui qui a donné lieu au plus grand nombre d'échanges. Ces échanges ont exprimé des interrogations, des craintes mais aussi des erreurs voire des propagations de rumeurs; certains ont pu par exemple dire que la CNIE serait «*un premier pas vers une puce sous-cutanée implantée chez tous les Français*». Comme le remarque Pierre Trudel, professeur à l'université de Montréal<sup>276</sup>: «*Il demeure troublant de constater à quel point les risques de dérives semblent dominer les débats lorsqu'il est question d'outils et de procédés*

---

276. Contribution sur internet de Pierre Trudel, 11 mai 2005.

*qui concernent l'identification des personnes [...] Rituellement, on exprime des préoccupations sur le potentiel liberticide des technologies de l'information [...]. La plupart des craintes à l'égard de l'usage des technologies de l'information concernent les opérations de surveillance policière.»*

De façon générale, beaucoup d'intervenants ont estimé que le passage de l'identité papier à l'identité électronique recèle un certain nombre de dangers en termes de protection de leur vie privée: la CNIE pourrait préfigurer la possibilité de fichier les individus, de recouper diverses informations et, à terme, de voir l'apparition d'une administration orwellienne – spectre du «Big Brother». Ils craignent également avec cette carte d'être «tracés». À cet égard, de nombreuses discussions ont eu lieu entre les internautes. À ceux qui notent que ce traçage existe déjà de facto dans la vie de tous les jours (carte bancaire, téléphone portable...), d'autres répondent que le risque n'est pas le même car avec ce projet ce serait l'État qui mettrait en place un tel principe.

En revanche, pour d'autres participants, la mise en place d'une carte nationale d'identité électronique ne suscite pas de craintes particulières et permettrait de sécuriser utilement l'identité.

#### **Sur les risques dans l'utilisation d'un fichier centralisé des empreintes digitales numérisées**

De nombreuses interrogations et critiques ont porté sur la mise en place d'une base centrale et sur les risques qui peuvent en découler. Pour Pierre Piazza, historien de la carte d'identité et chargé de recherche à l'Institut National des Hautes Études de Sécurité<sup>277</sup>, «*la constitution de bases de données centralisées contenant des informations relatives aux demandeurs de cartes d'identité a constamment été au cœur des préoccupations des autorités*» depuis 1921. Il note également qu'avec «*l'émergence des débats sur l'informatisation de la carte d'identité à partir du début des années 1980, les tentatives de création de fichiers centralisés de données nominatives par le ministère de l'intérieur font l'objet des critiques les plus virulentes*»<sup>278</sup>.

À cet égard il est très intéressant de comparer les résultats du sondage avec les impressions générales et réactions telles qu'issues du débat public. À la question: «*le ministère de l'intérieur prévoit de constituer un fichier informatique national des empreintes digitales. Laquelle de ces deux opinions se rapproche le plus de la vôtre?*», 75 % des sondés répondent que c'est «*une bonne chose car cela permettra de lutter plus efficacement contre les fraudes*». 23 % estiment que «*c'est une mauvaise chose car cela constitue une atteinte à la liberté individuelle*».

Le débat a montré que, parmi ceux qui s'interrogent sur la mise en place d'une base centrale, deux types de risques ont principalement été évoqués: le risque de croisement de fichiers et de fichage des individus (à cet effet, beaucoup ont d'ailleurs proposé des schémas alternatifs à une base centrale) ainsi que celui d'une évolution future de l'usage de la base.

---

277. Pierre Piazza, *Histoire de la carte nationale d'identité*, Paris, Odile Jacob, 2004.

278. Message sur internet de Pierre Piazza, 13 avril 2005.

### **Le risque de croisement de fichiers et de fichage des individus**

Constatant que les fichiers actuels sont décentralisés, certains craignent qu'une base centrale touchant toute la population ne conduise à terme à un fichage généralisé des individus. Constatant que les interconnexions de fichiers existent depuis déjà longtemps, d'autres estiment que la véritable question est celle de l'encadrement de ces interconnexions et des consultations des données.

Pour d'autres encore, comme l'internaute Beretta, tout est «*un problème de finalité : si la biométrie a pour unique finalité d'associer un titre à son porteur quelle est l'utilité d'un fichier central des empreintes si ce n'est une vaste opération de police ? [...] Si le fichier n'a pas de vocation policière cela devrait suffire à détecter la fraude ou les identités multiples*». De nombreux internautes vont d'ailleurs dans ce sens, Zorglub42 se demande s'il est vraiment nécessaire, en fonction de l'objectif recherché, de mettre en place un fichier centralisé ; il précise que «*si le but du fichier est de «lutter contre l'usurpation d'identité [...] un simple fichier de signature/hash/checksum des empreintes suffirait*». De même AAA propose «*un fichier central de gestion des cartes sans lien avec l'identité en clair du porteur. Le seul lien serait un hash d'une empreinte biométrique pour éviter les fraudes. La gestion des cartes permettrait de savoir si une carte est valide, perdue, volée... Le hash permettrait d'éviter qu'un même individu puisse avoir deux cartes avec des identités différentes*». Enfin, l'internaute Alice propose un même type de scénario qui empêche de retrouver l'identité d'une personne à partir de ses données biométriques. Cet internaute précise que ce scénario protégerait davantage les données personnelles (empêcherait tout passage d'une base à l'autre et l'utilisation des données pour une autre fin que celle pour laquelle elles ont été collectées) mais que son unique finalité serait de gérer la fraude au renouvellement et d'assurer une délivrance sans doublon de cartes. Enfin, comme Alice le précise «*cette approche paraît robuste au détournement de finalité par contre, elle a un inconvénient structurel : elle ne permet pas d'identifier des victimes de catastrophes ou des amnésiques, et ne permet pas de lever le doute dans le cas où la biométrie est ou a été rendue illisible... Mais il faut savoir ce que l'on veut.*»

De plus, lors du débat de Lyon, il a été proposé deux alternatives au projet :

1) Il a été suggéré d'abandonner le projet de CNIE en renforçant la sécurité de l'actuelle carte nationale d'identité, en la rendant obligatoire et en sécurisant et informatisant l'état civil. De façon générale, il a d'ailleurs été souligné que, quel que soit le projet retenu par le Gouvernement, sans informatisation de l'état civil, le projet INES risque d'avoir des failles.

2) Plutôt que d'instaurer une carte d'identité électronique avec une base centralisée d'empreintes digitales numérisées, il a été proposé de créer une CNIE sans base centrale où les données numérisées seraient uniquement dans la puce de la carte. Ce scénario a rencontré un certain écho et de nombreux intervenants ont ainsi souhaité, à l'instar d'Éric Caprioli<sup>279</sup>, que les données biométriques soient uniquement dans la puce et qu'une base centrale ne soit pas mise en place. Meryem Marzouki, prési-

---

279. Contribution sur internet d'Éric Caprioli, 1<sup>er</sup> juin 2005.

dente de l'association IRIS (Imaginons un Réseau Internet Solidaire) a présenté<sup>280</sup> un schéma alternatif qu'elle considère acceptable. Dans ce schéma, qui se rapproche, pour partie, de celui susmentionné, la CNIE ne doit qu'authentifier le porteur (la personne est bien celle qu'elle prétend être), à l'exclusion de toute possibilité d'identification d'un individu anonyme parmi une population; la puce ne doit donc servir qu'à authentifier la carte comme étant un document non falsifié. IRIS estime également que la carte ne devra comporter aucun élément biométrique (cf. l'Italie, qui a développé une carte électronique où les empreintes digitales sont facultatives; la Belgique propose une carte sans biométrie mais avec base centrale), que la photographie ne devra pas figurer sous forme numérisée dans la puce, mais uniquement de manière visible sur la carte pour identification par un contrôleur humain et qu'enfin il ne devra pas y avoir de constitution de base de données centralisée à l'image par exemple de l'Italie où la carte fonctionne sans base centrale.

Cette solution fait écho aux remarques de François Giquel, vice-président de la Commission nationale de l'informatique et des libertés, qui a rappelé<sup>281</sup> qu'il existe d'autres scénarios pour la mise en place d'une CNIE en Europe. C'est le cas en Italie (carte sans base centrale et avec biométrie) ou encore en Belgique (carte sans biométrie mais avec base centrale car ce pays dispose d'un Registre national de la population).

De façon générale, le ministère a estimé que cette alternative ne répondrait pas à l'objectif du projet qui est de lutter contre la fraude à l'identité: seule une base centrale des empreintes permettrait d'éviter la délivrance à une même personne de titres sous plusieurs identités différentes ou à plusieurs personnes d'un titre sous une même identité. En revanche, le ministère de l'intérieur a proposé, dans le débat sur internet, une alternative en termes de biométrie en envisageant (à titre théorique, car cela ne figure pas dans le projet INES) que la puce de la carte contienne les empreintes (qui sont faciles à vérifier lors d'un passage de frontière), mais que la base centrale ne contienne pas les empreintes digitales, mais un autre élément biométrique comme l'iris de l'œil.

#### ***Le risque d'une évolution possible de l'usage de la base***

À l'instar de Michel Tubiana<sup>282</sup>, président de la Ligue des droits de l'Homme ou encore de Meryem Marzouki<sup>283</sup>, de nombreux intervenants ont noté les risques d'une évolution possible de l'usage de la base par les pouvoirs publics via un élargissement de l'accès à d'autres agents (cf. élargissement du nombre d'agents ayant accès au fichier du Système de Traitement des Infractions Constatées – STIC) ou un élargissement du contenu de la base à d'autres données. L'hypothèse la plus noire d'un changement de régime – spectre du retour d'un régime du type vichyste – a même été évoquée.

---

280. Contribution de Meryem Marzouki, débat de Lille, 27 avril 2005.

281. Contribution de François Giquel, débat de Paris, 11 avril 2005.

282. Contribution de Michel Tubiana, débat de Paris, 11 avril 2005.

283. Contribution de Meryem Marzouki, débat de Lille, 27 avril 2005.

### **Sur la maîtrise de la carte par son titulaire et sur les personnes habilitées à consulter les données stockées**

Beaucoup ont souhaité savoir quelle maîtrise aura le citoyen sur les données inscrites sur sa carte et dans les fichiers. Certains, comme Le Guet, souhaitent que toutes les informations de la puce puissent être lues et effacées par le titulaire, que le chargement d'autres informations ne soit possible qu'avec son autorisation expresse et que celui-ci sache exactement quelles sont les informations qui peuvent être consultées par un tiers. De même Michel Elie estime que *«la cnie ne doit pas pouvoir être lue sans le consentement explicite de son porteur [...] Seul le porteur peut affirmer qu'il reconnaît pouvoir être identifié au moyen de cette carte»*. Darhf souhaite que *«L'État n'ait accès à des données privées sur le citoyen qu'avec son propre consentement ou celui de la justice (indépendante) dans les affaires relevant de la sécurité»*.

D'autres se demandent quelles garanties seront apportées sur les personnes pouvant accéder aux données (quels seront ces agents, de quels droits et de quelles façons auront-ils accès aux données, quelle habilitation aura un agent de mairie par rapport à un magistrat ou un policier?). Beretta et Zorclub42 se demandent *«Qui habilite qui ? Qui surveille la piste d'audit ?»*.

À ces interrogations, le ministère de l'intérieur a répondu :

1) En ce qui concerne l'accès du citoyen aux données contenues dans la puce et dans la base :

– l'accès au contenu de la puce se fera par le biais d'un accès direct, probablement à partir de bornes installées dans les lieux de délivrance des titres. De plus, le titulaire de la carte, en saisissant son code PIN, pourra donner accès aux administrations qui en auraient besoin dans le cadre des téléprocédures administratives.

En revanche, l'accès du citoyen au contenu de la base se fera par le biais d'un accès indirect, ce mode d'accès étant celui réservé aux fichiers gérés habituellement par le ministère de l'intérieur. Un accès direct ne peut être envisageable car, outre les données d'état civil et biométriques, la base contiendra le *«journal»* des consultations de la base réalisées par les agents habilités.

2) En ce qui concerne l'accès des agents aux données contenues dans la puce et dans la base :

L'accès aux données de la puce sera *«hiérarchisé»* selon le caractère confidentiel des informations contenues. Pour les empreintes digitales, seules les forces de police pourront les lire, à des fins de contrôle d'identité et ce dans le cadre de l'article 78-2 du code de procédure pénale.

L'accès à la base se fera de la façon suivante :

– le système sera géré par des agents habilités (agents chargés de la délivrance des titres, mairies et préfectures). Ces agents se contenteront de rentrer les données pour la délivrance des titres. Ils n'auront un accès à la base qu'en mode écriture, et limité aux données alphanumériques (nom, prénoms etc...) et à la lecture de la photo. Ils ne pourront ni consulter les empreintes digitales, ni lire les données personnelles d'un autre individu;



– seules la police et la gendarmerie auront accès à la base des données biométriques, dans le cadre que fixera le projet de loi (possibilité réservée aux seuls officiers de police judiciaire sous le contrôle du parquet, à des fins de vérification d'identité et dans les conditions prévues par l'article 78-3 du code de procédure pénale). Ces consultations seront tracées (elles feront l'objet d'un «*journal*» qui retracera les interrogations faites).

#### **Sur le risque de lecture, à distance et à l'insu du porteur, des données inscrites sur la carte**

Le dossier de présentation du programme INES précise que «*la consultation des données d'identité (photo et empreintes) par les autorités habilitées se fera sans contact*».

La notion de «*sans contact*» a fait l'objet de nombreuses craintes. Certains se sont opposés à son principe même qui conduit à un contrôle de masse quantitatif et automatique des individus, assimilés à «*du bétail*». Plus globalement, la perception générale est qu'il y a un risque, qu'à l'insu du porteur, la puce sans contact puisse être lue à distance. «*L'identification*» sans contact «*aggravera encore le flicage, puisqu'on pourra être contrôlé sans même qu'on le sache*» dit, par exemple, Fanchick. L'association IRIS<sup>284</sup> estime à cet égard que la lecture de la puce ne doit pas se faire sans contact.

Lors des débats le ministère a, par la suite, justifié ce choix en expliquant que le «*sans contact*» de la carte se conjuguerait avec les applications passeport (qui comportera également une puce sans contact insérée dans le livret), serait plus facile à utiliser (lors de contrôles de masse dans des aéroports par exemple) et s'userait moins.

#### **Sur la création d'un organisme de contrôle ad hoc**

Certains ont noté l'absence d'un véritable contre-pouvoir face au projet de CNIE et dénoncent la difficulté pour la CNIL de remplir ce rôle.

Zorglub<sup>42</sup> estime que «*la fiabilité du système doit absolument être garantie et surtout certifiée par un organisme indépendant*». Banjo trouve qu'il pourrait être opportun de «*créer un nouvel organisme indépendant chargé de réguler les transferts de données qui seront inscrites sur la carte*». Vincemdk et Freez proposent également «*la création d'une autorité administrative indépendante*» qui aurait «*pour mission la surveillance des données et des personnes qui y ont accès et de toutes les opérations possibles à partir de ces données [...] Ses membres devront jouir des mêmes protections que les magistrats qui pourront garantir un peu contre les pressions [...] Des organisations/ associations de citoyens devront pouvoir être présentes.*»

#### **Sur l'utilisation du Répertoire national d'identification des personnes physiques (RNIPP)**

Le projet prévoit que l'état civil soit dématérialisé pour que les actes puissent être transmis directement et de manière sécurisée entre mairies de naissance et mairies

---

284. Débat de Lille, 27 avril 2005.

de délivrance du titre. Pour ce faire, il serait prévu de permettre une consultation du Répertoire national d'identification des personnes physiques (RNIPP), tenu par l'INSEE, afin de valider si les données d'état civil communiquées par la personne qui souhaite la délivrance d'un titre correspondent à celles enregistrées dans le RNIPP au niveau de la filiation.

Pour certains, utiliser le RNIPP semble logique dès lors que l'on utilise un circuit et une base existante et fiable. Pour d'autres, au contraire, cette solution a un impact symbolique fort et est porteur d'un certain nombre de craintes. C'est ce qu'ont exprimé des syndicats de l'Insee par le biais d'une lettre ouverte à leur directeur général<sup>285</sup>. Dans cette lettre, ils estiment que la participation de l'Insee à la constitution d'un fichier national d'identité n'a pas de précédent : il y a actuellement une séparation entre les fonctions statistiques et les fonctions de gestion policière de la population et l'usage du RNIPP comme une des sources pour constituer ou vérifier un fichier de police serait une rupture majeure (utilisation d'informations sur la filiation, problème de confiance...).

Plus généralement et d'un point de vue strictement historique, Pierre Piazza<sup>286</sup> rappelle que ce n'est pas la première fois que l'utilisation du RNIPP est envisagée : notamment entre « 1946 et 1951, des rencontres sont organisées entre des fonctionnaires du ministère de l'intérieur et des représentants de l'INSEE. Il est alors prévu de recourir au Répertoire général d'identification constitué sous l'Occupation pour identifier chaque demandeur de la nouvelle » carte nationale d'identité dont la création est envisagée. Cependant, ce sont, principalement, des « divergences de points de vue » sur la question de l'identification des Français musulmans d'Algérie qui aboutissent à l'abandon de ce projet.

## Sur la biométrie

La mise en place d'identifiants biométriques suscite de nombreux débats.

### **Des débats sur cette forme particulière d'identification par le biais d'une partie du corps**

La biométrie<sup>287</sup> est apparue comme étant un sujet sensible qui fait débat car il touche directement au rapport au corps. Gérard Dubey<sup>288</sup>, sociologue à l'Institut National des Télécoms, estime ainsi, à partir d'enquêtes et entretiens menés sur ce thème, que face à l'introduction de la biométrie, certains semblent vouloir dire : « C'est une part

---

285. Lettre ouverte du 17 mai 2005 des syndicats nationaux CGT, CFDT, SUD, CGT-FO, CGC, CFTC de l'Insee au Directeur général de l'Insee intitulée « *L'Insee n'a pas vocation à être une annexe du ministère de l'intérieur!* », message sur internet du 1<sup>er</sup> juin 2005.

286. Message sur internet de Pierre Piazza, 13 avril 2005.

287. Analyse des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable. La biométrie repose sur le principe de la reconnaissance de caractéristiques physiques (empreintes digitales, l'iris de l'œil, forme de la main, la voix etc.) qui sont censées offrir une preuve irréfutable de l'identité d'une personne puisqu'elles constituent des caractéristiques biologiques uniques qui distinguent une personne d'une autre et ne peuvent être associées qu'à une seule personne.

288. Contribution de Gérard Dubey, message sur internet du 22 mars 2005.

*de moi que je laisse, donc je ne veux pas que mon intimité soit comme ça perdue sans que je sache ce qui va en être fait* ». Il estime que ceci révèle autre chose que la crainte d'être fiché ou enregistré sur une base de donnée: *«la question est plutôt: que devient l'individualité, ce qu'il y a de singulier en chacun, une fois numérisé?»*

Ce questionnement fait écho au fait que dans les débats beaucoup ont estimé que, même si l'on a toujours eu recours à la biométrie, la grande différence réside actuellement dans l'introduction de l'informatique qui multiplie la puissance de cette technique d'identification. Comme l'exprime Yannick Comenge<sup>289</sup>, docteur en Biochimie, cette *«rencontre entre biométrie et informatique est perturbante* ». De plus, l'utilisation de la biométrie est assimilée par certains à une méthode de police principalement utilisée pour *«ficher»* les délinquants: l'internaute Eupalinos explique ainsi sa méfiance vis-à-vis de cette technologie *«parce que la biométrie est un processus policier et que sa généralisation serait la consécration d'un État policier»*.

À ce titre, le projet INES de numériser les empreintes digitales et la photographie suscite de nombreux débats.

Certains ont estimé, à l'instar de Bernard Didier<sup>290</sup>, Directeur du développement des affaires à la division sécurité de Sagem, que parce qu'elle permet de mesurer le vivant et d'identifier les individus de façon performante, seule la biométrie permet de s'assurer que lors de la délivrance d'un titre celui-ci est délivré à la bonne personne. C'est d'ailleurs ce que confirment des internautes comme Michel Lo qui estime qu'il y a *«des aspects positifs»* dans la biométrie comme *«le renforcement de la preuve de l'identité qu'on ne peut rejeter»* ou encore Richard qui se prononce en faveur des empreintes digitales estimant que cela permettra de résoudre davantage de crimes et délits. De plus, pour Emmanuel-Alain Cabanis<sup>291</sup>, professeur de médecine et président de la Société de Biométrie Humaine, la rencontre entre la biométrie et l'électronique permet paradoxalement de mieux protéger l'identité de l'individu. C'est ce qu'il appelle le *«paradoxe de la liberté»*: le fait de pouvoir être connu, identifié avec certitude permet à un être humain de garantir son identité et ainsi d'être libre car démontrer son unicité, c'est, pour lui, affirmer sa différence vis-à-vis des autres.

L'introduction de la biométrie a fait l'objet d'enquêtes sociologiques. Les sociologues Gérard Dubey<sup>292</sup> et Xavier Guchet<sup>293</sup> estiment ainsi, d'après leurs travaux portant sur la biométrie aux Aéroports de Paris et dans des cantines scolaires, que l'introduction de cette technique s'accompagne d'*«une forme d'atonie sociale, une quasi-absence de réaction de la part des usagers vis-à-vis de la mise en place de ces dispositifs»*, voire une *«quasi-acceptation»*.

Gérard Dubey explique ceci par le fait qu'il est *«très rare que les usagers sachent comment fonctionnent ces dispositifs et tout aussi rare qu'ils cherchent à le savoir*.

---

289. Message sur internet du 19 mars 2005.

290. Contribution de Bernard Didier, débat de Paris, 11 avril 2005.

291. Contribution d'Emmanuel-Alain Cabanis, débat de Rennes, 11 mai 2005.

292. Contribution sur internet de Gérard Dubey, 30 mars 2005.

293. Contributions sur internet de Xavier Guchet, 30 mars 2005 et dans le débat de Marseille du 25 mai 2005.

*En fait il n'y a quasiment pas de discours sur ces techniques, de distance critique. Certains évoquent parfois le spectre de Big Brother, d'une traçabilité ou d'un flicage, mais pour la majorité, ces techniques n'évoquent rien de particulier. On évoque parfois leur côté pratique, plus sûr, dans un monde qui est ressenti comme l'étant de moins en moins». Cette «acceptation sociale ne doit pas pour autant dissimuler les contradictions et les tensions qu'elle engendre». Il note enfin que l'introduction de la biométrie n'entraîne pas de «profonds bouleversements», de changements radicaux et immédiats dans la façon de se représenter l'individu mais ce serait plutôt par une «analyse minutieuse et patiente des petites peurs, des inquiétudes exprimées par les usagers sur le mode imaginaire, que l'on peut s'approcher des dangers propres à ces dispositifs, de leurs véritables enjeux sociétaux». Or, il estime que ceci ne peut se quantifier facilement et mériterait «d'être approfondi et confirmé par d'autres études».*

Xavier Guchet<sup>294</sup> estime que cette introduction relativement indolore de la biométrie auprès des individus ne signifie pas pour autant que la requalification biométrique de l'identité est sans problème: il reconnaît qu'il est impossible, en l'état, de savoir si la biométrie sera bien acceptée à l'échelle d'une population et recommande à cet effet une analyse précise des usages. Il précise également que la biométrie n'est pas un outil neutre au service de problématiques purement techniques, elle est aussi un instrument de pouvoir car elle s'accompagne de rapports de force et de changements qui modifient la nature même du pouvoir qui s'exerce sur les gens. Ce thème est apparu fortement dans le contexte scolaire où la biométrie inaugure un nouveau type de pouvoir et de contrôle social qui ne passe plus forcément par les surveillants traditionnels mais s'appuie sur d'autres relais.

Le rapport de mars 2005 de la *London School of Economics & Political Science*<sup>295</sup> ainsi que l'étude de la Commission européenne sur les incidences des techniques biométriques d'avril 2005<sup>296</sup> confirment cette impression. L'étude de la Commission insiste d'ailleurs sur la nécessité de veiller à faire accepter les applications biométriques par les citoyens, en leur expliquant clairement la finalité et les limites de ces applications.

### **Des débats sur la fiabilité de la biométrie**

Quelle fiabilité pour la biométrie? Pourquoi utiliser l'empreinte digitale plutôt que l'iris de l'œil alors que cette dernière technique semble plus fiable pour certains? Les questions des internautes s'interrogeant sur les types de biométrie utilisés et leur fiabilité ont été nombreuses. Pingouin se demande ainsi si l'utilisation de l'iris de l'œil ne serait pas plus sûre que le recours à une empreinte digitale. 10cd29 rapporte les difficultés pratiques qui peuvent surgir lors de tentatives de lecture d'empreintes digitales sur des personnes dont le doigt a été abîmé (exemple donné: les mains en

---

294. Contribution de Xavier Guchet, débat de Marseille, 25 mai 2005.

295. *The Identity Project. An assessment of the UK Identity Cards Bill & its implications*, London School of Economics & Political Science, Londres, Mars 2005.

296. *Biométrie aux frontières: évaluation des impacts sur la société*, étude réalisée par le Centre commun de recherche de la Commission européenne, à la demande de la Commission des libertés et des droits des citoyens, de la justice et des affaires intérieures du Parlement européen, avril 2005.

contact prolongé avec une lessive à base de soude...). Pshunter estime que «*le vrai problème de la biométrie est sa relative non-fiabilité (il est assez facile de tromper un lecteur d'empreintes digitales) mais surtout sa non-révocabilité*». Il rejoint à cet égard Ielou qui relate les propos écrits en 2003 par l'un des responsables actuels de la Direction centrale de la sécurité des systèmes d'information (DCSSI) pour qui la biométrie «*a au moins deux limites: ce n'est pas une méthode confidentielle et c'est une méthode rigide. L'authentification par empreintes ne remplacera pas un login/mot de passe car une empreinte n'est pas un secret: c'est exploitable: on laisse 20 traces de doigt/jour exploitables [...] De plus il existe de nombreuses techniques permettant de passer outre les mécanismes de sécurité reposant en tout ou partie sur la biométrie.*» Certains, lors du débat de Rennes, ont d'ailleurs confirmé ces propos et évoqué l'exemple d'un chercheur japonais qui a fabriqué avec de la gélatine de vraies-fausse empreintes digitales qui ont leurré 11 des 15 systèmes biométriques testés.

Sur ce point, le ministère de l'intérieur a assuré qu'il existe des moyens de se prémunir de ce type de manœuvre par l'acquisition de matériels suffisamment pointus et fiables. En outre, toute utilisation des titres lors des contrôles aux frontières, ou des contrôles d'identité, se fait et demeurera sous le contrôle d'un agent. Le ministère met en avant le facteur humain qui est, à ses yeux, une sécurité supplémentaire contre l'utilisation de fausses empreintes.

### **Des débats sur l'opportunité des biométries choisies**

Certains, comme Emmanuel-Alain Cabanis, soulignent que l'on peut éventuellement recueillir des informations médicales à l'occasion d'une identification par l'iris de l'œil (l'iris peut changer de couleur avec l'absorption de certains médicaments); cependant, reprenant des chiffres avancés dans le rapport du député Cabal<sup>297</sup>, il estime que les empreintes sont moins fiables que l'iris.

De l'autre, Bernard Didier<sup>298</sup> a précisé que les empreintes bénéficient de plus d'un siècle d'expérience par les pouvoirs publics français en matière de lutte contre la criminalité. Il précise qu'il s'agit d'une technique fiable, maîtrisée et ayant acquis une certaine maturité industrielle. En revanche, il estime que l'iris de l'œil fait l'objet d'une technologie plus jeune sur laquelle on ne dispose pas assez de recul. Il a également précisé<sup>299</sup> que la technologie de l'iris «*offre un potentiel plus élevé de détection des fraudeurs (FAR), mais les rejets à tort sont plus importants (...)* Les temps de transac-

---

297. Christian Cabal est intervenu lors du débat de Lille. Député, il a présenté en juin 2003 un rapport sur la biométrie au sein de l'Office parlementaire d'évaluation des choix scientifiques et technologiques. Ce rapport parlementaire précisait que le FAR («*False Acceptation Rate*», c'est-à-dire le taux qui détermine la probabilité pour un système de «reconnaître» une personne qui normalement n'aurait pas dû être reconnue) est plus fort pour les empreintes digitales (0,008 %) que pour l'iris (0,0001 %). De même, le FRR («*False Rejection Rate*», le taux qui détermine la probabilité pour un système donné de ne pas «reconnaître» une personne qui normalement aurait dû être reconnue) est plus fort pour les empreintes digitales (2,5 %) que pour l'iris (0,25 %). La reconnaissance faciale est la moins fiable (respectivement 0,45 % pour le FAR et 17 % pour le FRR).

298. Contribution de Bernard Didier, débat de Paris, 11 avril 2005.

299. Message sur internet de Bernard Didier, 31 mai 2005.

tion sont de même très longs car il est procédé à plusieurs tentatives de reconnaissance en cas de rejet.»

### **Des débats sur le marché de la biométrie et le coût de la biométrie associée à la carte à puce**

Un certain nombre de personnes ont évoqué des aspects de politique industrielle nationale qui expliqueraient, plutôt que les performances respectives de chaque biométrie, les choix retenus. Par exemple, Yves Bismuth<sup>300</sup> a estimé que le choix d'utiliser les empreintes digitales comme élément de biométrie a également été fait pour des raisons économiques parce qu'une entreprise française, Sagem, a une position dominante dans ce domaine et que d'autres choix technologiques (iris de l'œil) dépendent de brevets américains. À cela Bernard Didier a souhaité répondre<sup>301</sup> que Sagem «ne réduit pas sa position de leader à la seule technologie de l'empreinte digitale. Elle maîtrise depuis plus de deux ans les deux autres technologies de référence que sont la reconnaissance du visage et de l'iris. Cette maîtrise s'est traduite par l'obtention des deux plus importantes références mondiales en la matière».

Pierre Piazza rappelle<sup>302</sup> que certains, comme le député européen danois Ole Sorensen, font valoir que les coûts financiers liés la généralisation des dispositifs biométriques risquent d'être exorbitants au regard des bénéfices que les citoyens pourraient en retirer. Meryem Marzouki estime que le marché de la biométrie et de la carte à puce présente de très forts potentiels économiques et que, de l'avis de tous les acteurs industriels, il est encore seulement en émergence.

Bernard Didier a précisé que le surcoût d'une carte lié à la biométrie représente environ 20 % du coût total. Ceci reviendrait à une estimation de 2 à 4 euros par personne. Hubert Vigneron, président de la section «Carte à puce» du Gixel (Groupement des industries électroniques qui rassemble Axalto, Gemplus, Sagem, Thalès) et Directeur Marketing Stratégique chez Axalto<sup>303</sup> a, quant à lui, annoncé que le marché de la carte à puce dans ses applications d'administration électronique est prometteur puisqu'il est estimé à 60 millions de cartes au niveau mondial en 2005 et plus de 100 millions en 2006 (selon IDC). Cela ne représente toutefois qu'une faible part des cartes à microprocesseur dans le monde (1,7 milliard en 2005 dont 1,2 en téléphonie mobile). Aujourd'hui l'industrie française de la carte fournit 60 à 70 % du marché mondial. À cet effet, Hubert Vigneron estime que l'intérêt des industriels français est de permettre l'émergence de standards internationaux tout en capitalisant sur une implémentation nationale de référence; c'est pourquoi le Gixel travaille également avec les Allemands.

---

300. Contribution d'Yves Bismuth, débat de Lyon, 31 mars 2005.

301. Message sur internet de Bernard Didier, 31 mai 2005.

302. Contribution sur internet de Pierre Piazza, 7 mars 2005.

303. Contribution de Hubert Vigneron, débat de Lille, 27 avril 2005.

## Sur la sécurité du système

En l'état actuel des technologies et de la sécurisation des systèmes, les internautes ont majoritairement noté qu'il sera très difficile de pouvoir assurer une sécurité à 100 % de la carte. D'autres se demandent comment il sera possible de faire évoluer le système pour que le niveau de sécurité soit constamment adapté aux nouveaux risques. De façon générale, beaucoup rejoignent l'avis de Sylvain Gombault, enseignant à l'École nationale supérieure des télécommunications de Bretagne et membre du projet SERES (Sécurité des réseaux et des applications réparties) et estiment que *«le fait d'utiliser internet comme réseau de transport n'est jamais neutre pour la sécurité d'un système. Il expose les postes clients aux dangers d'internet comme les vers et les virus, et il devient difficile, voire impossible, de garantir un niveau de sécurité de chacun des postes compatible avec la manipulation des données à caractère personnel contenues dans la carte INES<sup>304</sup>»*.

### Sur les certificats et la signature électronique

Certains font a priori confiance à la sécurité d'un système fondé sur de la signature électronique. Ainsi, pour AAA *«INES présente des garanties suffisantes. Je peux confirmer que du fait de la longueur des clés proposées la carte INES est actuellement inviolable. Il faudra qu'elle le reste et il faut donc utiliser des clés plus longues que le strict nécessaire.»*

En revanche, d'autres, comme Fabien Petitcolas, estiment qu'en ce qui concerne la signature électronique, *«l'authentification se fait jusqu'au niveau de l'ordinateur utilisé pour la signature. Le lien entre cet ordinateur et (le contenu du message) reste incertain...»* Tatoute précise qu'il suffirait de *«diffuser un ver»* sur le réseau pour que le système soit attaqué. Beretta constate que même si le niveau de protection est élevé et implique des moyens financiers très importants pour tenter de le dépasser, il ne s'agit pas d'un obstacle insurmontable pour certains *«États voyous ou certaines multinationales»*.

Cela reflète un constat général: l'échange d'information «sensible» sur un réseau ouvert comme internet est potentiellement dangereux car le risque d'attaques et de failles de sécurité est réel.

### Sur l'emploi de la carte à puce

Concernant la lecture de la carte à puce par les ordinateurs familiaux, phil13 note *«le manque ÉNORME de sécurité sur les ordinateurs familiaux (et même ordi de sociétés) pleins de petits spy très curieux, sans parler des 300 nouveaux virus découverts quotidiennement par les sociétés spécialisées)»*.

À ces réserves, il a été répondu que les cartes à puce sont beaucoup plus sécurisées que tout autre support. Olivier Chavrier, Directeur de la division identité et sécurité de Gemplus a rappelé<sup>305</sup> qu'un système sécurisé à 100 % n'existe pas. Pour autant, il

---

304. Message sur internet de Sylvain Gombault, 7 juin 2005.

305. Contribution d'Olivier Chavrier, débat de Marseille, 25 mai 2005.

estime que l'introduction des cartes à puce a renforcé la sécurité. En effet, introduites dans les années 1990 pour le paiement, elles ont permis une diminution de 80 % des fraudes au paiement bancaire alors que, dans le même temps, les volumes de paiement augmentaient de 120 %. De plus, la carte associée à un code PIN permet une sécurité accrue dans l'accès aux données. Dans ce cadre, une carte d'identité électronique fondée sur une carte à puce et de la signature électronique permettra une authentification sécurisée sur le net. Enfin, si l'on veut davantage de garanties sur la sécurité d'un système, il convient que celui-ci fasse l'objet d'une évaluation par des laboratoires indépendants puis de certification par un autre organisme.

### **Des propositions pour améliorer la sécurité du système**

En ce qui concerne la consultation des données par les agents habilités, holyvier2 propose que le « matériel spéciaux » soit « équipé d'un système comparable à une sorte de boîte noire qui garderait la trace de l'heure, de la date des identifiants des CNIE consultées et des identifiants des personnes habilitées ayant procédé à l'identification ». Vis-à-vis de cette proposition, le ministère de l'intérieur a annoncé que « les spécifications de ce matériel ne sont pas arrêtées à ce jour ; votre suggestion est intéressante et devra être étudiée (d'où l'intérêt de ce débat : on peut encore prendre en compte les bonnes idées) ».

Pour l'internaute toto37 : « il pourrait être envisagé de former un groupe d'experts, reconnus et mandatés par les différentes parties prenantes pour valider cette étude EBIOS et informer leurs mandants des conclusions à retenir [...] Ces experts valideront également les cibles de sécurité (fonctions et niveau d'assurance) des éléments devant subir une évaluation. » À cet égard, Beretta propose également que soit menée une « étude indépendante de la CNIE par des chercheurs ».

Enfin, faisant écho aux débats intervenus sur le thème de la vie privée (possibilité de lecture à l'insu du porteur), certains ont précisé qu'il existe des moyens techniques d'empêcher une lecture sans contact des données. Abadie note ainsi que « tout système de lecture à distance par induction peut être neutralisé simplement en enfermant la carte à lire dans une enveloppe métallique ». Beretta, comme bien d'autres, confirme ce point : « l'utilisation d'un étui métallique peut être jugé un brin paranoïaque mais c'est la seule protection absolument fiable qui rend la fonction de lecture de dialogue à distance inopérante [...]. C'est un peu extrême comme solution mais c'est une double protection, dans un étui métallique qui fera office de cage de Faraday, la carte ne peut plus être alimentée en énergie (pas d'induction possible et la carte n'est pas autonome). »

### **La faille de sécurité au niveau de l'état civil**

Le projet INES prévoit que la procédure de délivrance des titres soit sécurisée, en amont, par la mise en œuvre d'un processus d'échange direct des données d'état civil entre services source (la mairie de naissance) et services chargés de la délivrance des titres. Les citoyens n'auraient donc plus à prendre contact avec leur mairie de naissance pour obtenir un extrait de naissance mais l'échange d'information se ferait directement entre les mairies concernées. Pour ce faire, un projet, conduit par le ministère de la justice, prévoit de dématérialiser les actes de l'état civil afin de mettre



en œuvre un système d'échange d'informations entre services. Le déploiement des deux projets doit contribuer à conférer une sécurisation supplémentaire aux documents d'identité délivrés.

Cependant, certains ont noté, notamment lors des débats de Lyon et de Paris, que le projet de carte nationale d'identité électronique ne semble pas s'articuler avec celui de dématérialisation de l'état civil; qu'il est donc un peu illusoire de renforcer la sécurisation des titres si, dans le même temps, les données d'état civil sur lesquels ils se fondent, ne sont pas entièrement fiables; qu'à ce titre, il risque d'y avoir des failles de sécurité.

## Sur les usages

### **Un intérêt très limité pour l'aspect « portfolio personnel »**

L'aspect portfolio personnel consiste à permettre aux titulaires, s'ils le souhaitent, de stocker, à titre personnel, des informations complémentaires dans la carte. Ceci pourrait permettre, par exemple, de remplir plus facilement des formulaires à partir d'informations que l'on porterait toujours sur soi (ex: permis de conduire, numéro fiscal, etc.). Il ressort du débat que cette fonctionnalité de la carte n'intéresse pas les intervenants même si son aspect « *espace mémoire* » serait une « *avancée intéressante* » pour l'AMGVF<sup>306</sup>.

### **Des confusions et des incompréhensions**

Un certain nombre de confusions ou d'incompréhensions ont pu être notées. Ainsi, certains ont eu peur que toutes les actions de la vie courantes apparaissent (« *liste des habitudes de consommation* ») ou que la CNIE ne soit une carte de paiement. Beaucoup ont pensé également que la CNIE accueillerait les données de santé, voire serait fusionnée avec la carte Vitale. Sur ce point, le ministère de l'intérieur a régulièrement répondu que les données de santé et à caractère sanitaire et social ne seront pas dans la CNIE, qu'une telle disposition serait, en tout état de cause, inconstitutionnelle.

### **Peu d'intérêt voire des interrogations quant aux fonctionnalités internet de la carte (certificat et signature électronique)**

Le ministère de l'intérieur, dans son dossier de présentation du projet INES, précise que la CNIE pourra donner accès à des téléprocédures administratives et permettra de s'identifier de façon certifiée sur internet auprès de sites marchands<sup>307</sup>.

Certains ont été intéressés par les nouveaux services qu'offre la carte. L'internaute RC note que « *la CNIE offre beaucoup d'avantages: elle remplace les certificats élec-*

---

306. Message sur internet de l'Association des maires de grandes villes de France, 18 mai 2005.

307. Dossier de présentation du ministère de l'intérieur du 1<sup>er</sup> mars 2005: le bloc « *identification certifiée* » permettrait d'accéder à des téléprocédures publiques ou privées via un code PIN et le bloc « *signature électronique* » de signer électroniquement des documents authentiques, soit à l'intention d'une e-administration, soit pour toute transaction électronique privée.

troniques qui sont nécessaires à la réalisation des formalités administratives comme TELETV (et qui coûtent 50 euros par an), elle pourrait aussi servir à s'identifier sur Internet pour la réalisation d'opérations sur les comptes bancaires (ce qui serait beaucoup plus sûr que les actuels codes secrets)». D'autres ont estimé que la CNIE permettrait un gain de temps pour les formalités administratives courantes, et qu'elle s'inscrit dans le cadre de la modernisation de l'administration : « cette carte recèle un énorme potentiel pour faciliter la vie des citoyens et diminuer les coûts administratifs » (Aymeric77), « cette carte permettra aux utilisateurs du service public (c'est-à-dire nous) de faciliter les démarches administratives » (vicoleboss).

Cependant, de façon générale, l'intérêt pour les téléprocédures administratives est limité. De plus, les internautes Franchick ou Necronick estiment que certains actes citoyens, comme la possibilité de voter électroniquement par le biais de la CNIE, ne doivent pas être rendus possibles du fait des risques : risques d'attaques contre le système, atteinte à la confidentialité du vote, usurpation d'identité...

De plus, certains ont fait part de leurs inquiétudes sur le fait que la carte permette d'authentifier un accès, voire de signer électroniquement, auprès de sites marchands. Ceci créerait une confusion entre la fonction régaliennne (attribution de l'identité) et les applications privées, commerciales ou non, associées à ce nouvel outil d'identification des personnes. Cyril Rojinsky<sup>308</sup>, avocat, estime ainsi qu'il convient d'insister sur le fait qu'un « titre national d'identité, électronique ou non [...] matérialise, signe pour ainsi dire l'identité strictement légale de chacun. Sous prétexte de simplification, de réduction du nombre de cartes dont nous pouvons disposer, le projet d'une carte unique intégrant des applications commerciales viendrait pervertir le rôle même de l'État à cet égard ». Pour d'autres, comme l'association IRIS<sup>309</sup>, la CNIE ne doit pouvoir faire l'objet d'aucune autre utilisation. Les certificats de signature électronique et autres utilisations individuelles doivent être complètement dissociés de la carte, de son support et de sa gestion.

D'autres, comme l'avocat Thierry Piette-Coudol<sup>310</sup>, se demandent : « Quel besoin d'une identification forte pour les téléprocédures ? D'autant que l'anonymat de l'agent public correspondant pourrait, lui, être respecté, « si des motifs intéressant la sécurité publique ou la sécurité des personnes le justifient » (art. 4 de la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations). » Il se demande également : « Pourquoi une « identification certifiée » [...] pour une transaction électronique privée ? En somme, si le commerce repose depuis l'antiquité sur la confiance, le commerce électronique devrait-il reposer sur l'authentification forte et les mesures biométriques ? »

Daniel Kaplan, délégué général de la Fondation internet nouvelle génération (FING)<sup>311</sup> estime également que le développement d'une carte « signeuse » est potentiellement dangereux. En effet, parce que la CNIE bénéficiera d'un statut officiel et qu'elle propo-

---

308. Contribution sur internet de Cyril Rojinsky, 7 mars 2005.

309. Contribution de Meryem Marzouki, débat de Lille, 27 avril 2005.

310. Contribution sur internet de Thierry Piette-Coudol, 7 mars 2005.

311. Contribution de Daniel Kaplan, débat de Marseille, 25 mai 2005.

sera un dispositif très fort d'authentification, elle risque d'inciter un grand nombre d'acteurs à se reposer sur elle pour leurs relations avec des tiers (clients, fournisseurs...) même si ce niveau d'authentification n'est pas nécessaire.

D'une manière générale, la plupart des intervenants ont souhaité une variabilité de l'authentification en fonction de l'usage.

### **Quelques questions sur le contexte européen**

Le contexte européen a fait l'objet de peu de questions. Les questions ont principalement porté sur l'interopérabilité (la carte sera-t-elle «*lisible*» à l'étranger?) et l'articulation entre le projet français et ceux de nos voisins européens. À cet effet, Michel Elie<sup>312</sup> souhaite une généralisation la carte «*à l'espace européen*» et que la carte devienne «*un document d'identité unique applicable au moins à toute personne résidant en Europe communautaire*». Dans cet esprit, certains se sont demandé quel est l'intérêt de développer une carte nationale dans un contexte européen et s'il ne fallait pas mieux concentrer ses efforts sur un projet de carte d'identité électronique européenne. À leurs yeux, le projet devrait avoir une portée européenne car désormais les décisions sont prises au niveau européen (passeport biométrique et Règlement de décembre 2004, titres de séjours et visas biométriques). Les problématiques posées se retrouvant dans les autres États membres, l'internaute Pierre Rostaing estime que le débat ne devrait pas être uniquement national mais porté à un niveau européen («*pourquoi à l'heure de l'Europe, penser franco-français, et ne pas penser ensemble ces problèmes... inévitablement communs?*»).

Le ministère de l'intérieur a précisé que la France et l'Allemagne coopèrent dans le domaine de la carte d'identité électronique. Cette coopération ne porte que sur les normes et les standards. Il s'agit donc avant tout d'une coopération industrielle.

## **Sur les mesures d'accompagnement**

### **Le coût**

Pour de nombreux intervenants, le projet de CNIE va coûter cher. Ils se demandent concrètement combien va coûter le projet dans son ensemble; l'annonce faite par le Ministre de dépenser 205 millions d'euros par an en a choqué certains «*en ces périodes de restrictions budgétaires*»; mais ils se demandent aussi qui va payer la carte: la collectivité ou l'individu lui-même.

À cet égard, les contributions rappellent que l'actuel CNI papier est gratuite, la rendre payante serait mal perçue, les nouveaux services proposés ne le justifiant pas. D'une façon générale, le souhait se porte sur la gratuité de la carte (important en termes d'acceptation et d'insertion surtout pour les catégories défavorisées). Si elle devait être payante, l'internaute Julesandolfi suggère qu'elle ne le soit que «*pour les personnes imposables sur les revenus*». Eupalinos écrit que «*même si le citoyen n'aura pas à payer directement la CNIE, il en supportera les frais indirectement via le*

---

312. Message sur internet de Michel Elie, 8 avril 2005.

*budget de l'État et les impôts*». Simix évoque le coût du matériel entourant la CNIE (lecteur de carte à puce au domicile pour justifier de son identité sur internet, lecteur d'empreintes digitales ou rétinienne pour éviter les problèmes liés à la perte du lecteur de carte...) pour constater que la mise en place d'une telle carte posera des problèmes de financement. Lors du débat de Bordeaux, Patrick Nouvel<sup>313</sup>, Directeur commercial domaine identitaire de Thalès, a précisé que si la carte proposait des services associés, le secteur privé y trouverait une source de revenus et, de ce fait, pourrait prendre en charge une partie des coûts.

D'autres intervenants seraient favorables au paiement de la carte en cas de renouvellement de papier ou de perte. Christian Cabal<sup>314</sup> a d'ailleurs estimé, en tant que parlementaire, qu'il serait intéressant de songer à ne rendre la carte payante que dans ces deux situations.

À l'idée de savoir combien coûtera au final une CNIE pour l'utilisateur, Hubert Vigneron précise<sup>315</sup> que le prix d'une carte dépend de nombreux facteurs et que les prix annoncés englobent souvent plusieurs éléments (le prix de fabrication de la carte, le coût de son émission, et le coût du système – ou son amortissement). Dans les projets traités par Axalto, la partie carte représentait de 30 à 50 % du total du projet. Il a précisé que les cartes actuellement développées coûtent entre 10 € en Belgique (proche du prix de revient car le prix de revient d'une carte est toujours à un chiffre) et 35 £ au Royaume-Uni en passant par des coûts moyens (Italie: 25 à 30€). Hubert Vigneron a enfin précisé que la carte d'identité électronique en Finlande coûte 40€ mais que, du fait de son caractère non obligatoire, elle ne se vend pas et se développe peu.

De façon générale, le ministère a souhaité préciser que, depuis que la carte est gratuite, le taux de perte a été multiplié par 10 et atteint 10 % de la production. La rendre payante pour l'utilisateur permettrait de responsabiliser ce dernier. De plus, le ministère a rappelé que la délivrance des cartes d'identité et des passeports coûte actuellement 180 millions d'euros par an. Le ministère a souhaité rapporter ce chiffre à celui annoncé par Dominique de Villepin le 12 avril dernier: 205 millions d'euros. Le ministère estime que l'écart va progressivement diminuer et la carte coûter de moins en moins cher au regard des économies escomptées (diminution de la fraude, simplification et automatisation de certains actes, gains de temps...).

### **Le caractère obligatoire**

Ce point a fait débat: certains ont annoncé que si la carte n'est pas obligatoire elle ne sera jamais adoptée largement (cf. Finlande: carte de 40 euros pas obligatoire) et dès lors ne servira pas. À cet effet, il est intéressant de voir les résultats du sondage: à la question *«quelles opinions se rapprochent le plus de la vôtre? La future carte d'identité électronique devrait être obligatoire car cela garantit une réelle diminution des fraudes ou facultative comme c'est le cas actuellement de la carte d'identité?»*,

---

313. Contribution de Patrick Nouvel, débat de Bordeaux, 8 mars 2005.

314. Contribution de Christian Cabal, débat de Lille, 27 avril 2005.

315. Contribution d'Hubert Vigneron, débat de Lille 27 avril 2005.

69 % des sondés répondent que c'est « *une bonne chose car cela permettra de lutter plus efficacement contre les fraudes* ». 30 % estiment que « *c'est une mauvaise chose car cela constitue une atteinte à la liberté individuelle* ».

Il a été rappelé que le projet INES rend obligatoire la détention d'une CNIE mais conserve la liberté du mode de preuve<sup>316</sup>. Il a aussi été remarqué que, même si le fait de porter une CNIE en permanence sur soi ne pourra être imposé, on ne pourra plus se prévaloir de ne pas avoir une carte d'identité.

De plus, beaucoup craignent que la carte ne devienne à terme obligatoire dans les faits pour la plupart des échanges avec l'administration, voire avec le secteur privé. En effet, comme le précise Thierry Piette-Coudol<sup>317</sup>, avocat, « *la facilité de pouvoir utiliser le certificat embarqué dans la carte pourrait entraîner une utilisation systématique apportant ainsi aux relations électroniques un niveau d'authentification qui n'est pas nécessairement demandé par le Droit* ». Ce faisant, un tel niveau d'authentification risque, dans les faits, d'entraîner une forme de pression sociale. Cette préoccupation est très présente dans les débats. De même, Annie Blandin, maître de conférences à École Nationale Supérieure des Télécommunications de Bretagne<sup>318</sup>, rappelle que l'identification de haut niveau fournie par l'État risque d'être utilisée à tout propos sous la pression éventuelle de destinataires imposant le recours aux certificats de la CNIE. Ces craintes font logiquement écho à celles exprimées dans la partie 5. c selon lesquelles la carte pourrait devenir un standard quasi obligé pour tous les usages de la vie quotidienne.

D'une manière plus générale, la grande majorité des intervenants aux débats se sont opposés très clairement au caractère obligatoire de la carte. Ils estiment qu'il y a là non seulement un risque de fracture technologique (ceux qui ne savent pas se servir des usages) mais surtout une rupture avec la « tradition » républicaine française. En effet, comme le rappelle Pierre Piazza<sup>319</sup>, le principe du caractère facultatif de la carte a été affirmé sous la Troisième République, réaffirmé à la Libération et jamais remis en cause par les différents gouvernements successifs, jusqu'à nos jours.

Enfin, le ministère de l'intérieur a précisé que la carte sera obligatoire à partir de la majorité, soit à l'âge de 18 ans (pour rappel, la carte d'identité électronique sera obligatoire en Belgique à partir de 12 ans).

### **Le lieu et le mode de délivrance**

Le ministère de l'intérieur a annoncé lors des débats qu'en raison du coût, mais aussi pour des raisons de sécurité et de charge de travail pour les petites collectivités, il serait impossible d'équiper les 36 500 communes françaises. Le projet prévoit donc de concentrer l'émission et la délivrance de la nouvelle carte sur quelques centaines de mairies. Afin que les petites collectivités locales ne soient pas défavorisées, des

---

316. L'article 78-2 du Code de procédure pénale, qui dispose que l'on peut « *justifier, par tout moyen, de son identité* », s'appliquera toujours.

317. Contribution sur internet de Thierry Piette-Coudol, 1<sup>er</sup> mars 2005.

318. Contribution d'Annie Blandin, débat de Rennes, 11 mai 2005.

319. Message sur internet de Pierre Piazza du 13 avril 2005.

dispositifs de stations d'acquisition mobiles devraient être déployés; cela permettra également la délivrance de la carte pour les personnes ne pouvant se déplacer (personnes handicapées, personnes âgées, prisonniers...). Le ministère a précisé que l'État financera les appareils de transmission des actes d'état civil, mettra en place de l'internet sécurisé haut débit dans chaque lieu de délivrance et indemnisera les collectivités pour cette nouvelle tâche.

Sur ce point, les avis ont été partagés. Jean Péringuey<sup>320</sup>, en tant que président d'une communauté de communes où les mairies ont 400 habitants en moyenne a rappelé que les citoyens sont très attachés à une carte nationale d'identité électronique délivrée dans un service de proximité et il estime que la mise en place de la CNIE ne doit pas diminuer l'offre de services publics locaux. Pour beaucoup de maires ruraux, la délivrance d'une carte nationale d'identité est souvent le moyen d'entretenir des liens avec leurs administrés. À cet égard, de nombreuses réserves ont été exprimées sur le fait, qu'en milieu rural, la carte soit délivrée par le biais d'une borne itinérante (station d'acquisition) allant dans chaque mairie.

Alain Risson<sup>321</sup>, en tant que responsable du groupe de travail «Nouvelles technologies» de l'Association des maires de France, a exprimé ses craintes quant à l'apparition de «*supers mairies*» seules à même de pouvoir délivrer les cartes. Il se demande si le plus simple ne serait pas que le nombre de «*super-mairies*» soit «*ramené, pour des raisons purement financières, à quelques centaines, ces super-mairies pouvant être alors parfaitement suppléées par les sous-préfectures qui sont au nombre de quelques centaines aussi...*»<sup>322</sup>.

L'Association des maires des grandes villes de France<sup>323</sup> s'interroge finalement sur le rôle de la mairie dans la chaîne de traitement des CNIE et à l'étendue de ses responsabilités: «*Les mairies auront-elles la possibilité ou le devoir de demander des pièces justificatives supplémentaires en cas de dossiers litigieux; aura-t-elle le rôle que joue la préfecture actuellement? Le contentieux administratif ne risque-t-il de s'accroître pour les villes?*». L'AMGVF se demande également ce qu'il est prévu en termes organisationnels pour «*l'adaptation des locaux pour garantir la confidentialité des opérations, l'organisation de l'attente [...] la formation du personnel...*».

Un point plus ponctuel a été discuté: celui des photographies d'état-civil. Les nouvelles modalités de photographie (il est prévu que l'utilisateur n'amène plus de photos d'identité, celles-ci seront prises sur place par les agents équipés en matériel de photographie numérique) posent problème à l'Association pour la promotion de l'image<sup>324</sup>. Tout en proposant un système qui permettrait de numériser les photos remises par les usagers (photos réalisées par des professionnels), cette association estime que le système proposé dans le cadre d'INES est «*contraignant pour l'utilisateur*» («*absence de liberté de choix de leur photo d'identité et de choix du prestataire réali-*

---

320. Contribution de Jean Péringuey, débat de Bordeaux, 8 mars 2005.

321. Contribution d'Alain Risson, débat de Lyon, 31 mars 2005.

322. Message sur internet d'Alain Risson, du 18 avril 2005.

323. Message sur internet de l'Association des maires de grandes villes de France, 18 mai 2005.

324. Message sur internet de l'Association pour la promotion de l'image, 15 mars 2005.

sant leur photo d'identité»), «contraignant pour l'administration» («La prise de photo d'identité est une activité professionnelle à part entière, qui suppose une expérience et une formation spécifiques») et «lourd et complexe» («Les communes les plus importantes devront recourir à des compétences externes en engageant des formateurs ou des professionnels, et les plus petites communes ne pourront disposer des compétences spécifiques ou des moyens d'engager des formateurs sur ce système»).

## Sur les questions plus générales

### La place de l'identité

Le projet INES prévoit la création, par l'État, d'une identité nationale électronique sécurisée; ce faisant il fait également évoluer les relations des citoyens avec le concept même d'identité. Le débat a donc tourné autour du postulat suivant: comment trouver un juste équilibre entre d'un côté «la légitimité dans une démocratie de disposer d'un moyen de s'assurer de façon aussi sûre que possible de l'identité des personnes»<sup>325</sup> et de l'autre le droit à l'anonymat. De manière générale, les participants au débat se sont demandé dans quelle mesure on doit protéger davantage son identité à l'heure du numérique.

### La carte nationale d'identité électronique permettra utilement de sécuriser l'identité

Les débats ont régulièrement rappelé que cette volonté de sécuriser l'identité s'inscrit également dans un contexte actuel de fraude et d'usurpation à l'identité sur les réseaux. L'avocat Thierry Wickers<sup>326</sup> a rappelé qu'une entreprise américaine (*ChoicePoint*) s'est récemment fait voler 145 000 «identités» (numéros de sécurité sociale, permis de conduire...) de clients dont elle avait la charge. Les débats en ligne ont rappelé l'affaire de «*phishing*»<sup>327</sup> de mai 2005 où des banques françaises furent victimes de cette escroquerie; à cette occasion le ministère de l'intérieur a d'ailleurs estimé que si les internautes utilisaient leur CNIE pour se connecter à leur banque, cette technique de fraude disparaîtrait. C'est pourquoi certains, comme Emmanuel-Alain Cabanis<sup>328</sup>, ont pu dire que le recours à l'électronique protège notre identité en faisant en sorte qu'on ne la confonde pas avec celle de notre voisin ou celle d'un usurpateur intentionnel (cf. le «*paradoxe de la liberté*» évoqué précédemment).

---

325. Contribution de Michel Elie, message sur internet du 8 avril 2005.

326. Contribution de Thierry Wickers, débat de Bordeaux, 8 mars 2005.

327. Contraction des termes anglais *ishing* («pêche») et *phreaking* («piratage des lignes téléphoniques»): escroquerie qui consiste à envoyer un courriel usurpant une identité pour obtenir des données personnelles. Le 27 mai 2005, quatre banques françaises ont été victimes de ce type de fraude: un courriel usurpant leur identité demandait au client de se connecter vers un faux site bancaire afin d'obtenir de ce dernier des données confidentielles (codes d'accès, numéro de compte).

328. Contribution d'Emmanuel-Alain Cabanis, débat de Rennes, 11 mai 2005.

### Quelle gestion de l'identité à l'heure du numérique ?

Face à ces changements, il a souvent été rappelé dans les débats que la gestion de l'identité à l'ère du numérique doit être observée avec la plus grande prudence. Yves Bismuth<sup>329</sup> estime ainsi, en tant qu'avocat, que la loi pourrait instaurer un «*Habeas Data*» qui protégerait officiellement les droits du citoyen à l'ère du numérique et notamment son identité.

Daniel Kaplan, quant à lui, note<sup>330</sup> que les relations humaines reposent depuis toujours sur une part de confiance souvent prépondérante. Dans certains cas, le fait de ne pas exiger de preuve d'identité peut même constituer le ciment d'une relation forte et durable, le signe d'une confiance réciproque. Si le recours a priori commode à la CNIE contribue à faire basculer ces relations de l'informel au formel, de la confiance à la sécurité, cela peut avoir des conséquences sur les relations sociales. Trop sécuriser une relation enlève paradoxalement de la confiance.

C'est ce que confirme et développe Gérard Dubey<sup>331</sup> qui remarque que «*la notion même d'identité numérique doit être au cœur de toute réflexion sur la biométrie. Ces techniques sont censées donner plus de confort aux usagers, protéger contre la fraude et faciliter les contrôles. On insiste moins sur le fait qu'elles vont se traduire, comme tout processus d'automatisation, par la suppression de médiations sociales ou humaines. Or, on le sait, la disparition progressive de la présence humaine renforce le sentiment d'insécurité. Ce qui est fragilisé, plus profondément, ce sont les rapports de confiance sans lesquels il n'existe pas de société.*» À ses yeux la question est donc «*de savoir ce que signifie et ce que change le fait de déléguer à des automatismes le soin de définir l'identité, à commencer par sa traduction en langage numérique*». Il note enfin que «*l'intolérance contemporaine à la fraude, à l'erreur, au risque de falsification [...] ne doit pas faire oublier qu'il n'y a d'identité réelle que sociale, sujette au changement, et la définition de l'identité civile n'échappe pas à cette règle. L'identité comporte nécessairement des marges d'incertitude ou d'indétermination qui constituent autant de sources d'erreurs potentielles et d'occasions de fraude. À moins d'en livrer une image extrêmement dégradée ou appauvrie, l'identité civile ne recouvre donc jamais l'identité réelle, mais doit au contraire refléter en partie cette indétermination*».

De plus, beaucoup se sont demandé dans quelle mesure la volonté de certifier l'identité ne va pas à l'encontre du droit à l'anonymat. À cet égard, Bruno Villalba<sup>332</sup>, maître de conférences à Lille II, a rappelé que l'anonymat est un droit et qu'un espace où il n'y a plus d'anonymat possible est un lieu où il n'y a plus d'espace privé. De même, Jean-Jacques Lavenue<sup>333</sup>, professeur de droit à Lille II, estime qu'avec la mise en place d'une identité certifiée apparaît le risque que le bénéfice de l'anonymat, le droit à l'oubli, voire à la dissimulation, disparaissent. Il insiste sur la nécessité de veiller à

---

329. Contribution d'Yves Bismuth, débat de Lyon, 31 mars 2005.

330. Contribution de Daniel Kaplan, débat de Marseille, 25 mai 2005.

331. Contribution de Gérard Dubey, message sur internet du 22 mars 2005.

332. Débat de Lille, 27 avril 2005.

333. Contribution de Jean-Jacques Lavenue, débat de Lille, 27 avril 2005.



ce que la sécurité ne devienne pas une idéologie et à cet égard rappelle les propos de Benjamin Franklin : « *Quiconque est disposé à abandonner une partie de sa liberté au nom d'une prétendue sécurité, ne mérite ni l'une ni l'autre.* »

Arnaud Belleil<sup>334</sup>, du groupe « Identité Numérique » de la FING, propose une « option » pour concilier sécurité de l'identité et protection de l'anonymat qui serait de faire en sorte que la CNIE « *ne soit pas systématiquement une carte d'identité mais, pour certains usages, uniquement une carte d'habilitation. On pourrait imaginer bien des cas de figure où le porteur de la carte aurait juste besoin de prouver qu'il est majeur, qu'il est de nationalité française, qu'il possède des droits [...] ou qu'il n'est pas déchu de certains droits [...] sans avoir pour autant à justifier de son identité.* »

## **Le rôle et la responsabilité de l'État**

### **Quelle responsabilité pour l'État certificateur ?**

Dans le cas où l'État remplit le rôle d'autorité de certification, beaucoup se sont demandé, à l'instar d'Annie Blandin<sup>335</sup> ou d'Éric Caprioli<sup>336</sup>, dans quelle mesure il sera responsable de la fiabilité du procédé. Pour ce dernier, l'État sera responsable de la fiabilité du procédé de signature électronique (outil de signature et certificat). Il estime de plus que l'on pourrait limiter la valeur d'usage du certificat : pour toute transaction au-delà d'une certaine somme le certificat ne serait plus valable. La responsabilité de l'État ne serait ainsi engagée que dans le cadre de cette somme (transaction de 10 000 euros par exemple).

D'autres, comme Marie-Laure Laffaire, avocate, et Thierry Autret, expert en sécurité<sup>337</sup>, ont estimé que la responsabilité de l'État ne doit être liée qu'à la délivrance des certificats et pour une durée limitée.

D'autres encore proposent que l'État développe une politique de certification dans laquelle sa responsabilité serait décrite exhaustivement.

### **L'intervention de l'État dans la sphère marchande**

Certains se demandent dans quelle mesure cette mainmise de l'État sur l'activité de certification ne va pas nuire à un marché privé qui a déjà du mal à décoller ou si, au contraire, c'est le seul moyen d'instaurer la confiance dans ce domaine.

Pour certains, l'État, qui serait son propre certificateur, entrerait en concurrence avec des prestataires de services de certification (PSC). Et il disposerait d'un avantage en termes de moyens et de confiance. Annie Blandin<sup>338</sup> estime ainsi que le risque n'est pas nul de voir émerger un monopole de la certification qui fausserait la concurrence sur ce marché. Elle note qu'avec cette intervention directe « *ès qualité sur le marché*

---

334. Contribution d'Arnaud Belleil, message sur internet du 3 mars 2005.

335. Contribution d'Annie Blandin, débat de Rennes, 11 mai 2005.

336. Contribution d'Éric Caprioli, débat de Marseille, 25 mai 2005.

337. Contribution de Marie Laure Laffaire et de Thierry Autret, 1<sup>er</sup> juin 2005.

338. Contribution d'Annie Blandin, débat de Rennes, 11 mai 2005.

*dit de la confiance, on est ici à contre-courant de la tendance actuelle qui consiste à exclure un nombre croissant d'activités du champ de la sphère publique lorsqu'elles sont de nature économique». À l'inverse, des internautes comme Beretta notent que «l'État en matière de signature électronique et de cryptage ne fait que le minimum syndical, remplir le vide laissé faute de rentabilité par le secteur privé en évitant soigneusement de concurrencer ce dernier».*

Au contraire, d'autres craignent que si l'État n'investit pas dès maintenant dans le domaine de la certification, il doive acheter au prix fort des certificats aux entreprises privées spécialisées, voire laisser l'offre de certificats venir uniquement du secteur privé. À ce titre, Martial Gabillard<sup>339</sup> estime que si l'État ne développe pas une offre dans le domaine de l'administration électronique et des certificats, le secteur privé risque de s'emparer de ce domaine. Il précise que le secteur de l'administration en ligne doit rester le fait de la puissance publique afin d'éviter une privatisation rampante des services qu'offre l'État et une remise en cause consécutive des exigences de service public.

## **Le principe de précaution en matière de nouvelles technologies**

Un grand nombre de participants aux débats ont souhaité que soit menée une réflexion sur le principe de précaution appliqué aux technologies de l'information et de la communication. Ces technologies devraient pouvoir faire l'objet d'actions de prévention pour faire face à des risques éventuels de dérives dans leur utilisation, à l'instar de ce qui a été mis en place pour l'environnement.

## **La fracture numérique**

Sur ce point trois remarques principales ont été énoncées lors des débats.

Tout d'abord, avant de développer, voire de généraliser, une carte nationale d'identité électronique, certains rappellent qu'il convient de prendre en compte le risque de «fracture numérique» entre ceux qui ne savent pas se servir des technologies de l'information et de la communication et les autres (personnes âgées etc.).

Ensuite, d'autres rappellent le risque de «fracture territoriale» entre les territoires desservis par l'internet haut débit et les autres mais surtout entre ceux qui bénéficieront de lieux de délivrance et ceux qui n'auront la carte que par le biais de stations d'acquisition mobiles. Il y a là, pour beaucoup, un risque de rupture dans le fonctionnement des services publics locaux.

Enfin, dans le cas où la CNIE serait obligatoire et payante, des risques de «fracture sociétale» entre ceux qui auront les moyens financiers et les autres sont soulignés. De façon générale, et comme cela a été rappelé par l'internaute danyd44, il y a une crainte de la marginalisation de ceux qui sont les «*ni-ni (ni urbains, ni jeunes)*» et de «*déshumanisation*» des relations avec l'administration.

---

339. Contribution de Martial Gabillard, débat de Rennes, 11 mai 2005.

## Analyse critique du processus du débat

Organiser un débat public n'est pas une chose nouvelle en France. En effet, il existe la Commission nationale du débat public<sup>340</sup> qui est chargée d'organiser un débat public sur les objectifs et caractéristiques principales des grandes opérations d'aménagement ou d'équipement d'intérêt national. De plus, de nombreuses consultations publiques (par exemple, actuellement est menée une « Consultation publique sur le service public des communications électroniques ») ou consultations nationales sont régulièrement mises en place (cf. sur la laïcité, sur l'école etc.). De même sur internet, le Gouvernement avait mis en place en 1999 une « Consultation publique sur l'adaptation du cadre législatif de la société de l'information » préparant la loi sur la société de l'information. Depuis, il existe [www.forum.gouv.fr](http://www.forum.gouv.fr), espace de discussion proposé par le gouvernement sur des sujets de société (réforme de l'état et service public, avenir de l'Europe, famille...).

Cependant, le Forum des droits sur l'internet a souhaité mettre en place une forme de débat à la fois innovante et complémentaire.

**Innovante tout d'abord dans les modalités de la consultation publique.** Le Forum des droits sur l'internet a souhaité conjuguer différentes façons de consulter les Français et de toucher divers types de population. Les débats en ligne et en régions, la mobilisation des experts, l'organisation du sondage ont permis de cerner au plus près les attentes des Français.

**Innovante surtout du fait du positionnement du Forum des droits sur l'internet.** Il ne s'agit en effet pas d'une consultation organisée par les pouvoirs publics eux-mêmes au soutien d'un projet mais d'un processus plus neutre mis en œuvre par un organisme situé à la confluence des pouvoirs publics, des entreprises et des utilisateurs.

Le but du Forum est de recueillir l'avis des Français, leurs interrogations et propositions ; il est aussi d'animer un processus interactif entre les Français et le ministère qui conduit celui-ci à expliquer, clarifier, identifier les points de blocage, le cas échéant, à modifier son projet. Le projet INES a ainsi été questionné, débattu et amendé avant même sa présentation en Conseil des ministres et auprès des institutions compétentes (CNIL, Conseil d'État, Parlement...).

Le débat public mis en œuvre par le Forum n'est donc pas une photographie de l'avis des Français sur le projet mais une dynamique aidant à la prise de décision.

**Innovante enfin par rapport aux autres pays.** Très peu ont mené des consultations avant de mettre en œuvre une CNIE et aucun n'a organisé de débat similaire au nôtre.

---

340. La loi du 2 février 1995 relative à la protection de l'environnement, dite loi « Barnier », crée la Commission nationale du débat public (CNDP). La loi du 27 février 2002 relative à la démocratie de proximité transforme la CNDP en une autorité administrative indépendante, garante du débat public, élargit son domaine de compétence et diversifie ses modes d'intervention : elle impose que les projets importants soient connus du public et confirme le principe que la CNDP organise un débat public sur l'opportunité, les objectifs et caractéristiques principales des grandes opérations d'aménagement d'intérêt national de l'État, des collectivités territoriales, des établissements publics et des personnes privées.

Deux pays ont néanmoins mené quelques consultations : le Canada et le Royaume-Uni.

Ainsi, au Canada, le « débat » autour d'un projet de CNIE s'est matérialisé par un colloque de deux jours précédé d'un sondage, le tout organisé par le Gouvernement sans véritable débat contradictoire. Le ministère fédéral de la citoyenneté et de l'immigration a envisagé de rendre obligatoire une carte d'identité avec indications biométriques mais n'a pas encore statué sur l'émission d'un tel document. Auparavant, ce ministère avait organisé un forum de deux jours sur le sujet (« *Biométrie, incidences et applications pour la citoyenneté et l'immigration* », les 7 et 8 octobre 2003 à Ottawa). Avant que ne s'ouvre ce forum, un sondage avait été réalisé. Il portait sur l'éventuelle instauration d'une carte nationale d'identité électronique. À la question « *compte tenu, d'une part des avantages possibles au niveau de la sécurité, d'autre part du risque possible pour la liberté, est-ce une bonne idée d'introduire une carte nationale d'identité électronique ?* » 57 % des Canadiens ont répondu positivement et 30 % négativement. Il ressort du sondage que la majorité des Canadiens estiment que l'utilisation frauduleuse de documents d'identification constitue un problème. Ils sont favorables au recours à la biométrie et à la mise au point d'une nouvelle carte d'identité mais dans l'optique où celle-ci serait délivrée de manière facultative. Les préoccupations portent principalement sur le respect de la vie privée, le coût élevé de la mise en œuvre, la capacité des criminels à contrer la technologie ou encore la possibilité que le gouvernement utilise abusivement ces renseignements personnels.

Au Royaume-Uni, le « débat » a également été mené uniquement par le Gouvernement par le biais d'auditions, de consultations et de sondage. Mais il a été souvent reproché à Tony Blair de ne pas avoir organisé de véritable débat national indépendant pouvant apporter la contradiction (seuls les experts ont véritablement été consultés). Ainsi, en juillet 2002, le Gouvernement a lancé une consultation sur la fraude à l'identité (jusqu'en janvier 2003). Un résumé a été rendu public le 11 novembre 2003, date à laquelle le projet pour une carte d'identité électronique a été annoncé. D'avril à juillet 2004, le Gouvernement a lancé un « *consultation paper* » (« *Legislation on Identity Cards – A consultation* ») auprès de nombreux organismes, syndicats etc. Sur les 5 000 personnes et organisations qui ont répondu, 4 200 se sont réellement exprimées. 60 % d'entre elles se sont prononcées pour l'instauration d'une carte nationale d'identité électronique. De plus, un sondage a été commandé : il indique que 80 % de la population est favorable à la CNIE mais seulement 50 % se déclare prêt à payer pour en disposer. Enfin, un site d'information a été ouvert sur le site du Home Office (<http://www.homeoffice.gov.uk/comrace/identitycards>). Parallèlement, et devant l'absence de véritable débat sur un sujet aussi fondamental, une forte campagne a été lancée contre le projet : 5 000 courriels ont été envoyés contre l'instauration d'une carte nationale d'identité électronique (sur [identitycards@homeoffice.gsi.gov.uk](mailto:identitycards@homeoffice.gsi.gov.uk)) et l'opposition s'est fédérée autour de [www.no2id.net](http://www.no2id.net) et [www.privacyinternational.org](http://www.privacyinternational.org).

Le projet de loi devrait être adopté prochainement, la carte serait alors déployée progressivement dès 2008 puis à terme rendue obligatoire.

**En outre, la démarche du Forum des droits sur l'internet est complémentaire de celle que mènent d'autres instances.** Ainsi la Commission nationale de l'informatique et des libertés rendra son avis en temps voulu sur le projet de loi, après avoir

mené ses travaux d'expertise. De même, la commission des lois du Sénat a mis en place une «mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire» en février 2005; elle devrait rendre prochainement ses travaux. Les conclusions du débat public peuvent aider ces instances dans leurs travaux, bien qu'elles poursuivent des objectifs différents.

Ces deux caractéristiques du débat public organisé par le Forum étant soulignées, deux questions légitimes peuvent être posées quant au processus engagé :

–le débat est-il efficace, c'est-à-dire, a-t-il été suivi d'effet ?

–le débat public est-il fiable, c'est-à-dire, ses conclusions sont-elles dignes de foi ?

## Le débat est-il efficace ?

### **Le débat en chiffres**

Le débat sur internet a reçu 3060 contributions soit plus de 50 % des taux de fréquentation habituels des forums en ligne de ce type. Le débat en régions a compté une présence moyenne de 100 personnes par débat dans six villes avec une présence allant de 70 personnes à Bordeaux à 205 à Paris, soit plus de 600 personnes en régions.

Le Forum des droits sur l'internet a également souhaité faire intervenir des experts à même d'éclairer le grand public et d'alimenter ainsi le débat par leurs connaissances et leurs réflexions sur le sujet. Des avocats, des chercheurs, des universitaires, des sociologues, des représentants de la société civile travaillant sur les notions d'identité numériques sont ainsi intervenus, soit sur le forum de discussion, soit lors de manifestations en régions. Ces contributions ont fait l'objet de nombreux commentaires de la part des internautes et de discussions en régions. Cinquante experts ont ainsi participé au débat (liste complète des experts en annexe).

### **Une fonction d'alerte sur un sujet sensible**

Le débat a permis de faire connaître aux Français le projet INES et les nombreux changements qu'il allait apporter dans la vie de tous les jours, de questionner utilement le ministère de l'intérieur et de proposer des recommandations qui viendront nourrir la réflexion gouvernementale et les débats parlementaires qui auront lieu par la suite.

Le débat a ainsi eu le mérite d'alerter l'opinion sur ce sujet. Le projet de carte nationale d'identité électronique a d'ailleurs progressivement été l'objet de prises de position de la part de nombreuses associations dont c'est naturellement le rôle. Ainsi, la Ligue des Droits de l'Homme, le Syndicat de la magistrature, le Syndicat des avocats de France, l'association IRIS (Imaginons un réseau Internet solidaire), l'intercollectif DELIS (Droits et libertés face à l'informatisation de la société) et l'Association française des juristes démocrates ont, le 26 mai, rendu public une pétition exigeant le retrait total et immédiat du projet INES. De son côté, le collectif «Souriez vous êtes filmés» a envoyé, le 21 mai 2005, une «*Lettre ouverte aux maires de France. Exprimez votre désaccord sur le projet de carte d'identité électronique à votre maire*». Les syndicats CGT, CFDT, SUD, CGT-FO, CGC, CFTC de l'INSEE ont rédigé, le 9 mai

2005, une «*Lettre ouverte au Directeur général de l'Insee: l'Insee n'a pas vocation à être une annexe du ministère de l'intérieur!*». L'association des Maires des Grandes Villes de France a envoyé un message sur le fond du projet le 12 mai 2005 et de nombreux autres organismes ou associations se sont exprimés par la suite.

Ces prises de position se sont d'ailleurs souvent faites dans le débat en ligne ou en régions, soit directement («*Souriez vous êtes filmés*», lettre ouverte des syndicats nationaux de l'Insee, AMGVF, AMF, FING, APRIL, Club de l'Hyper-République, FNTC, Association photographes...), soit indirectement par le biais d'alertes des internautes ou de communications en régions (pétition de la LDH, SM, SAF, IRIS, DELIS et AFJD).

## **L'impact du débat sur le projet de carte nationale d'identité électronique**

Ce débat a-t-il eu un impact sur le projet de carte nationale d'identité électronique? Dans quelle mesure le ministère de l'intérieur va-t-il en tenir compte? Ce débat n'est-il pas en fait qu'un prétexte, pour les pouvoirs publics, d'obtenir un assentiment populaire avant la mise en place de la CNIE? Quelle est la crédibilité pour ce débat alors que le ministre de l'intérieur a rendu public ses orientations et que le projet a reçu l'aval du Premier ministre avant même la fin des débats? Toutes ces questions ont été régulièrement posées lors des débats.

D'autres personnes ont également regretté que le processus de débat ne soit pas suffisamment connu et que, pour un débat de portée nationale, il n'y ait ni campagne de presse ni informations diffusées à la télévision (Eupalinos regrette que ce débat ne touche «*qu'une infime partie de la population. Quand nos présentateurs TV des trois premières chaînes parleront-ils de même?*»). Ce manque d'informations fait craindre à certains, comme Cogex ou Katwoman, que le débat n'ait été qu'une «*pseudo-consultation*».

Le Forum des droits sur l'internet reconnaît qu'aucun moyen ne lui a été alloué pour faire connaître le débat auprès du grand public; il s'en est d'ailleurs régulièrement plaint auprès du ministère.

En revanche, il a pu être constaté que les débats en région ont toujours bénéficié d'une très large couverture presse: le sujet, quand il est connu, intéresse!

En outre, c'est dans le débat que le ministère de l'intérieur a choisi de préciser divers éléments du projet, comme l'accès indirect à la base, les modes de lecture des données sur la carte, les modes de délivrance... C'est aussi au cours du débat que le ministère a reconnu les insuffisances dans le projet ou les points qui méritaient réflexion: l'absence de chiffres sur la fraude à l'identité, l'articulation avec le projet de dématérialisation de l'état civil, le manque de lien entre les projets passeport et CNIE... Le processus de débat a donc, dans sa fonction clarificatrice, eu des impacts.

Il a même, dans quatre cas, conduit à des changements concrets du projet CNIE:

1) L'aspect portfolio enlevé

Le ministère proposait un bloc «*portfolio personnel*»: cette fonction optionnelle devait permettre de stocker des informations complémentaires dans la carte, soit pour faci-

liter des transactions électroniques (par exemple stocker de manière « exportable » nom, prénom et adresse pour remplir des formulaires), soit pour remplacer d'autres papiers (ex : numéro de permis de conduire, numéro fiscal, etc.). Les gens ont montré dans le débat soit une opposition, soit peu d'intérêt. Au cours du débat, le ministère de l'intérieur a annoncé son souhait de retirer cette fonctionnalité du projet.

## 2) Le « sans contact » reconsidéré et plus sécurisé

Les nombreux débats sur le « sans contact » ont montré qu'il est impératif pour le ministère de fournir des preuves sur la sécurité de cette fonctionnalité avant de valider son utilisation. Dans les débats en région le ministère a précisé que tous les États s'interrogent sur la possibilité d'utiliser cette technologie et a reconnu qu'elle ne serait introduite en France pour la carte nationale d'identité électronique que si les études montrent qu'il n'y a pas de risque de capture des informations à l'insu du porteur, et selon les normes qui permettront de s'en assurer. Dans le débat en ligne, de nombreuses propositions ont été faites (cage de Faraday/étui métallique) et recon- nues utiles par le ministre de l'intérieur, qui va reconsidérer cet aspect du système.

## 3) Une proposition de schéma alternatif prise en considération par le ministère

Aux propositions concernant une gestion différente de la base d'empreintes, le ministère a estimé possible de suivre l'une d'entre elle (décrite dans le rapport par les internautes Alice et Zorglub42...) tout en précisant que ce choix était lié à la finalité même du projet.

## 4) Introduction de mesures de traçabilité de consultation des données de la carte

Le ministère a souhaité étudier les suggestions issues du débat sur le traçage des contrôles de carte pour éviter les abus, que ce soit par une « boîte noire » dans le lecteur, ou par inscription dans la puce. Le ministère a également pris en considéra- tion la possibilité pour le citoyen de vérifier sur un serveur l'habilitation des personnes l'ayant contrôlé.

## Le débat public est-il fiable ?

Le débat a rassemblé un grand nombre de personnes : plus de 600 présentes en régions, plus de 3000 contributions sur internet. À titre d'exemple, le sujet qui a connu le plus de succès sur le site institutionnel <http://www.forum.gouv.fr> (« Réforme de l'État : Quel service public pour demain ? ») a reçu 1 908 contributions. Les citoyens ont entendu parler de l'existence du débat par la presse qui en a fait un large écho, ou par les moyens d'information mis en place par le Forum, relayés par les pouvoirs publics (site du Premier ministre, de l'ADAE, de la CNIL...) et l'univers associatif, qui s'est progressivement mobilisé sur ces enjeux.

De plus, les contributions reçues furent de qualité. En effet, il semble que l'on ait souvent eu affaire à des « citoyens-experts » car les personnes « contributrices » se sont avérées être bien informées, alertées quant aux enjeux du projet de CNIE et posant des questions pertinentes. Les échanges qui sont intervenus étaient le plus souvent de haute qualité. Cependant, des propos erronés, voire des rumeurs, ont parfois pu être présents (le fait que la carte puisse être lue à plusieurs centaines de mètres, l'existence prochaine d'une puce sous cutanée...). Il se dégage une grande

homogénéité entre les réactions/contributions dans les débats en ligne et celles qui se sont exprimées en régions. Beaucoup de propositions concrètes ont pu être faites. Certaines sont d'ailleurs reprises dans le présent rapport. De plus, les « experts » qui se sont exprimés ont apporté de nouveaux éléments et ont utilement éclairé le projet dans le domaine qui est le leur. Enfin, de nombreux organismes et associations sont intervenus directement dans le débat en ligne ou en régions (cf. LDH, IRIS, AMGVF, FING, APRIL, FNTEC...), permettant d'analyser certains points du projet au regard de leurs préoccupations spécifiques.

Enfin, le fait d'avoir mené des débats et commandé un sondage a permis de combiner divers outils en associant une approche à la fois qualitative et quantitative du sujet. Ce faisant, le Forum a obtenu des résultats larges et complets sur l'état de l'opinion. En effet, les appréciations qualitatives apportées par les débats en ligne ou en régions (public averti, contributeurs parfois revendicatifs, débats de qualité...) ont été complétées par les résultats quantitatifs d'un sondage (appréciation neutre d'un échantillon représentatif de la population, soit 950 personnes a priori moins sensibilisées à ces questions).

À ce titre on peut donc estimer que le débat public est fiable et a couvert, par une approche plurielle, un large éventail d'opinions.

## **Analyse et recommandations du Forum des droits sur l'internet**

Compte tenu des enseignements du débat en ligne et en région mais également des indications du sondage, le Forum des droits sur l'internet formule aux pouvoirs publics les analyses et recommandations suivantes.

À titre liminaire, on constate deux choses :

D'une part, que ce **débat sur la carte d'identité électronique est un débat qui intéresse les Français** : ils se sont mobilisés tout au long du débat public et, au vu du sondage, sont peu à ne pas avoir d'opinion sur ce sujet majeur.

**D'autre part, en raison de l'impératif de sécurité, le sondage montre que les Français sont, pour les trois quarts, favorables au projet de carte d'identité électronique**<sup>341</sup>.

---

341. Il est intéressant de rapprocher ce résultat de celui, quasiment similaire, d'un autre sondage réalisé en août 2002 par la SOFRES pour le Forum des droits sur l'internet sur une question très proche : «*Seriez-vous favorable ou opposé à ce que l'État délivre aux personnes qui en font la demande une carte d'identité électronique sécurisée (carte à puce) qui pourrait leur servir dans l'accomplissement de toutes leurs démarches administratives sur Internet (identification, signature, paiement en ligne) ?* » 73 % des sondés avaient répondu favorablement, 25 % négativement. Le sondage est disponible sur : <http://www.foruminternet.org/telechargement/documents/sdg-admelec-res-020924.pdf>



**Cependant, en contrepoint à cette tonalité globalement positive, les débats en ligne et en région ont fait remonter des réticences très fortes sur certains aspects du projet. Le gouvernement et le Parlement devront répondre à celles-ci s'ils souhaitent poursuivre le déploiement du projet dans un climat de consensus.** Les propositions ci-après ont l'objectif d'y contribuer.

Les enjeux de sécurité sont essentiels  
aux yeux des Français mais les arguments avancés  
à l'appui du projet n'ont pas convaincu

Si le sondage IPSOS et le débat public, dans une certaine mesure, ont montré que les Français sont sensibles aux enjeux liés à la sécurisation de leur identité, le débat a aussi montré que les arguments avancés par le ministère de l'intérieur justifiant le projet INES n'ont pas véritablement convaincu. Les raisons sont apparues minces, voire inadaptées, la plupart du temps mal comprises. En particulier la fraude à l'identité, présentée comme un argument majeur n'a pas pu être clairement chiffrée et le lien avec le projet de passeport électronique est apparu artificiel et même contre-productif.

### **Des études sur la fraude à l'identité**

Il semble difficile d'envisager un tel projet sans avoir de données chiffrées sur la fraude à l'identité en France.

**Le Forum des droits sur l'internet recommande que soit réalisée une étude rigoureuse visant à mesurer l'ampleur réelle de la fraude à l'identité en France.**

### **Un découplage avec le projet passeport**

Le débat a montré que si la France est tenue par les dispositions européennes visant à adopter un passeport biométrique dans un bref délai, ces textes et l'urgence de transposition qui leur est liée, ne s'appliquent pas à la carte d'identité nationale.

En outre, le couplage des deux procédures a donné l'impression que la France, sur un domaine régalién, subissait des pressions étrangères (européennes et surtout américaines).

**Au regard des enjeux et de l'impact du projet INES, le Forum des droits sur l'internet recommande que sa mise en œuvre ne soit pas couplée avec le projet passeport.**

## La protection de la vie privée est une préoccupation majeure à laquelle le projet doit apporter des garanties complémentaires

Une majorité des contributions enregistrées au cours du débat public concernent la protection de la vie privée. Au-delà du débat théorique sur le changement de société que susciterait la CNIE, elles s'inquiètent tant des dérives éventuelles dans l'utilisation de la base centrale par l'administration que d'un rapprochement entre fichiers publics et privés. Concernant la base centrale, de nombreux débats ont porté sur sa finalité précise. Des internautes ont estimé que si le projet se limitait à lutter contre la fraude à l'identité (gérer la fraude au renouvellement et assurer une délivrance sans doublon de cartes), un autre scénario de base, plus protecteur en termes de protection des données, serait alors possible (voir page 236).

De façon générale, la relative incompréhension des objectifs du projet conduit à renforcer la sensibilité des individus sur les aspects liés à la protection de leur vie privée.

### **Un nouveau pacte social doit être conclu entre l'État et le citoyen**

Le projet de CNIE est l'occasion pour l'État de préciser les relations qu'il souhaite entretenir avec le citoyen dans un contexte de déploiement de l'administration électronique. À un contrôle accru des titres et de l'identité individuelle doit correspondre une possibilité accrue de maîtrise par le citoyen des données qui le concernent dans les téléprocédures administratives. Cette réciprocité est un gage d'équilibre et de confiance.

**Dans la mesure où la carte nationale d'identité électronique donne accès à des téléprocédures administratives, le Forum des droits sur l'internet recommande que le citoyen ait un accès en ligne, gratuit et permanent, à ses dossiers administratifs et au suivi de l'état d'avancement de sa démarche.**

### **Il convient de porter une attention particulière sur la mise en place d'un identifiant unique**

Le projet INES prévoit que la CNIE permettrait de conjuguer, sur un support unique, des finalités différentes comme le contrôle d'identité et l'accès à des téléprocédures administratives. Ceci pourrait conduire à ce que les individus soient identifiés de façon unique et centralisée quel que soit l'usage. Cette perspective d'identifiant unique serait un changement significatif avec le principe de pluralité des identifiants sur lequel l'administration électronique s'est fondée jusqu'à présent.

**Le Forum des droits sur l'internet appelle l'attention des pouvoirs publics sur la cohérence entre l'identification unique et centralisée, telle que prévue dans le projet INES, et le principe de pluralité des identifiants utilisé actuellement dans le cadre de l'administration électronique.**

## **Le projet de carte nationale d'identité électronique doit faire l'objet d'un contrôle global et permanent**

Face aux enjeux du projet de CNIE, face aux craintes liées à la protection de la vie privée et de l'introduction de la biométrie et aux doutes quant à la sécurité du système, un contrôle fort et effectif a été souhaité. Ce contrôle devra non seulement s'effectuer en amont du déploiement de la carte (études...) mais aussi de façon continue pour prévenir d'éventuelles dérives (un élargissement de l'accès de la base à d'autres agents ou des usages de la base au-delà de ceux initialement prévus...).

**Le Forum des droits sur l'internet estime fondamental que l'aspect contrôle soit étudié et mis en œuvre en même temps que le déploiement du projet. À cet effet, le Forum recommande un contrôle global et permanent du système sous la responsabilité de la CNIL<sup>342</sup>. Pour ce faire, cette institution devra disposer de moyens juridiques et financiers nécessaires pour contrôler, de façon effective, le dispositif. Il conviendra notamment de voir dans quelle mesure l'actuelle loi Informatique et Libertés permet d'assurer de telles missions. Une partie du financement du programme de la carte nationale d'identité électronique pourrait être affectée à cette fonction de contrôle.**

### Des incertitudes à lever en termes de sécurité

De nombreux intervenants ont noté que, si le projet INES allait sans nul doute renforcer la sécurité des titres d'identité, celle-ci devait être étudiée de façon globale, à tous les stades d'élaboration et d'usage de la carte. En particulier, en amont, l'articulation du projet avec la gestion de l'état civil est apparue critique, tout comme en aval, les aspects «sans contact» de la carte (risque de lecture à l'insu du porteur) et

---

342. Le contrôle devra répondre aux objectifs suivants :

1) En amont du déploiement du projet de carte d'identité électronique :

– Réaliser une expertise sur l'architecture du système dans le domaine de la sécurité informatique.

– Mener une étude sur l'acceptabilité de la biométrie afin de connaître, à une grande échelle, l'appropriation individuelle qui sera faite de cette technique.

– Mener des études sur l'impact du projet sur la vie privée (*les pouvoirs publics pourraient prendre exemple sur les procédures d'évaluation de la conformité d'un projet ou d'une technologie aux exigences générales de protection de la vie privée mises en place au Canada dans le cadre du «Personal Information Protection and Electronic Documents Acts». Cette «démarche d'évaluation d'impact sur la vie privée» permet d'identifier les risques d'atteinte à la vie privée des projets gouvernementaux et privés, de traiter les non conformités etc. Ces éléments sont ensuite présentés aux autorités décisionnaires et au public*).

2) À partir de la mise en œuvre d'une carte d'identité électronique :

– Contrôler de façon permanente le fonctionnement de la base, les agents qui y ont accès et les motifs d'accès ainsi que le journal des consultations. Ceci pour permettre la rectification des informations et prévenir toute évolution possible de l'usage de la base.

– Recevoir les réclamations des particuliers.

– Assurer une évaluation permanente du système sous tous ses aspects (sécurité, protection des données, sociologique, financier) ainsi qu'une veille juridique, scientifique et technologique.

– Rendre compte de son activité par le biais de la publication d'un rapport spécifique qui devra notamment se préoccuper des évolutions constatées et des incidences des mesures prises et envisagées.

Pour remplir cette mission nouvelle la CNIL pourrait associer, dans un souci d'adjonction des compétences, des représentants de la société civile et du secteur privé.

les usages sur internet (réseau ouvert sujet à de nombreuses attaques et failles de sécurité).

### **Une évaluation de l'aspect lecture « sans contact » de la carte**

Les nombreux échanges sur le « sans contact » ont montré qu'il est impératif de fournir des preuves de la sécurité de ce canal avant de pouvoir valider son utilisation.

**L'aspect « sans contact » de la carte ayant fait l'objet de nombreuses craintes, le Forum des droits sur l'internet recommande que cette technologie ne soit introduite en France pour la carte nationale d'identité électronique que si les études montrent qu'il n'y a pas de risque de capture des informations à l'insu du porteur, et selon les normes qui permettront de s'en assurer.**

### L'articulation entre le projet INES et celui de dématérialisation de l'état civil

Le projet INES prévoit que la procédure de délivrance des titres soit sécurisée en amont par la mise en œuvre d'un processus d'échange direct des données d'état civil entre mairie de naissance et mairie de délivrance des titres. La conjugaison de ces deux démarches devrait contribuer à conférer une sécurisation supplémentaire aux documents d'identité. Pour ce faire, un projet, conduit par le ministère de la justice, prévoit de dématérialiser les actes de l'état civil.

À cet égard, certains ont noté qu'à ce jour il semble que le projet de CNIE ne s'articule pas avec celui de dématérialisation de l'état civil, chaque ministère ayant son propre calendrier. Or, il apparaît que sans une informatisation concomitante de l'état civil, le projet de CNIE risque d'avoir des failles de sécurité.

**Le Forum des droits sur l'internet, regrettant le manque de coordination entre les projets du ministère de la justice et de l'intérieur, recommande que la délivrance d'une carte nationale d'identité électronique ne soit mise en place que lorsque l'informatisation de l'état civil sera achevée, sinon la délivrance des cartes risque d'avoir des failles de sécurité.**

Une attente mitigée par rapport à une carte de services

### **Un faible intérêt pour une CNIE utilisable pour les téléprocédures administratives**

Même si certains participants au débat, et notamment des représentants de collectivités locales, ont exprimé leur intérêt pour une carte combinant des fonctions d'identification et d'accès à des téléprocédures administratives, les réactions ont majoritairement montré un faible intérêt pour cette orientation.

**Il conviendra, si cette orientation devait être confirmée, de mener une campagne**

**énergique d'explication, soulignant l'articulation de la carte nationale d'identité électronique avec les cartes locales déjà existantes ou en projet.**

### **Une réticence assez forte pour une carte « signeuse » pour les échanges marchands**

Si le projet INES n'est pas entièrement clair sur la possibilité d'utiliser ou non les certificats de la carte sur des sites marchands, une relativement forte opposition s'est dégagée sur cette idée qui conduit à combiner, sur un même support, des usages régaliens et marchands.

Des réticences sur le caractère payant  
et obligatoire de la carte nationale d'identité électronique

### **La carte doit être gratuite à la première délivrance**

**Dans le cas où le Parlement décide de rendre la carte nationale d'identité électronique payante, le Forum des droits sur l'internet recommande qu'elle soit gratuite à la première délivrance mais payante en cas de perte ou de renouvellement.**

Un débat devant le Parlement sur le caractère obligatoire

Ce point a fait débat : certains ont annoncé que si la carte n'est pas obligatoire elle ne sera jamais adoptée largement et ne servirait pas dans les faits ; le sondage semble confirmer cette opinion. Cependant, la très grande majorité des intervenants au débat se sont opposés au caractère obligatoire estimant que celui-ci serait une rupture avec une tradition républicaine.

**Le Forum des droits sur l'internet recommande au Parlement d'étudier l'éventualité du caractère obligatoire de la carte avec la plus grande attention. L'hypothèse d'une carte nationale d'identité électronique obligatoire représenterait, dans l'esprit des traditions républicaines d'un pays comme la France, un changement de première importance.**

La sensibilité de l'enjeu territorial

Le projet prévoit, en raison du coût, mais aussi pour des raisons de sécurité et de charge de travail pour les petites collectivités, de concentrer l'émission et la délivrance de la nouvelle carte sur quelques centaines de mairies. Cette décision suscite beaucoup de controverses, tant auprès des collectivités locales qui veulent toutes garder le lien privilégié avec les citoyens que constitue la délivrance de la carte, qu'auprès des individus très attachés à une offre de service public répartie sur l'ensemble du territoire.

À cet égard, la solution d'une borne itinérante (station d'acquisition) allant dans chaque commune rurale n'apparaît pas comme une véritable réponse.

De plus, des problèmes de formation des agents municipaux, d'équipements des mairies en matériels ou encore organisationnels (l'adaptation des locaux pour garantir la confidentialité des opérations, l'organisation de l'attente etc.) se posent.

**Compte tenu des enjeux liés à l'aménagement du territoire, le Forum des droits sur l'internet estime que la délivrance en mairie de la carte nationale d'identité électronique mérite une large concertation avec les élus et leurs représentants afin que puisse être trouvée une solution de consensus.**

## Le contexte européen

La carte nationale d'identité est reconnue comme document de voyage dans un certain nombre de pays (les pays membres de l'Union Européenne mais aussi l'Islande, la Norvège, ou encore la Suisse et la Turquie). Le projet doit permettre à la carte nationale d'identité électronique de pouvoir être acceptée par ces pays.

**Le Forum des droits sur l'internet insiste sur le fait que la CNIE devra impérativement être acceptée dans tous les pays où elle sert déjà de document de voyage. Pour ce faire, des travaux d'harmonisation avec les normes et standards adoptés en la matière et d'interopérabilité avec les autres pays devront être menés.**

## Conclusion

Le projet de CNIE est un projet majeur qui peut modifier la vie des Français et le rapport qu'ils entretiennent avec l'État. Malgré leur forte sensibilité aux enjeux de sécurité qui conduit plus des trois-quarts d'entre eux à se déclarer favorables au projet de carte nationale d'identité électronique, le débat public a mis en lumière de fortes réticences sur certains points. Dès lors, le ministère doit revoir le projet afin de répondre à celles-ci s'il souhaite poursuivre son déploiement dans un climat de consensus.

# Annexe 1

## Lettre de mission



MINISTÈRE DE L'INTERIEUR,  
DE LA SECURITE INTERIEURE ET DES LIBERTES LOCALES

LE MINISTRE

Paris, le - 6 JAN. 2005

Madame la Présidente,

Le programme INES a été élaboré pour apporter aux citoyens à la fois plus de sécurité et plus de facilités dans leurs relations avec l'administration :

- plus de sécurité, face à la fraude documentaire qui prend des proportions croissantes (immigration illégale, fraude aux prestations sociales, escroqueries diverses), et dont le coût pour la Nation tout entière devient alarmant ; et face au terrorisme qui profite des lacunes des systèmes actuels pour se jouer des contrôles.
- plus de facilités, en réformant et en unifiant les procédures actuelles de demandes de titres, et en proposant d'autres usages nécessaires à la vie quotidienne des Français.

Ce programme doit également respecter des contraintes internationales concernant l'introduction, dans un délai court, de la biométrie dans les titres de voyage.

.../...

Madame Isabelle FALQUE-PIERROTIN  
Présidente du Forum des droits sur l'internet  
6, rue Déodat de Séverac  
75017 PARIS

Des interrogations légitimes peuvent naître dans l'opinion publique sur un tel projet. Aussi, compte tenu de ces éléments, je souhaiterais que vous puissiez organiser un débat public sur l'ensemble de ces enjeux, afin d'informer l'opinion sur ce dossier et de recueillir les avis et les propositions des citoyens.

Ce débat se déroulerait sous deux formes :

- d'une part, un débat en ligne avec modérateur, ouvert sur le site internet du Forum des droits sur l'internet ;
- et d'autre part, des débats régionaux grand public dans plusieurs villes de France.

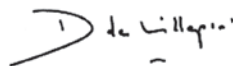
La période 1<sup>er</sup> février – 30 avril 2005 paraîtrait la plus favorable.

Si cette coopération rencontre votre adhésion, le ministère de l'intérieur de la sécurité intérieure et des libertés locales se chargerait de l'annonce publique dans le cadre de son point de presse. Les préfetures de région assureraient l'organisation matérielle des débats en région, et le ministère prendrait en charge les frais de déplacement. Un agent du programme INES coopérerait avec le Forum pour la modération et l'animation conjointes du débat en ligne.

La direction de programme INES fixera avec vous les modalités pratiques de préparation et de lancement de ce débat, et notamment le choix des sujets à aborder et leur traitement.

Je tiens à vous remercier tout particulièrement de cette opération conjointe entre le Forum et le Ministère.

Je vous prie d'agréer, Madame la Présidente, l'expression de mes sentiments les meilleurs.



Dominique de VILLEPIN



## Annexe 2

### **Experts intervenus aux débats en ligne et en région**

Cinquante experts sont intervenus dans le débat en ligne ou en régions :

**Association des maires de grandes villes de France**

**Association pour la Promotion et la Recherche en Informatique Libre (APRIL)**

**Thierry AUTRET**, expert Sécurité, Groupement des cartes bancaires

**Arnaud BELLEIL**, directeur associé de Security.com et Co-animateur du groupe « Identité Numérique » de la Fondation internet nouvelle génération (Fing)

**Yves BISMUTH**, avocat, président d'honneur de l'Association française du droit de l'informatique et de la télécommunication

**Annie BLANDIN**, maître de conférences à École nationale supérieure des télécommunications de Bretagne

**Christian CABAL**, député et auteur d'un rapport sur la biométrie au sein de l'Office parlementaire d'évaluation des choix scientifiques et technologiques

**Emmanuel-Alain CABANIS**, professeur de médecine et président de la société de biométrie humaine

**Éric CAPRIOLI**, avocat et membre de la délégation française auprès des Nations unies sur les questions de commerce électronique

**Olivier CHAVRIER**, directeur de la division identité et sécurité, Gemplus

**Simon CHIGNARD**, vice-président de l'association multimédia BUG

**Club de l'Hyper République**

**Alain DAMASIO**, écrivain

**Claudine DARDY**, professeur de sociologie à l'université Paris XII

**Marcel DESVERGNES**, président d'Aquitaine Europe communication

**Bernard DIDIER**, directeur développement des affaires, division sécurité Sagem

**Gérard DUBEY**, sociologue à l'Institut national des Telecoms, chercheur au CETCOPRA (Centre d'étude des techniques, des connaissances et des pratiques)

**Youval ECHED**, secrétaire général de l'Académie internationale des droits de l'homme, administrateur et trésorier de l'Association française du net

**Bernard FITOUSSI**, préfet, directeur du programme INES, ministère de l'Intérieur

**Patrice FLICHY**, professeur de sociologie à l'université de Marne-la Vallée

**François GIQUEL**, vice-président de la Commission nationale de l'informatique et des libertés

**Martial GABILLARD**, président de l'Association des villes et collectivités pour les communications électroniques et l'audiovisuel (AVICCA)

**Sylvain GOMBAULT**, enseignant/chercheur à l'École nationale supérieure des Telecoms de Bretagne, membre du projet SERES (Sécurité des réseaux et des applications réparties)

**Xavier GUCHET**, philosophe, chercheur au CETCOPRA (Centre d'étude des techniques, des connaissances et des pratiques), université de Paris I

**Claudine GUERRIER**, enseignant chercheur à l'Institut national des Telecoms

**Olivier ITÉANU**, avocat à la Cour d'appel de Paris

**Christophe JOLIVET**, membre du bureau du Club de la sécurité des systèmes d'information français

**Vania JOLOBOFF**, Silicomp – AQL, société d'ingénierie en informatique

**Daniel KAPLAN**, délégué général, Fondation internet nouvelle génération

**Marie-Laure LAFFAIRE**, avocat à la Cour d'Appel de Paris

**Frédéric LAGANDRÉ**, responsable du Pôle technique, direction de la sûreté, Aéroports de Paris

**Amar LAKEL**, chercheur associé, université de Paris X, Nanterre

**Thomas LAMARCHE**, enseignant chercheur à l'université Lille III

**Jean-Jacques LAVENUE**, professeur de droit, université Lille II

**Meryem MARZOUKI**, présidente de l'association IRIS (Imaginons un réseau internet solidaire) et chercheuse au CNRS

**Patrick NOUVEL**, directeur commercial domaine identitaire Thales Security System

#### **Observatoire des Usages de l'Internet (OUI)**

**Jean PÉRINGUEY**, président de la communauté de commune de Villandraut et maire de Noaillan

**Pierre PIAZZA**, chargé de recherche à Institut national des hautes études de sécurité

**Thierry PIETTE-COUDOL**, avocat près la Cour d'appel de Paris

**Gilbert PUECH**, président de l'université de Lyon II

**Philippe RIGAUT**, sociologue, enseignant à l'université de Picardie – Jules Verne

**Alain RISSON**, maire de Gluiras et responsable du groupe de travail «Nouvelles technologies» de l'association des maires de France

**Cyril ROJINSKY**, avocat au barreau de Paris

**Pierre TRUDEL**, professeur à l'université de Montréal, Canada

**Michel TUBIANA**, président de la Ligue des droits de l'homme

**Hubert VIGNERON**, président de la section «carte à puce» du Gixel (groupement des industries électroniques) et directeur marketing stratégique, Axalto

**André VITALIS**, directeur du Centre d'étude des médias université Michel de Montaigne, Bordeaux III

**Gérard WEISZ**, secrétaire général de la Fédération nationale des Tiers de confiance

**Thierry WICKERS**, avocat, président de la Conférence des bâtonniers

## Annexe 3

# Comptes rendus des débats en régions et en ligne et les contributions des experts en ligne

### Les débats en ligne ont été animés par :

**Jean Gonié**, Juriste, le Forum des droits sur l'internet

**Fabrice Mattatia**, Ingénieur en chef des Télécommunications, Direction de programme INES (Identité Nationale Électronique Sécurisée), ministère de l'intérieur

**Sophie Planté**, Adjointe au Directeur, Direction de programme INES (Identité Nationale Électronique Sécurisée), ministère de l'intérieur

**Yann Tésar**, Modérateur, Le Forum des droits sur l'internet

### Les débats en régions ont été animés par :

**Jean Gonié**, Juriste, le Forum des droits sur l'internet

**La Direction de programme INES** (Identité Nationale Électronique Sécurisée) du ministère de l'intérieur a été représentée dans les débats par **Bernard Fitoussi**, Préfet, directeur du Programme INES et **Sophie Planté**, adjointe au directeur.

## Liens vers les comptes rendus des débats itinérants

### **Bordeaux (8 mars 2005) :**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-bordeaux-20050308.pdf>

### **Lyon (31 mars 2005) :**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-lyon-20050331.pdf>

### **Paris (11 avril 2005) :**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-paris-20050411.pdf>

### **Lille (27 avril 2005) :**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-lille-20050427.pdf>

### **Rennes (11 mai 2005)**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-rennes-20050511.pdf>

### **Marseille (25 mai 2005) :**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-marseille-20050525.pdf>

### **Synthèse générale :**

<http://www.foruminternet.org/telechargement/forum/cpte-rendu-debats-itinerants.pdf>

Liens vers les comptes rendus des débats  
en ligne (du 1<sup>er</sup> février au 7 juin 2005)

**Synthèse de la première semaine de débats -8 février 2005:**

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese1.pdf>

**À propos de la lecture «sans contact» de la carte et la création d'une base  
d'empreintes digitales numérisées -24 février 2005:**

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese2.pdf>

**Deuxième synthèse des contributions des internautes du 8 février au 29 mars  
2005:** <http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese3.pdf>

**Synthèse des contributions des internautes sur le thème «biométrie» du 29 mars  
2005**

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese4.pdf>

**Synthèse des contributions des internautes sur le thème «vie privée» du 22 avril  
2005**

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese5.pdf>

**Synthèse des contributions des internautes sur le thème «sécurité» du 27 mai  
2005**

<http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese6.pdf>

**Réponses du ministère de l'intérieur sur le thème «biométrie» -30 mars 2005**

[http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese4\\_rm.pdf](http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese4_rm.pdf)

**Réponses du ministère de l'intérieur sur le thème «vie privée» -25 avril 2005**

[http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese5\\_rm.pdf](http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese5_rm.pdf)

**Réponses du ministère de l'intérieur sur le thème «sécurité» -1<sup>er</sup> juin 2005**

[http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese6\\_rm.pdf](http://www.foruminternet.org/telechargement/forum/cnie-enligne-synthese6_rm.pdf)

**Synthèse générale:**

[http://www.foruminternet.org/telechargement/forum/syntheses\\_cnie.pdf](http://www.foruminternet.org/telechargement/forum/syntheses_cnie.pdf)

Liens vers les contributions des experts en ligne

Les contributions des experts ayant contribué en ligne:

<http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnie.pdf>

## Annexe 4

# Le sondage Ipsos / Forum des droits sur l'internet 20 et 21 mai 2005

### FICHE TECHNIQUE

**SONDAGE EFFECTUÉ POUR :** le Forum des droits sur l'internet.

**DATES DU TERRAIN :** les 20 et 21 mai 2005.

**ÉCHANTILLON :** 950 personnes, constituant un échantillon national représentatif de la population française âgée de 18 ans et plus.

**MÉTHODE :** échantillon interrogé par téléphone. **Méthode des quotas :** sexe, âge, profession du chef de famille, catégorie d'agglomération et région.

### RÉSULTATS

#### 1/ Opinion à l'égard de la carte d'identité électronique

**Question :** dans le cadre de la lutte contre la fraude à l'identité, le ministère de l'intérieur envisage de remplacer la carte d'identité actuelle par une carte d'identité électronique comportant des données personnelles numérisées telles qu'empreintes digitales, photographie, voire iris de l'œil. Personnellement, êtes-vous très favorable, plutôt favorable, plutôt défavorable ou très défavorable à la mise en place de cette nouvelle carte d'identité ?

Base : à tous

	Pourcentage (%)
• Très favorable	30
• Plutôt favorable	44
<b>S/T Favorable</b>	<b>74</b>
• Plutôt défavorable	14
• Très défavorable	11
<b>S/T Défavorable</b>	<b>25</b>
• Ne se prononce pas	1

#### 2/ Opinion à l'égard de la constitution d'un fichier informatique national des empreintes digitales

Question : pour mettre en œuvre cette mesure, le ministère de l'intérieur prévoit de constituer un fichier informatique national des empreintes digitales. Laquelle de ces deux opinions se rapproche le plus de la vôtre ? Constituer un fichier informatique national des empreintes digitales...

Base : à tous

	<i>Pourcentage (%)</i>
• Est une mauvaise chose car cela constitue une atteinte à la liberté individuelle	23
• Est une bonne chose car cela permettra de lutter plus efficacement contre les fraudes à l'identité	75
• Ne se prononce pas	2
Total	100

### **3/ Opinion à l'égard du caractère obligatoire de la future carte**

Question: laquelle de ces deux opinions se rapproche le plus de la vôtre? La future carte d'identité électronique devrait être...

Base : à tous

	<i>Pourcentage (%)</i>
• Obligatoire car cela garantit une réelle diminution des fraudes	69
• Facultative comme c'est le cas actuellement de la carte d'identité	30
• Ne se prononce pas	1
Total	100

## **Les autres publications du Forum des droits sur l'internet**

**19 mai 2005 – Deuxième rapport sur la cyber-consommation «Les paiements sur Internet»**

<http://www.foruminternet.org/publications/lire.phtml?id=906>

**2 novembre 2005 – Guide «Je blogue tranquille»**

<http://www.foruminternet.org/publications/lire.phtml?id=948>

**17 novembre 2005 – Guide «Achats en ligne, suivez le guide...»**

<http://www.foruminternet.org/publications/lire.phtml?id=946>

**13 décembre 2005 – Dossier «Comprendre le projet de loi sur le droit d'auteur et les droits voisins dans la société de l'information»**

<http://www.foruminternet.org>

Troisième partie

# **La médiation**



## Bilan d'activité 2004-2005

Le Forum des droits sur l'internet a souhaité apporter sa contribution à l'instauration d'une plus grande confiance dans l'usage de l'internet, qu'il soit commercial ou privé, en mettant en place, en septembre 2004, un service de médiation chargé de traiter les différends liés à l'internet.

Ce service est l'aboutissement d'une longue et riche réflexion menée, dès 2001, par le Forum des droits sur l'internet sur «*Les modes alternatifs de règlement des différends*». Une des pistes d'action du Rapport<sup>343</sup>, issu de cette réflexion, était de travailler «à la mise en place d'une structure opérationnelle de résolution des différends liés aux litiges en ligne». De 2003 à 2004, le Forum a donc expérimenté une plate-forme électronique d'échange permettant la résolution à distance des litiges de l'internet. Cette expérimentation s'est révélée très positive et c'est naturellement que le Forum a ouvert son service au grand public le 16 septembre 2004.

Le service prend en charge les conflits liés à l'usage de l'internet et impliquant au moins un particulier. Il doit s'agir de problèmes juridiques et non techniques. Il s'adresse aux personnes dont les démarches préalables pour régler leur différend n'ont pas abouti. Respectant en cela les Recommandations communautaires de 1998 et 2001<sup>344</sup>, son rôle est celui d'un tiers indépendant et impartial garant de l'établissement d'un dialogue serein ayant pour objectif de résoudre à l'amiable les différends.

Le Forum des droits sur l'internet est très attaché aux principes fondamentaux de la médiation que sont notamment le dialogue, la concertation entre les acteurs, la recherche de solution en équité... Ces principes sont clairement énoncés dans le règlement de médiation du service<sup>345</sup>. Ils sont également à la base de sa méthode de travail : la «corégulation» qui réunit acteurs publics et acteurs privés autour d'une même table pour agir en commun sur les questions de droit et d'usage de l'internet.

Le service de médiation du Forum fait partie de ces nouveaux lieux et de ces nouvelles formes de régulation des conflits. Il ne réinvente pas les principes de la médiation ; il les adapte à un nouvel univers, celui de l'internet. Il s'inscrit, à ce titre, comme un mode d'action complémentaire de l'ensemble des outils déjà à la disposition des acteurs pour résoudre les conflits sur le réseau.

Le premier bilan du service de médiation, arrêté en décembre 2005, après plus d'un an d'existence, est extrêmement encourageant. Il démontre que dans le secteur des communications en ligne, un certain nombre de demandes peuvent être utilement traitées par la voie d'un tel recours extra judiciaire.

---

343. Rapport du Forum des droits sur l'internet, «*Les modes alternatifs de règlement des litiges*», 17 juin 2002. Disponible en ligne :

<http://www.foruminternet.org/telechargement/documents/rapp-mard-20020617.html>

344. La première, en date du 30 mars 1998/257/CE porte sur l'ensemble des modes alternatifs. La seconde, du 4 avril 2001, 2001/310/CE ne porte que sur les modes alternatifs relatifs aux conflits de consommation.

345. V. annexe 2 p. 299.

En outre, au-delà de l'originalité de chaque affaire examinée, ce service assure un « retour terrain » très instructif des secteurs d'activité en ligne, qu'il s'agisse de la vente, de la fourniture d'accès internet ou des échanges non commerciaux sur le réseau. L'ensemble des informations recueillies et anonymisées permet au Forum des droits sur l'internet d'alimenter la réflexion de ses groupes de travail et de formuler, le cas échéant, des recommandations.

## Bilan quantitatif du service

### Les chiffres clés du service

De septembre 2004 à décembre 2005, le service de médiation du Forum des droits sur l'internet a reçu un total de 5 495 demandes de médiation. Sur ce total, et après examen de chaque cas, 3 122 ont été déclarées recevables, soit 56,8 %, et 2 373 irrecevables, soit 43,2 %.

Les demandes émanent en très grande majorité de particuliers français. Toutefois, quelques demandes sont présentées par des internautes étrangers ayant un litige avec une entreprise française. Certaines de ces demandes ont été adressées par le Centre européen des consommateurs de Kehl (<http://www.euroinfo-kehl.com>).

Par ailleurs, les demandes concernent une très grande majorité d'entreprises françaises (98 % des demandes). Pour les cas impliquant une entreprise étrangère en Europe ou hors Europe, le service a eu de très grandes difficultés à engager une médiation, l'entrée en contact avec ces entreprises s'avérant bien souvent impossible.

Selon le règlement de médiation<sup>346</sup>, le service est compétent pour traiter des différends liés à l'internet et impliquant au moins une personne physique. Dans ce cadre, trois grands types d'affaires ont été traités :

- les différends qui mettent en relation un internaute avec une entreprise (*Business to Consumer – BtoC*) ;
- les différends qui font intervenir deux internautes<sup>(347)</sup> dans le cadre d'une relation commerciale (*Consumer to Consumer – CtoC*), ceci représente notamment les transactions sur des plates-formes de mise en relation (comme les sites d'enchères en ligne) ;
- et, les différends entre deux particuliers, hors relations commerciales (*Person to Person – PtoP*).

Les affaires « BtoC » constituent la très grande majorité des demandes de médiation (91 %).

Les affaires « CtoC » représentent, quant à elles, 6 % des demandes et les affaires « PtoP » représentent 3 % de l'activité du service.

---

346. V. annexe 2 p. 299.

347. Les différends faisant intervenir un vendeur professionnel sur une plate-forme de mise en relation sont intégrés à la catégorie « BtoC ».

Bien que chaque cas présente un caractère d'originalité, il a été possible d'établir, pour une facilité de traitement, une nomenclature précise de chaque grand type d'affaires.

Il existe deux grands types d'affaires «BtoC» :

–les affaires d'«achat par internet», dites «API», celles-ci confrontent généralement un consommateur à un cyber-marchand agissant à titre professionnel. Ces demandes sont la plupart du temps liées à l'achat d'un bien ou d'un service en ligne. Il peut s'agir d'une non livraison d'un bien commandé ou encore de sa livraison avec un vice caché. Ces affaires représentent 61 % des cas «BtoC» traités ;

–les affaires de «fourniture d'accès internet», dites «FAI», qui opposent un consommateur à un fournisseur d'accès à internet. À titre d'exemple, il peut s'agir de questions relatives aux conditions de conclusion d'un contrat avec un fournisseur d'accès à internet ou encore aux conditions du passage d'un abonnement bas débit à un abonnement haut débit. Ces affaires «FAI» représentent 39 % des cas «BtoC» traités.

Pour les différends rencontrés par les internautes lors d'un achat par internet (affaires «API» précitées), les différends les plus couramment rencontrés concernent la non réception des biens. Ce phénomène peut s'expliquer, d'une part, par une gestion des stocks à flux tendus dans certains cas et, d'autre part, par la perte ou le vol des colis pendant la phase de transport. Les autres sources majeures de difficulté se situent au niveau du remboursement de la commande et des commandes incomplètes.

Pour les différends liés à la fourniture d'accès, 41,89% des problèmes rencontrés sont des problèmes de résiliation de contrat. À titre d'exemple, il peut s'agir de demandes de résiliation anticipée de contrat, lorsque le service proposé ou le tarif appliqué par l'opérateur n'est plus jugé attractif par l'abonné, ou encore lorsque le service est devenu indisponible pour des raisons d'ordre technique. Ces demandes de résiliation concernent également des offres dites «*sans engagement de durée*» lorsque les abonnés contestent l'application de frais de résiliation<sup>348</sup>.

Au même titre que les différends impliquant une entreprise vendant sur internet, les contestations issues des affaires «CtoC» portent principalement sur des biens non reçus.

Souvent, le particulier – vendeur sur un site de mise en relation – ne va pas faire parvenir son produit par colis suivi afin de minimiser les coûts de transport. Par ailleurs, il s'avère que certains vendeurs ne sont pas suffisamment précautionneux pour emballer le bien vendu. Il est alors fréquent de voir le produit arriver endommagé chez l'acheteur (9%).

Par ailleurs, de nombreux internautes reçoivent des biens qui ne correspondent pas réellement à la description faite par le vendeur sur le site de mise en relation (12%).

Des problèmes apparaissent également en cas d'échec de la transaction entre un vendeur et un acheteur, lorsque, par exemple, ce dernier se rétracte. Il arrive, en

---

348. Le service de médiation, en ce qui concerne les problèmes de fourniture d'accès internet, est en contact régulier avec six entreprises qui représentent 81,4 % du marché ADSL en France.

effet, que le vendeur se voit néanmoins réclamer par le site de mise en relation une commission sur le prix de vente (7 %) <sup>349</sup>.

Concernant enfin les relations non commerciales entre particuliers, les litiges touchent essentiellement l'atteinte à la vie privée (32 %) et 26 % concernent des demandes de retrait de contenus considérés comme diffamatoires ou injurieux.

Les problèmes liés à la vie privée portent, la plupart du temps, sur le retrait d'informations à caractère personnel ou de photographies de la personne, diffusées sans son autorisation.

Concernant les problèmes liés aux droits d'auteur, il s'agit essentiellement de la mise en ligne de contenus sans autorisation préalable de leur auteur (21 %).

Les problèmes liés aux noms de domaine – autres que les .fr <sup>350</sup> – représentent également une part non négligeable des affaires traitées par le service (12 %).

## Profil des utilisateurs et montant des différends

En février 2005, le Forum des droits sur l'internet a fait réaliser, par un cabinet d'étude indépendant, un audit du service auprès de 500 internautes utilisateurs.

Le portrait-robot de l'utilisateur est celui d'un homme de 40 ans, cadre ou ingénieur, qui surfe depuis 6 ans sur le web, une douzaine d'heures par semaine, qui a réalisé une demie douzaine d'achats en ligne en 2004 et a déjà rencontré un litige dans sa vie d'internaute.

Pour l'instant, un utilisateur sur quatre est une femme. Les jeunes de moins de 25 ans sont rares (10 %), la tranche 26-45 ans agrège la moitié des effectifs. Un utilisateur sur sept est retraité mais seulement un sur vingt est étudiant.

Toutes les catégories socioprofessionnelles sont représentées mais les catégories supérieures dominent.

Les pratiques internet du panel sont très intensives. Plus de deux heures d'internet par jour pour 40 % de celui-ci; et pour un tiers plus de dix achats en ligne par an, pour un autre tiers plus de sept ans de pratique ou encore pour un tiers toujours, plus de deux litiges rencontrés.

En conclusion, le service a été, pour sa première année, face à un public d'internautes actifs et rodés au web.

Près d'un utilisateur du service sur trois est un internaute de longue date.

En ce qui concerne, le montant des différends, si certains des cas soumis au service n'ont pas directement de valeur pécuniaire, notamment pour les différends de parti-

---

349. La commission est payée par le vendeur à l'exploitant de la plate-forme. Elle correspond généralement à un pourcentage du montant de la transaction effectuée via la plate-forme de mise en relation.

350. L'AFNIC (Association Française pour le Nommage Internet en Coopération) a mandaté le CMAP (Centre de médiation et d'arbitrage de Paris) pour régler les différends liés aux noms de domaine en .fr.

culier à particulier, pour les autres, les montants se répartissent en quatre quarts relativement équilibrés allant de moins de 50 € (19 %), de 50 à 119 € (31 %), de 120 à 299 € (25 %) et plus de 300 € (25 %).

Certaines affaires peuvent même représenter un montant très élevé. À titre d'exemple, le service a effectué des médiations mettant en jeu des sommes allant de 2 500 € à 4 000 €.

Ces chiffres témoignent de la confiance désormais acquise par un certain nombre d'internautes dans les achats en ligne ce qui peut les conduire à des achats de valeur. Ceux-ci concernent essentiellement des produits liés aux nouvelles technologies (ordinateur, appareil photo numérique, écran plasma...), ainsi que du gros électroménager (réfrigérateur, machine à laver...) ou des voyages. Par ailleurs, s'agissant des différends liés à la fourniture d'accès à internet, il n'est pas rare que les montants soient supérieurs à 300 €; il s'agit essentiellement d'affaires portant sur la résiliation du contrat ou sur la facturation du modem.

## Efficacité du service

L'activité de médiation du Forum des droits sur l'internet expose directement son service de règlement des différends à des personnes en conflit. Celles-ci, en s'adressant au service, nourrissent des attentes de traitement efficace de leur dossier et de résolution rapide de leur problème.

Cette mission souvent délicate a mobilisé l'ensemble de l'équipe qui a travaillé à la mise en place de procédures lui permettant de répondre à l'ensemble des attentes tout en faisant face à une forte demande.

En décembre 2005, 1 614 affaires recevables avaient été traitées et étaient clôturées. Sur ces 1 614 affaires, 1 437 avaient été résolues à l'amiable, ce qui représente un taux de réussite de 89 %.

177 affaires ont été clôturées sur un constat de défaut d'accord entre les parties. 166 de ces affaires concernaient des cas « BtoC » (dont 64 % d'affaires « API » et 36 % d'affaires « FAI »), les autres cas se répartissant équitablement entre des affaires « CtoC » et « PtoP ».

Ce taux de réussite est extrêmement encourageant et démontre que la médiation peut être une manière efficace de régler certains types de différends.

Toutefois, ce taux de réussite ne doit pas occulter les difficultés rencontrées en amont du règlement des affaires. En effet, il convient de mentionner que le service est confronté à un nombre important d'irrecevabilités (43,2 % des demandes faites au service). Celles-ci intègrent, outre les demandes qui n'entrent pas dans le champ de compétence du service ou les demandes d'information (près de 2 % des demandes), les refus des parties contactées d'entrer dans la médiation (plus de 8 %). Ces refus peuvent être explicites, il s'agit d'entreprises indiquant clairement ne pas vouloir engager de processus de médiation avec leurs clients par l'intermédiaire du service. Ces cas sont extrêmement rares. Le service est le plus souvent confronté à des refus implicites des entreprises qui, malgré les multiples contacts tentés sous différentes formes restent silencieuses n'opposant jamais un refus clair à l'égard du processus

de médiation. Parmi ces entreprises, certaines vont recueillir sur la plate-forme technique, grâce à l'identifiant et au mot de passe qui leur sont communiqués, les informations qui leur sont utiles (en l'occurrence des éléments d'identification de leurs abonnés) afin de traiter en direct avec eux. Ces types de comportements dilatoires, voire manipulateurs, prennent beaucoup de temps au service et aboutissent, au final, à un constat d'impossibilité d'enclencher le processus de médiation. Une meilleure diffusion de la « culture » de la médiation au sein des entreprises peut contribuer à diminuer progressivement ce chiffre de 8 %.

Le service a une durée moyenne de traitement pour les affaires qui lui ont été soumises entre janvier et décembre 2005 (*i.e.* hors période de mise en place des processus de traitement) inférieure à trois mois dans 63 % des cas. L'objectif du service est d'améliorer cette durée de traitement grâce notamment à la poursuite de la désignation de correspondants au sein des entreprises avec lesquelles il est en contact.

En décembre 2005, le service de médiation a une vingtaine de correspondants ce qui permet un traitement rapide et efficace des dossiers.

Toutefois, un point faible a été constaté concernant les difficultés de prise de contact avec certaines entreprises installées sur le web (« *pure players* »). Ces difficultés peuvent être dues à des identités incomplètes ou à des points de contact défaillants. Ainsi, outre la question du numéro de téléphone surtaxé, dont les internautes se plaignent du temps d'attente avant d'obtenir un interlocuteur, les clients sont souvent confrontés à des boîtes vocales ou des numéros de télécopie. Le contact par le biais du formulaire en ligne où il faut décrire son problème se répand également.

Si certaines entreprises se manifestent rapidement après avoir été contactées par ces différents modes, beaucoup d'autres vont rester silencieuses.

Face à cette situation d'évitement, le service de médiation perd beaucoup de temps et d'énergie; relancé par les parties demanderesses, il doit, au bout de quelques semaines, renoncer à entamer un processus de médiation et déclarer ces affaires irrecevables.

Bien évidemment, ces attitudes ralentissent considérablement les dossiers et agacent les internautes qui saisissent le service.

Au fil des mois, le service s'est adapté à ces comportements et déclare désormais irrecevables les affaires impliquant certaines de ces entreprises défaillantes dans la prise de contact afin de permettre à l'internaute de se tourner vers d'autres voies de recours.

Un audit du service a été réalisé en février 2005 par un cabinet d'étude afin de mesurer le degré de satisfaction des utilisateurs du service.

De façon générale, la satisfaction des internautes à l'égard du service est tout à fait encourageante.

Le service, via sa plate-forme technique, est considéré comme facile d'utilisation par une majorité d'utilisateurs. Le processus de médiation détaillé dans la présentation en ligne du service est trouvé clair par les internautes.

La plus-value humaine apportée par l'équipe qui prend en charge les demandes est souvent soulignée.

Une majorité d'internautes (87 %) dont la demande a été déclarée irrecevable se montre, quant à elle, insatisfaite de la prestation.

Une deuxième enquête a été menée par le même cabinet d'étude, en mars 2005, auprès cette fois d'un échantillon d'une vingtaine d'entreprises avec lesquelles le service de médiation était en contact.

Cette étude révèle une satisfaction globale des entreprises à l'égard du service. Toutefois, au niveau du principe même de la médiation, certaines d'entre elles se montrent préoccupées par la mise en place d'un nouveau guichet d'accueil des réclamations.

Mais cette étude révèle aussi qu'un certain nombre d'entreprises du panel réfléchissent à des formules de partenariat sur mesure avec le service comme, par exemple, l'apposition d'un label faisant état de leur recours à la médiation comme gage de sécurité supplémentaire pour le client.

## Comportements à risque

Internet, comme tout secteur en forte expansion, n'échappe pas à certains comportements en marge du droit ou des bonnes pratiques.

Si ces cas restent marginaux – environ 150 affaires de ce type répertoriées par le service de médiation – il convient, néanmoins, de les décrire afin d'attirer la vigilance de chacun sur ces pratiques. Le service de médiation, pour sa part, a déclaré irrecevables ces affaires et a renvoyé les internautes vers les autorités compétentes comme l'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication) ou la BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information) ou encore la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes).

Le problème des « *dialers* » arrive en tête. Il s'agit de kits de connexion à télécharger par les internautes pour accéder à certains contenus payants disponibles sur un site (contenus pornographiques, logiciels...). Ces programmes informatiques sont des outils de micropaiement permettant à l'utilisateur d'un service d'accéder à certains contenus sans qu'il ait besoin de s'abonner ou d'effectuer un paiement par carte bancaire. En pratique, lorsque le programme est installé sur la machine de l'internaute, il va composer bien souvent à son insu un numéro de téléphone surtaxé et non compris dans les abonnements des fournisseurs d'accès à Internet. L'internaute sera, par la suite, directement facturé par son opérateur téléphonique.

Plusieurs problèmes peuvent dès lors apparaître :

- si l'internaute se trouve connecté à l'internet via un numéro appelant l'étranger, le surcoût risque d'être très important (plusieurs milliers d'euros) ;
- si l'internaute ne se déconnecte pas de l'internet, il est susceptible de poursuivre sa navigation sur d'autres sites avec la même connexion surtaxée.

Le fait que ce procédé soit très souvent utilisé à l'insu des internautes génère beaucoup de mécontentement.

La médiation est très difficile pour ce type d'affaire car la plupart des interlocuteurs contactés ne s'estiment pas responsables de cette pratique.

Autres cas rencontrés, **les fraudes des vendeurs qui refusent les « tiers de confiance agréés »**<sup>351</sup>. En règle générale, les sites qui permettent la mise en relation de personnes souhaitant acheter ou vendre des biens sur internet conseillent, pour diminuer le risque de fraude, à leurs utilisateurs de recourir à des services de tiers de confiance agréés qui garantissent le paiement du prix au vendeur. Cependant, il arrive que des vendeurs mal intentionnés refusent sciemment de passer par ces services de tiers de confiance, préférant notamment un règlement par virement bancaire, par chèque ou en argent liquide. Dans ce type de cas, l'acheteur s'expose à ne pas recevoir le produit commandé et à se trouver face à un vendeur qui ne répond plus à ses courriers. Il est, par ailleurs, souvent constaté que le produit est remis en vente quelque temps plus tard, sur le même site et par le même vendeur, qui aura entre-temps changé de pseudonyme.

Le service a également été témoin de **faux sites de tiers de confiance**. Sur des sites de mise en relation, certains acheteurs peuvent proposer un prix supérieur aux vendeurs à condition de réaliser la transaction en dehors du site de mise en relation et de recourir à un site de tiers de confiance qui, généralement, est un faux site créé par l'acheteur lui-même. Le vendeur reçoit alors un courriel de ce faux tiers de confiance qui lui confirme que le montant de la vente lui a bien été versé et que cette somme lui sera reversée dès la confirmation de la livraison du produit. Le vendeur mis en confiance par cette manœuvre, livre le bien à l'adresse indiquée mais il ne reçoit plus aucune nouvelle du vendeur et du faux tiers de confiance.

Le service a reçu des **demandes d'internautes français ayant acheté des cigarettes ou des médicaments en ligne**. Or, la vente de tels produits est une activité strictement réglementée par le Code de la santé publique. De même, le code de la consommation n'autorise en ligne que les paris et loteries gratuits.

Quelques cas de **« scam nigerian »** ont été présentés. Il s'agit d'une escroquerie financière pratiquée via le spam. Le message envoyé est signé par une personne se présentant comme un officiel ou un proche d'un officiel d'un pays étranger. Il est demandé à l'internaute de l'aider à sortir du pays une grosse somme d'argent ou un bien de valeur qui se trouve bloqué pour une raison quelconque (changement de gouvernement, guerre civile, etc.). Il est alors promis à l'internaute qu'en contrepartie de son aide, il recevra une commission très importante (entre 15 et 50 % du montant qui se chiffre en millions de dollars). L'objectif de cette escroquerie est d'inciter l'internaute, soit à communiquer son numéro de compte bancaire, soit à lui soutirer de l'argent à titre d'avance pour les frais prétendument engendrés pour cette opération (honoraires d'avocats, frais de douane, taxe fiscale...).

Par ailleurs, des cas de **« phishing »** ont été identifiés. Des internautes reçoivent un courriel « de leur banque » leur indiquant qu'à la suite d'un problème informatique, ils doivent se rendre sur le site de la banque pour communiquer à nouveau leurs

---

351. Le rôle de ce tiers est d'assurer un séquestre financier des sommes versées par les acheteurs.



données bancaires (numéro de compte bancaire, numéro de carte bancaire etc.). En réalité, le lien figurant dans les messages envoyés aux internautes les renvoie vers un faux site où toutes les données sont recueillies à des fins délictuelles.

Enfin, des cas de «**vente pyramidale**» ont fait l'objet de demandes de médiation. Il s'agit d'un système de distribution de produits dans lequel des participants gagnent un revenu en fournissant les mêmes produits à d'autres participants qui, à leur tour, font des profits de la même manière. C'est donc un système par lequel une personne qui désire commercialiser un produit vend à des «gérants» ou «distributeurs» des titres leur donnant le droit de recruter d'autres personnes pour leur vendre, à leur tour, des titres semblables. Chaque membre d'un tel réseau verse une somme d'argent à celui qui l'a recruté (qui en reverse une partie à son propre recruteur). Une telle pratique est illégale en France.

## **Le déroulement de la médiation**

L'ensemble des chiffres présentés l'atteste, le service de médiation du Forum des droits sur l'internet a été, pour sa première année d'existence, fortement sollicité. Il a pu gérer un tel volume d'affaires grâce à des procédures de travail très précises couplées à l'usage d'une plate-forme logicielle créée spécifiquement pour le service.

Une des particularités du service de médiation du Forum des droits sur l'internet est de traiter des cas liés à l'internet avec l'outil internet lui-même. En effet, le service s'appuie sur une plate-forme logicielle sécurisée élaborée spécifiquement pendant près de trois ans. Le service n'exclut toutefois pas les traitements plus classiques par courriers postaux et rencontres physiques.

Le processus de traitement d'une affaire par le service de médiation du Forum des droits sur l'internet est organisé en cinq étapes principales que sont la saisine, la recevabilité, le complément d'information, la médiation et la clôture.

L'ensemble de ces étapes est décrit dans le document de référence du service, son règlement de médiation.

Ce processus est mis en place par une équipe interne au Forum des droits sur l'internet qui s'appuie également sur des ressources externes.

### **Un processus de traitement en cinq étapes**

Le service de médiation peut être saisi de deux façons : par voie électronique ou par voie postale.

L'internaute accède, via le site <http://www.mediateurdunet.fr>, d'un simple clic au formulaire de pré-inscription situé en haut à droite de son écran.

#### **Saisine**

Sur ce formulaire de pré-inscription, la partie va donner des informations permettant de l'identifier et de connaître son différend ainsi que les démarches préalables déjà accomplies. Son nom, son téléphone ainsi que son adresse électronique sont des

champs qui devront obligatoirement être renseignés. Ces informations sont indispensables pour contacter la personne, notamment dans le cas où l'adresse électronique indiquée serait invalide.

La personne qui ne dispose d'aucun accès internet et d'aucune adresse électronique a la possibilité de soumettre son différend au service de médiation par voie postale à l'adresse du Forum des droits sur l'internet.

À réception du courrier postal, le service prend contact avec l'expéditeur pour lui demander s'il dispose d'un accès internet et d'une adresse électronique.

Sur plus de 5495 demandes soumises au service, seules 207 de celles-ci ont été présentées par voie postale. 110 de ces cas ont été traités hors plate-forme, les autres ont pu être rebasculés sur la plate-forme.

Une fois l'inscription en ligne effectuée par la partie, le service accuse réception de la demande par l'envoi d'un message électronique.

Si le message ne peut être délivré, c'est que l'adresse n'est pas valide. La personne sera alors contactée téléphoniquement par le service pour rétablir la bonne adresse.

## **Recevabilité de la demande**

Cette étape d'identification franchie, le service va étudier la recevabilité de la demande et veiller à ce que les critères fixés par le service dans son règlement de médiation soient remplis.

Le descriptif du différend doit suivre un formalisme très précis. Pour ce faire, la partie va être guidée sur la plate-forme.

La demande doit notamment contenir la date du différend. L'indication de celle-ci permet de vérifier que la prescription d'une éventuelle action en justice est suffisamment éloignée de la date de saisine du service, pour que ce dernier puisse mener à bien le processus de médiation sans entraver la possibilité d'un recours devant le juge.

Une autre condition est fondamentale. Il convient pour l'internaute d'avoir mené les démarches préalables auprès de l'autre partie pour tenter de résoudre son différend. Ce n'est que si cette démarche n'a pas abouti qu'une médiation peut être lancée.

Au cours de cette première année d'exercice, le service a été de plus en plus vigilant à faire respecter cette condition.

Le nom de l'autre partie, ainsi que ses coordonnées, et toutes les informations nécessaires à son identification client doivent être fournies (numéro de commande, numéro de compte client, numéro de ligne ADSL pour les différends avec une entreprise). Ces dernières informations sont primordiales, car si un processus de médiation est engagé, il ira beaucoup plus vite avec des parties clairement identifiées.

Toute demande incomplète est déclarée irrecevable. Dans cette hypothèse, un message est envoyé à l'internaute l'invitant, s'il le souhaite, à saisir une nouvelle fois le service, via le formulaire de pré-inscription, en reformulant sa demande complétée des informations manquantes.

Le règlement de médiation impose que la personne qui saisit le service soit majeure et de bonne foi.

Il faut également qu'elle ait un intérêt direct à agir. Une personne ne peut se faire représenter. Le service de médiation requiert une participation active, directe et volontaire de la partie qui le saisit.

À partir de là, il s'agit de vérifier que la demande relève bien du champ de compétence du service. Si tel n'est pas le cas, la demande ne pourra être prise en charge, elle sera déclarée irrecevable.

Le service prend en charge les différends liés directement à l'internet, c'est-à-dire impliquant son usage et bien évidemment seule une demande décrivant un réel différend a vocation à être traitée.

Toutes les demandes portant sur de la simple information sont réorientées vers le service d'information pratique à destination du grand public du Forum des droits sur l'internet, DroitDuNet.fr (<http://www.droitdunet.fr>). Le site est constitué de fiches pratiques permettant aux internautes de trouver des réponses à leurs questions.

Le service ne prend pas en charge :

- les demandes indiquant qu'une action en justice a été engagée ;
- les demandes qui mettent en cause deux professionnels ;
- les demandes relatives à un nom de domaine en .fr. Le service n'a pas vocation à se substituer aux structures existantes mais à être complémentaire de celles déjà constituées. Le service ne prend donc pas en charge les différends liés aux noms de domaine en .fr ; l'AFNIC (Association française pour le nommage internet en coopération) ayant mandaté le CMAP (Centre de médiation et d'arbitrage de Paris) pour traiter ce type de différend ;
- les demandes relevant d'une infraction pénale. La vente d'objets contrefaits ou de cigarettes ainsi que l'incitation à la haine raciale ou la pédo-pornographie sont autant d'exemples pour lesquels le service de médiation ne peut intervenir pour se substituer à une action judiciaire ici indispensable ;
- les problèmes techniques : dégroupage total ou partiel, dysfonctionnement du modem, déconnexions intempestives... Le service n'a pas de compétence pour intervenir dans ces cas précis et renvoie les internautes vers les organismes compétents pour agir ;
- les différends de masse. Le service a pu, au regard de sa pratique, définir le différend de masse comme un problème identique rencontré par de très nombreux internautes avec un même prestataire ; dans ce cas, le fait générateur est identique. À titre d'exemple, il peut s'agir d'une modification des clauses d'un contrat par un prestataire touchant l'ensemble ou partie de ses abonnés ou encore d'une non-livraison en masse d'un bien promis dans le cadre d'une difficulté d'approvisionnement de l'entreprise. Ces demandes sont toutes identiques et ne présentent pas les caractères d'originalité et d'individualité indispensable pour entamer un dialogue exclusif et confidentiel entre deux parties ;
- les demandes faisant état d'une impolitesse, de faits inexacts ou de mauvaise foi flagrante de la part de l'une ou de l'autre des parties. Ces comportements ne sont pas acceptables car ils sont contraires à l'esprit de la médiation qui doit mener à l'instauration d'un dialogue serein entre les parties.

Une fois l'affaire examinée suivant la grille de critères ci-dessus décrite, un message est envoyé à la personne qui a soumis son différend. Ce message peut exprimer, soit un refus, soit la prise en charge de la demande par le service.

L'irrecevabilité de l'affaire est expliquée. Si le service n'est pas compétent, il indiquera, dans la mesure du possible, les organismes vers lesquels la partie peut s'adresser. Il peut s'agir des associations de consommateurs, des DDCCRF (Directions départementales à la concurrence, à la consommation et à la répression des fraudes), de l'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication), de l'ARCEP (Autorité de régulation des communications électroniques et postales), du BEFTI (Brigade d'enquêtes sur les fraudes aux technologies de l'information), des services publics ou encore du juge.

La prise en charge de l'affaire génère l'envoi d'un message automatique indiquant à l'internaute la marche à suivre pour continuer le processus de médiation. Un identifiant et un mot de passe lui sont alors communiqués pour lui permettre d'accéder aux fonctionnalités de la plate-forme.

## **Complément d'information**

L'étape de la recevabilité étant franchie, un complément d'information va être demandé afin de renseigner de façon encore plus complète l'affaire.

Ce complément doit être effectué par l'internaute dans les sept jours de la prise en charge de son affaire. S'il n'était pas transmis dans ce délai, le dossier serait clôturé.

Le complément d'information se présente sous la forme d'un questionnaire en cinq étapes, destiné à recueillir des informations plus précises sur la demande. Il est l'occasion pour l'internaute de joindre à son dossier tout document utile.

Outre la reprise des informations déjà délivrées dans la première étape de recevabilité, ce complément d'information va permettre à la partie demanderesse d'exprimer clairement ce qu'elle souhaite obtenir de l'autre partie. Cette demande servira de référent tout au long du processus. Il conviendra à la partie de ne pas la redéfinir de façon extensive en cours de processus.

Fort de l'ensemble de ces renseignements, le service de médiation du Forum des droits sur l'internet va pouvoir établir un contact avec l'autre partie et, si celle-ci accepte l'offre de médiation, enclencher le processus de médiation

## **Déroulement de la médiation**

Il convient d'établir désormais un contact avec l'autre partie. Ce premier contact s'effectue généralement par voie électronique. Le courriel présentant l'activité du service invite à se rendre sur le site internet <http://www.mediateurdunet.fr> pour avoir des informations sur le service et pour prendre connaissance du règlement de médiation. Un résumé de la demande de la partie requérante lui est également transmis. Des échanges téléphoniques peuvent précéder ou suivre ce courriel de prise de contact afin d'apporter toutes les précisions nécessaires dans le cadre de la participation de cette partie au processus de médiation.

L'acceptation par l'autre partie du processus de médiation marque le point de départ de la médiation. Un délai de trois mois commence alors à courir, pendant lequel les parties vont tenter avec l'aide du service de trouver une solution amiable à leur différend. En acceptant de participer au processus, la seconde partie s'engage à respecter les mêmes obligations que celles incombant à la partie demanderesse (confidentialité, diligence, courtoisie, politesse, etc.).

Le service de médiation est un facilitateur de dialogue entre les parties. Tout au long du processus, il sera l'interlocuteur privilégié des parties. Il les tiendra informées de l'évolution de leur affaire. Il sera le relais indispensable entre elles et transmettra tous les éléments utiles à l'avancement du dossier.

Ces échanges sont menés via la plate-forme sécurisée. Les parties y accèdent grâce à leur identifiant et leur mot de passe confidentiels. Cette plate-forme est dotée de trois fonctionnalités essentielles. Tout d'abord, un *agenda* personnalisé, véritable tableau de bord, qui permet aux utilisateurs qui se connectent à la plate-forme de connaître ou de retrouver tous les événements importants survenus au cours du processus de médiation. Ensuite, un *espace de dialogue*, cœur du dispositif, qui permet aux parties en présence du médiateur d'échanger entre elles et, éventuellement, de faire des propositions de règlement de leur différend, de nouvelles pièces peuvent également être apportées au dossier. Si cela se révèle utile au processus de médiation, il est également possible de dialoguer en direct grâce à une « *chat room* ». L'ensemble de ces échanges reste strictement confidentiel. Le règlement de médiation prévoit que toute personne associée au processus de médiation s'engage pendant et après le processus à ne pas révéler ou utiliser comme preuve ou d'aucune autre manière que ce soit les informations, opinions, suggestions, aveux ou propositions présentés par les parties et par le service au cours du processus de médiation. Enfin, un *module de messagerie* permet un échange bilatéral des parties vers le médiateur. Ainsi, la partie qui désire communiquer des éléments d'information confidentiels au seul médiateur, sans que l'autre partie puisse en prendre connaissance, peut adresser un message électronique depuis ce module de messagerie.

## **Clôture de l'affaire**

L'ultime étape de ce processus est la clôture de l'affaire. La médiation prend fin lorsqu'un accord est trouvé entre les parties ou *a contrario*, s'il est constaté par le service que les positions respectives des parties sont irréductibles et ne pourront pas évoluer vers un règlement amiable. Elle prend également fin en cas de désistement des parties ou si une action en justice est engagée en cours de processus.

La finalisation d'un processus de médiation consiste pour le médiateur, après que les parties se soient chacune exprimées sur le fond, à synthétiser les arguments de celles-ci. Le médiateur joue ici, suivant les cas, soit un rôle « d'accoucheur », soit un rôle « d'aviseur » entre les parties et met en évidence le ou les points sur lesquels il y a accord ou désaccord. Les parties peuvent, à partir de cette synthèse, répondre une ultime fois aux arguments échangés en présentant de nouvelles pièces et, le cas échéant, revoir à la baisse leurs demandes initiales.

Le médiateur doit alors s'assurer que les nouveaux éléments versés par les parties sont bien utiles à la résolution du différend et, en cas d'accord, que la solution trouvée

est satisfaisante au regard de l'équité. Le médiateur s'assure, enfin, que chaque partie a pu disposer d'un délai de réflexion suffisant pour donner son accord.

À la fin du processus de médiation, le médiateur rédige un compte rendu qui décrit l'accord de règlement amiable et, éventuellement, les modalités de son exécution. Ce compte rendu n'a aucune force contraignante; il ne peut pas être assimilé à une transaction, sauf accord en ce sens des parties.

Le service a vu, pour une trentaine de cas de différends BtoC, revenir vers lui une partie pour non respect de l'accord. Pour ces affaires, un nouveau contact a été établi par le service avec la partie «défaillante» pour connaître les raisons de cette inexécution et lui rappeler les engagements pris à l'issue du processus. À l'exception d'un cas, les parties après ce contact ont mis en œuvre l'accord. La raison du retard ne résidait pas dans une volonté de non exécution mais dans des démarches internes lourdes.

## Règlement de médiation

Le service de médiation du Forum des droits sur l'internet publie sur son site un règlement de médiation que le service et les parties s'engagent à respecter. Les principes de ce règlement résultent des travaux menés par le comité de suivi<sup>352</sup> qui a été mis en place à la suite du groupe de travail du Forum des droits sur l'internet sur les modes alternatifs de règlement des différends. Ce comité s'est réuni à de nombreuses reprises entre 2002 et 2003, accompagnant ainsi l'expérimentation du service lancée en mars 2003.

Le règlement de médiation s'inscrit pleinement dans l'esprit des Recommandations de la Commission européenne du 30 mai 1998 et du 4 avril 2001 sur les modes alternatifs de règlement des différends<sup>353</sup>.

Ce règlement apparaît en ligne, dès l'étape de la préinscription, où il est demandé aux internautes de prendre connaissance de celui-ci et de l'accepter afin de pouvoir continuer le processus.

Il met, tout d'abord, l'accent sur *l'importance des démarches préalables* qui doivent être accomplies par la partie requérante pour régler son différend. Ce n'est qu'en cas d'échec de ces démarches que le service de médiation pourra être saisi.

Il décrit, ensuite, avec la plus grande transparence les règles de saisine et le champ de compétence du service, les différentes étapes du processus de médiation et les modalités de l'accord final. La clarté de ces informations doit permettre d'obtenir le consentement éclairé des parties sur leur participation au processus de médiation.

Des principes essentiels sont rappelés. Tout d'abord, le *principe d'indépendance et d'impartialité* du service qui va garantir le traitement équitable de l'affaire; ensuite, le respect de la règle de la *confidentialité* des échanges et du respect de l'anonymat des

---

352. Ce comité réunissait un représentant du CNRS, de l'ISOC, de la CLCV, de l'AFA et du GBDe.

353. V. note 344.

parties qui va permettre à celles-ci de s'exprimer librement. Ces principes vont faciliter la recherche d'une solution amiable dans une affaire déterminée sans que cette solution soit érigée en exemple pour d'autres cas.

Les parties s'engagent, en outre, à respecter une certaine civilité lors des échanges car aucun dialogue ne peut sereinement s'instaurer entre les parties pour conduire à un accord amiable sans courtoisie, ni politesse. Si un écart de langage peut être toléré, tout manquement répété à cette obligation peut conduire à la clôture du processus de médiation.

Le règlement souligne également la démarche volontaire des parties qui ont la possibilité, à tout moment, de quitter le processus de médiation après en avoir informé le service.

Quant aux modalités de fin de processus, elles sont clairement décrites afin que les parties connaissent, dès le début de la médiation, la valeur de l'accord éventuellement obtenu.

## Organisation du service

L'équipe de médiation du Forum des droits sur l'internet est constituée de cinq personnes.

Le rôle de chaque membre de l'équipe de médiation est de prendre en charge le cas, dès sa soumission, en vérifiant le respect des critères fixés par le service. Il instruit l'affaire et porte une appréciation sur sa recevabilité. Dans l'hypothèse de l'éligibilité de celle-ci, il est chargé d'établir un contact avec l'autre partie via un courrier électronique, postal ou un appel téléphonique.

Chaque médiateur gère un pôle d'affaires (achats en ligne, fourniture d'accès internet, cas impliquant une partie étrangère...). Ce type d'organisation permet aux médiateurs de bien connaître les secteurs d'activité d'où les cas émanent ainsi que les parties avec lesquelles ils sont amenés à être régulièrement en contact.

Au cours de cette première année d'exercice, le service de médiation a établi au fil des mois des contacts réguliers avec les cyber-marchands et les fournisseurs d'accès à internet. Ces échanges réguliers basés sur le dialogue et la prise en compte des souhaits des uns et des contraintes des autres ont montré leur efficacité.

5 % des 460 entreprises répertoriées par le service regroupent près de 48 % des cas de BtoC.

Le service de médiation est donc confronté à deux situations: d'un côté, une petite quantité d'entreprises qui représentent près de la moitié des affaires BtoC du service; de l'autre, une kyrielle d'entreprises regroupant l'autre moitié. Dans ces conditions, les modalités de travail du service doivent s'adapter.

Sur les 460 entreprises avec lesquelles le service a engagé une médiation, 10 % d'entre elles ont désormais des correspondants en contact régulier avec le service de médiation. Ce dernier a adapté son mode d'action aux contraintes des entreprises. Avec certaines d'entre elles, des comptes rendus hebdomadaires sont faits sur les

affaires en cours, avec d'autres, ils sont bimensuels. Cette fréquence des contacts est dictée notamment par le volume d'affaires.

Le service se heurte, toutefois, à des difficultés importantes pour gérer les cas de la moitié des entreprises répertoriées avec lesquelles les contacts sont épisodiques, voire impossibles dans la durée. Ces entreprises n'ont généralement pas de service clientèle ou de personne qualifiée pour gérer les réclamations. La médiation s'avère bien souvent longue et les relances adressées à ces entreprises multiples.

Par ailleurs, certaines entreprises sont réticentes à utiliser pleinement la plate-forme de traitement des dossiers. En effet, celle-ci peut être vue comme concurrente de leur propre outil de gestion des plaintes et faire craindre un traitement « doublé » des dossiers.

Le service de médiation du Forum a compris qu'il était important pour les entreprises d'identifier rapidement les cas qui les concernaient. C'est la raison pour laquelle le service a amélioré les modalités de recevabilité au cours de l'année en demandant notamment à l'internaute de bien décrire les démarches préalables déjà effectuées auprès de l'entreprise, de fournir tous les éléments d'identification (n° de commande, n° de client) ainsi que les doubles ou triples saisines qui ont pu être effectuées (DDCCRF, juge...).

Il est, en effet, fondamental pour l'entreprise de connaître l'historique des démarches préalables réalisées dans le cadre d'une gestion rapide et efficace de ses affaires.

Les discussions régulières au cours de l'année entre les entreprises et le service de médiation ont permis de mettre au point des protocoles de gestion opérationnels qui devront encore s'approfondir.

Le service de médiation s'appuie également sur une équipe de *cinq médiateurs externes*, bénévoles, exerçant déjà une activité de médiation dans le cadre d'associations ou attachés à des centres universitaires (Association IRENE de l'ESSEC, CNAM...). Ces médiateurs sont surtout intervenus dans les différends entre particuliers et dans quelques différends commerciaux présentant un caractère de grande complexité.

En effet, ces différends sont très mobilisateurs. Les ressorts psychologiques de ces affaires sont lourds et le dialogue serein met du temps avant de s'instaurer. Il faut au médiateur généralement plusieurs semaines, voire plusieurs mois, avant d'aboutir à un règlement amiable.



## Conclusion

Le service de médiation du Forum des droits sur l'internet démontre après une année d'existence que la médiation et, plus particulièrement un mode en ligne de règlement des différends (*On Line Dispute Resolution – ODR*), peut être mis en place et régler des litiges de façon efficace.

Ce service de médiation respectant le principe d'indépendance et de neutralité a pu se développer au sein du Forum des droits sur l'internet, en harmonie avec la démarche de corégulation que celui-ci pratique depuis 2001. Celle-ci consiste à réunir, autour d'un thème de travail, des acteurs ayant des intérêts bien souvent divergents et permettre ainsi l'échange, le dialogue et la concertation dans un climat serein et productif.

Il démontre, également, que cet instrument de médiation répond aux besoins d'une époque qui cherche des outils de paix sociale permettant de renouer un dialogue rompu. Il agit comme interface de pacification raisonnant essentiellement en équité. Il offre aux parties un lieu de dialogue moins formel que les salles d'audience afin de « vider les conflits de leur substance ». Il est apprécié d'une majorité de citoyens car il leur permet d'être acteurs et non plus spectateurs de la sortie, à un moindre coût, du conflit les concernant.

En une année, le service de médiation a trouvé naturellement sa place, complémentaire des modes d'action déjà existants que sont les recours au juge, aux associations de consommateurs ou aux administrations compétentes. Il conviendra, néanmoins, pour l'année à venir de mettre l'accent: d'une part, sur une meilleure information des entreprises sur le rôle de la médiation et, d'autre part, sur une plus grande coordination des différentes actions de recours. Les discussions déjà engagées par le Forum avec des associations de consommateurs, des entreprises et les administrations compétentes devront être poursuivies pour une meilleure lisibilité et efficacité des dispositifs.

Le bilan du service est donc extrêmement encourageant et appelle à une réflexion sur son développement durable.

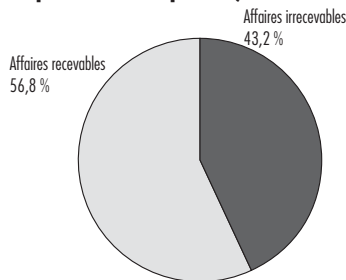
En effet, aujourd'hui, le service est gratuit conformément à ce qui avait été décidé en phase de lancement. La réflexion de cette nouvelle année devra porter sur la mise en place d'un modèle économique pérenne. Des discussions sont là encore engagées en ce sens, à la fois avec les entreprises et les pouvoirs publics, afin d'élaborer un dispositif idoine astucieux, de nature à fixer durablement l'indépendance du service et son efficacité.

## Annexe 1

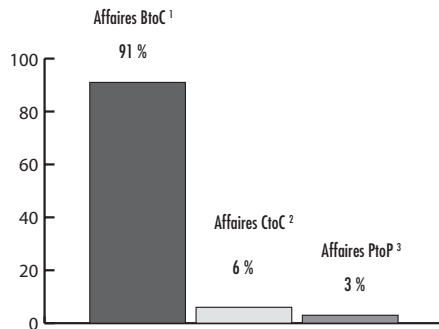
# Les chiffres clés du service de médiation

Septembre 2004 à décembre 2005: 5 495 demandes, 3 122 dossiers traités

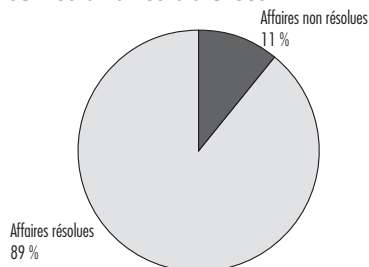
### Nombre d'affaires traitées (sur plateforme électronique ou par courrier postal)



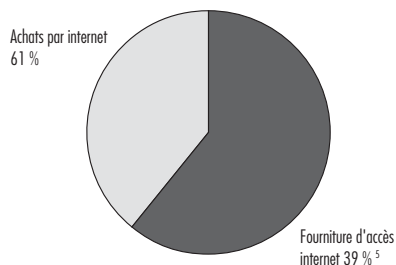
### Types d'affaires



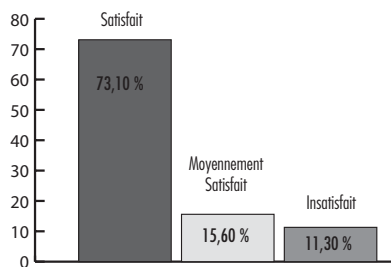
### Taux de résolution sur les affaires clôturées



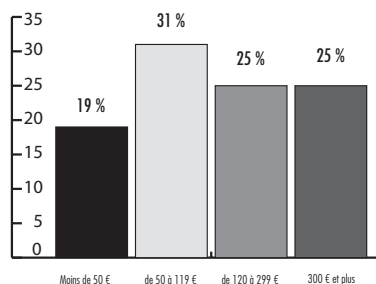
### Affaires BtoC



### Taux de satisfaction du service auprès des internautes<sup>4</sup>



### Montant des différends



1. BtoC : Différend entre un client et une entreprise.

2. CtoC : Différend lié à une plateforme de mise en relation (ex. site d'enchère en ligne...)

3. PtoP : Différend entre particuliers.

4. Satisfaction du service basée sur la facilité d'utilisation du site, sur la clarté du processus de médiation et sur le résultat obtenu (étude réalisée par un cabinet indépendant en février 2005).

5. Le service de médiation, en ce qui concerne les problèmes de fourniture d'accès internet, est en contact régulier avec six entreprises qui représentent 81,4 % du marché ADSL en France.

## Annexe 2

# Règlement de médiation

### Article 1. Présentation

1.1 <http://www.mediateurdunet.fr> est le site du Service de médiation du Forum des droits sur l'internet <http://www.foruminternet.org>. Il sera dénommé ci-après «le Service».

1.2 Le Service est offert à la personne qui souhaite être aidée dans la recherche d'un règlement amiable de son différend lié à l'internet (ci-après dénommée «la Partie Requérante») et l'opposant à une tierce personne (ci-après dénommée «l'Autre Partie»).

1.3 Le médiateur du Service est, tout d'abord, chargé d'analyser la recevabilité de la demande de médiation, de constituer un dossier avec la Partie Requérante et d'entrer en contact avec l'Autre Partie pour lui proposer de participer à un processus de médiation. Il lui revient ensuite la mission de mener le processus de médiation entre les parties.

1.4 Un médiateur externe peut être proposé à celles-ci par le Service pour conduire des médiations nécessitant notamment une spécialisation.

1.5 Toutes ces personnes, dénommées «les Intervenants» au processus de médiation, s'engagent à respecter le présent Règlement de médiation et ceci en vue de permettre aux parties de parvenir à une solution négociée et amiable au différend qui les oppose.

### Article 2. Principes fondamentaux

2.1 Tous les Intervenants qui ont volontairement accepté de participer au processus de médiation, s'engagent à respecter les principes de bonne foi, de loyauté, de courtoisie, de politesse et de réactivité, nécessaires dans la recherche d'une solution amiable.

2.2 Les parties gardent à tout moment la possibilité de se retirer du processus de médiation après en avoir informé le Service.

2.3 Les parties peuvent se faire assister par le conseil de leur choix. Elles ne peuvent cependant pas être représentées au cours du processus. Cela signifie que leur conseil ne peut se substituer à elles.

### Article 3. Domaine de compétence

3.1 Le Service traite des différends impliquant l'usage de l'internet et concernant au moins un particulier. Il doit s'agir d'un problème juridique. À ce titre, le Service est notamment compétent :

Pour les différends liés à un achat en ligne (BtoC), il peut s'agir d'une non livraison d'un bien ou non exécution d'un service; d'une non conformité d'un bien ou d'un service ou encore de la découverte de vices cachés sur un produit...

Pour les différends entre consommateurs (CtoC), il peut s'agir d'une transaction qui se déroule mal entre un acheteur et un vendeur sur le site d'une plate-forme de mise en relation.

Pour les différends entre particuliers (PtoP), il peut s'agir d'atteinte au respect de la vie privée; d'atteinte aux droits d'auteur (à l'exception notamment des différends entre les titulaires de droits et les utilisateurs au cas où ceux-ci estimeraient qu'une mesure technique de protection les empêche de bénéficier de l'exception de copie privée); il peut encore s'agir de diffamation, d'injure...

3.2 Le Service n'intervient pas pour :

- les problèmes techniques empêchant l'accès à internet (dégrouper, synchronisation du modem...);
- les demandes de retrait de contenus à caractère pédo-pornographique ou incitant à la haine raciale;
- les différends de masse c'est-à-dire les demandes émanant de plusieurs internautes contre une même personne et pour le même fait générateur;
- les différends de nom de domaine en .fr.

3.3 Le Service peut, notamment, refuser de prendre en charge une affaire si :

- la demande de médiation est incomplète, notamment si les éléments d'identification de l'Autre Partie ou les identifiants clients de la Partie Requérante sont absents ou encore si les démarches préalables auprès de l'Autre Partie n'ont pas été effectuées;
- une action en justice est déjà engagée;
- l'Autre Partie au différend est difficilement identifiable;
- il apparaît que l'une ou l'autre des parties est de mauvaise foi;
- les délais de prescription sont sur le point d'arriver à expiration.

3.4 Le Service peut également refuser à tout moment la prise en charge de nouvelles demandes de médiation pour assurer un niveau de prestation satisfaisant pour le traitement des affaires en cours.

3.5 Le Service peut, enfin, être suspendu en cas de maintenance de sa plate-forme de médiation en ligne.

#### **Article 4. Les conditions requises pour saisir le Service**

La personne qui souhaite saisir le Service doit :

- avoir préalablement tenté de résoudre son problème avec l'Autre Partie par écrit ou par tout moyen significatif dans le cadre d'une première prise de contact appelée « Démarches préalables »;
- vouloir trouver une solution amiable à son problème;
- être de bonne foi;
- être majeure ou avoir la pleine capacité juridique;
- avoir un intérêt à agir dans l'affaire.

#### **Article 5. Les modes de saisine du Service**

5.1 La demande de médiation doit se faire par voie électronique via le formulaire sur le site <http://www.mediateurdunet.fr> ou, si la Partie Requérante ne dispose d'aucun

accès à internet, par voie postale à l'adresse: Forum des droits sur l'internet, Service MediateurDuNet.fr, 6 rue Déodat de Séverac, 75017 Paris.

5.2 La demande de médiation doit obligatoirement comporter:

- le nom ou la dénomination sociale de la Partie Requérante;
- son numéro de téléphone;
- son adresse de courrier électronique;
- la nature du différend (commerce électronique, fourniture d'accès, diffamation....);
- les circonstances des faits;
- les coordonnées de l'Autre Partie (nom, téléphone ou adresse électronique);
- un identifiant (numéro client, numéro de ligne ADSL, pseudo...);
- si un autre service de médiation ou de conciliation a déjà été sollicité;
- si la justice, une association de consommateurs, la DGCCRF ou toute autre structure ont déjà été saisies pour les mêmes faits.

### **Article 6. Étude de recevabilité de la demande**

6.1 Après avoir accepté le présent règlement, la partie requérante reçoit un accusé de réception de sa demande par courrier électronique ou par courrier postal si la demande a été faite par voie postale.

6.2 Le Service s'assure alors de la recevabilité de la demande de médiation au regard de son domaine de compétence, des conditions requises pour participer au processus de médiation, et du niveau de renseignement de celle-ci.

6.3 Le Service avise dans les meilleurs délais la Partie Requérante de la recevabilité de sa demande.

6.4 En cas de recevabilité, des identifiants de connexion confidentiels ainsi qu'un numéro d'affaire sont attribués à la Partie Requérante. Celle-ci s'engage à les conserver tout au long du processus de médiation.

### **Article 7. Le complément d'information**

7.1 La Partie Requérante avisée de la recevabilité de sa demande doit effectuer un complément d'information en ligne ou par voie postale. À compter de la réception du courriel de confirmation de prise en charge du cas par le Service, le complément s'effectue sur l'espace sécurisé réservé à la Partie Requérante dans un délai de 7 jours. Dans l'hypothèse de non respect de ce délai, le Service se réserve la possibilité de clôturer l'affaire.

7.2 La Partie Requérante s'engage à donner une information claire et conforme à la réalité et à informer le Service de tout événement intervenu dans le différend depuis sa saisine.

7.3 La Partie Requérante appelée à exprimer ses attentes lors du complément d'information s'engage à ne pas formuler de nouvelle demande au cours du processus de médiation.

7.4 Outre, les informations complémentaires demandées, la Partie Requérante doit obligatoirement renseigner une question secrète figurant dans la rubrique « mon profil » qui lui est dédiée, celle-ci est nécessaire en cas de perte des identifiants de connexion.

## **Article 8. La prise de contact avec l'Autre Partie**

8.1 À la réception du complément d'information, le Service entre en contact avec l'Autre Partie pour lui faire part du différend dont il est saisi et pour lui proposer de participer au processus de médiation. Le présent Règlement est alors porté à sa connaissance par courrier électronique ou par courrier postal.

8.2 La réponse de l'Autre Partie fixe la date de commencement du processus de médiation.

8.3 La durée de la médiation ne doit pas, en principe, excéder trois mois à compter de la date de commencement du processus de médiation. Toutefois, le Service peut, avec l'accord des deux parties, proroger la durée du processus de médiation s'il le juge opportun.

8.4 En cas de refus implicite ou explicite de l'Autre Partie ou en cas d'impossibilité de prendre contact avec elle, le Service en avise la Partie Requérante; dès lors, le processus de médiation ne peut pas s'engager et le dossier est clôturé.

## **Article 9. Déroulement du processus de médiation**

9.1 Les parties ayant accepté de participer au processus de médiation s'engagent à respecter les principes de bonne foi, de loyauté, de courtoisie, de politesse et de réactivité nécessaires dans la recherche d'une solution amiable. À défaut, le Service pourra interrompre ou mettre fin au processus de médiation après en avoir informé chacune des parties concernées.

9.2 Le Service n'est ni juge, ni expert; c'est un facilitateur de dialogue entre les parties dont la mission peut aller jusqu'à émettre des propositions concrètes de compromis que les parties sont libres d'accepter ou de refuser.

9.3 Le Service s'engage à mener toute démarche utile, conformément au présent Règlement, pour faciliter le dialogue entre les parties dans un esprit d'équité. Il ne peut cependant en aucun cas garantir une issue favorable au processus de médiation. En ce sens, le Service n'est soumis qu'à une obligation de moyens.

9.4 Le Service ne pourra voir sa responsabilité engagée à l'égard d'aucune des parties au différend pour aucun propos, acte ou omission fait par l'une des parties au préjudice de l'autre avant, pendant et après le processus de médiation.

9.5 Le Service garantit son impartialité et son indépendance à l'égard des parties. Il leur fait connaître les circonstances susceptibles de les remettre en cause.

9.6 Sauf accord contraire des parties et du Service, toute personne associée directement ou indirectement au processus de médiation s'engage pendant et après le processus de médiation, à ne pas révéler ou utiliser comme preuve ou d'aucune manière les informations, opinions, suggestions, aveux ou propositions présentés sous quelque forme que ce soit par les parties ou le Médiateur au cours du processus de médiation. Ceci ne concerne pas les éléments établis antérieurement au processus de médiation ou qui n'auraient pas été produits au cours dudit processus.

Les Intervenants au processus de médiation autorisent néanmoins le Service à utiliser les éléments recueillis au cours de la médiation notamment dans le cadre de son

bilan d'activité ou dans ses publications statistiques. Dans ces hypothèses, le Service s'engage à respecter l'anonymat demandé par les Intervenants.

#### **Article 10. La désignation d'un Médiateur externe**

10.1 Avec l'accord des deux parties, le Service peut proposer la désignation d'un Médiateur externe, choisi en fonction de ses compétences spécifiques et répondant à un besoin ponctuel du Service.

10.2 Les parties disposent d'un délai de 15 jours ouvrables à compter de la notification de cette proposition pour accepter ou refuser ce Médiateur. Chacune des parties ne peut faire valoir un tel refus qu'une seule fois. En cas de refus, un nouveau Médiateur est proposé. À défaut d'accord des parties sur le choix du Médiateur, le processus de médiation prend fin et le dossier est clôturé.

10.3 Le Médiateur externe doit mener le processus de médiation dans le respect du présent Règlement de médiation, auquel il a adhéré. Il dispose des mêmes prérogatives et est soumis aux mêmes obligations que celles du Service telles qu'énumérées à l'article 9 des présentes.

10.4 Le Médiateur externe s'interdit, en outre, d'exercer avec les parties une autre fonction que celle de médiateur.

#### **Article 11. La fin du processus de médiation**

11.1 Le processus de médiation prend fin :

- en cas d'exécution volontaire ou de déclaration de volonté d'exécuter de l'une des parties, vidant le différend de sa substance, ou par la signature d'un accord de règlement amiable entre les parties ;
- par une décision écrite et motivée du médiateur du Service, si celui-ci estime que les règles de la médiation ne sont pas respectées ou lorsqu'il estime qu'il n'est plus en mesure d'assurer la poursuite de sa mission. Tous les Intervenants à l'affaire en sont alors avisés ;
- par une décision non équivoque de retrait du processus de l'une ou l'autre des parties au différend ;
- si une action en justice est engagée dans l'affaire en cause ;
- en l'absence de réponse prolongée de l'une des parties au différend ;
- à l'expiration du délai de médiation si celui-ci n'a pas été prorogé conformément aux stipulations de l'article 8.3 du présent règlement.

11.2 À l'issue du processus de médiation, le Service notifie aux parties la date de clôture et le résultat du processus de médiation.

11.3 L'accord de règlement amiable intervenu n'a pas de force contraignante. Les deux parties s'engagent néanmoins à le mettre en œuvre dans un délai raisonnable.

Quatrième partie

# **La coopération internationale**



# Policy statement on Internet Governance

*Report of the European Internet Coregulation Network  
Published in July 2005*

Internet governance is a controversial issue. For some observers, it should be limited to the production of technical norms for the network, for naming and the future of ICANN. For others, it should cover other issues, including content, evolution of uses...; in any case, everyone questions the specific role of the States and the other actors (civil society or private sector) in the management of this internet governance.

The subject has been submitted to the World Summit on the Information Society (WSIS) and it appears as a critical one.

In the absence of consensus between the States, and the various parties concerned, a working group has been launched under the United Nations Secretary-General. The mission of the group, chaired by Nitin Desai, is:

- to elaborate a practical definition of Internet governance;
- to identify issues of general interest related to it;
- to elaborate a common conception of the roles and the areas of responsibilities of governments, inter-government and international organizations, and other existing forums, as well as the private sector and civil society, in developing and developed countries;
- finally, to elaborate a report on the results of the mission, which will be examined in the course of the second phase of the Summit in Tunis in November 2005.

This is the context and the reflection to which the **European Internet Coregulation Network** (EICN)<sup>354</sup> wishes to contribute.

A working group was launched in April 2004 under the supervision of the French Internet Rights Forum. These conclusions were adopted by the members of the Network in July 2005.

---

354. The European Internet Coregulation Network (EICN) was initiated by the French organization, Le Forum des droits sur l'internet, in partnership with organizations from 6 European countries during the WSIS in Geneva in December 2003. One of its objectives is to feed the European institutions with proposals on the subjects of common interest. The members of the EICN are: Institutet för Rättsinformatik (Sweden), Observatoire des droits de l'internet (Belgium), Forum per la tecnologia della informazione (Italy), Internet Watch Foundation (United Kingdom), Oxford Internet Institute (United Kingdom), Információs Társadalom-és Trendkutató Központ (Hungary), Le Forum des droits sur l'internet (France), Österreichisches Institut für angewandte Telekommunikation (Austria) and the Confederation of European Computer User Associations. **The IWF is not a party to this paper because the subject matter is outside its remit.**

The objective of the EICN is to feed the public debate with its own vision of the notion of «internet governance». This vision is built on the expertise of its members in the legal and policy issues related to the internet. It is directly linked with the philosophy of regulation shared by the EICN members. It inspires recommendations or guidelines for a good internet governance.

## EICN philosophy of regulation

### **From regulation and self regulation to coregulation**

The Internet is a complex media because of three main characteristics: international geography without border, plurality of participants and decentralized organization without a central point of control. In the recent years, as it is an expanding social space, different ways of defining and implementing public policy issues have been applied with more or less success.

The first reaction of the States in 1996 was **regulation** because Internet was viewed as a new media which could be regulated as a broadcast media. But this attempt failed because of the very characteristics of the Network closer to «*an endless world conversation*» than to a traditional medium. Therefore, States interventions have been limited to monitoring the activities (liability regimes for Internet access providers, data hosts, technical intermediaries, users) and not the material circulating online.

In order to compensate for the limits of national laws, a policy of **self-regulation** has developed in the private sector, especially the trade sector. In many areas (protection of minors, e-commerce, etc), self-regulation was viewed as a method to set the rules without State intervention. This method has been criticized, its professional objectives pointed out as unable to take into account issues of public interest.

Since 1998, several States have adopted laws in order to regulate the circulation of material on the Web (DMCA in the United States, European directives on electronic signature, on e-commerce or on copyright and related rights in the information society, the Council of Europe's Convention on Cyber-crime, etc.). While binding norms are spreading, self-regulation tends to evolve to a more realistic vision: implement general principles set by the laws. For example, the new codes of conduct provide private parties with advice and implementation tools regarding the applications of recent laws.

But again, this way seems a bit limited in order to handle the policy issues of the internet.

In fact, **the complexity of the Net challenges traditional modes of regulation** and specifically the ability of the States to set rules in given physical spaces between all parties and regulate behaviours according to social or moral norms.

Two examples can be given :

–Spamming: the 2002 European legislation has set an opt-in obligation to the direct marketers but it cannot do anything to prevent from spam messages coming from unregulated countries collecting illegally addresses on the Web;

–Sharing and downloading music and video on P2P networks: it is not only a European directive that can prevent millions people to share music and films and being considered as «pirates».

A new path has to be elaborated, adapted to the specificities of the network. **It must be based on a new scheme of cooperation between the public and the private actors**, more balanced, more flexible, more open.

This smooth procedure, associating all parties in the elaboration of the rules of the network is called **coregulation**.

The word «coregulation» was born in France in 1998 and it is often quoted in international texts. Nevertheless, it can describe two ways of understanding the regulation philosophy generated by the internet:

In the first meaning, coregulation stands for «regulated self-regulation»: in this form of governance, the business entities or the civil society is associated with the public authorities in order for these latter to control or frame the self-regulatory tools. It generally leads to code of conducts elaborated by a group of actors, then validated and guaranteed by the public authorities.

**In the second meaning, coregulation has a wider prospective and leads to a real «multi-stakeholder partnership».**

This approach is based on the belief of shared responsibilities between the public and private actors on internet issues. The parties have to manage their interdependencies and articulate their specific tools of regulation. It leads to open and balanced discussions between the business sector, the public authority and the civil society in order to elaborate common solutions. These solutions are combining regulatory tools and preferences at the disposal of each actor (laws and decrees, codes of conducts, technical tools, self-awareness...)

This pattern of governance involves a matter of principle: all parties concerned in the development and the uses of the Internet have a legitimate right to contribute to the definition of the rules governing them. It is also built on a matter of efficiency: many problems quite simply cannot be solved without the active contribution of all parties.

The EICN believes that this meaning of coregulation is the governance pattern best adapted to the internet.

Nowadays, the coregulation principle is gaining widespread acceptance at the international level. In France, the Internet Rights Forum is implementing this approach since 2001 with great success. Furthermore, after the Paris meeting in June 2004 on the fight against racism, anti-Semitism and xenophobia on the Internet, the Organization for Security and Cooperation in Europe (OSCE) recommended the development in every State of areas for consultation between all parties concerned. Lastly, the United Nations have been trying to enhance greater participation of the private actors and the civil society in international conferences.

## Recommendations for a good «internet governance»

**The EICN believes that the expression «internet governance» should be clarified. For its members, it is less a question of subjects to be addressed (technical standards, contents issues...) than the way it is possible to address them. In fact, the characteristics of the Network generate specific processes to handle the policy issues and this is what internet governance is about.**

**The following recommendations tend to sum up the best practises and the knowledge gained by the EICN members in the recent years in this matter.**

### **1 Internet is a social space which needs regulation in all its aspects according to common social values.**

Internet cannot evolve in the future if the social dimension of this space is not recognized. Most of the human activities are now transferred on the internet and it implies new responsibilities for all the actors, public and private. At the same time, it is a new and very exciting frontier of our humanity.

Europe can play a distinguished role in defining the ways and the values which must be promoted at the international level.

### **2 Because the internet is decentralized, the method of regulation needs a bottom-up process.**

The Internet favours not only technological, but also methodological innovation. This is due to the fact that the complexity of this new social space (international, pluralist, borderless, decentralized) has fostered new ways of establishing rules. For example, in technical areas, an open, decentralized and participative process is operated by the entities in charge (W3C, EITF) and this process has allowed the production of legitimate, flexible and efficient standards.

Any governance pattern must be built on this type of methods that guarantee that all the parties concerned can express their views and that the solution adopted takes into account the needs from ground level.

### **3 Opening to all the stakeholders (business and civil society representatives) as a sign of their interdependence to contribute to every stage of the preparation of norms;**

Internet issues involve three kinds of stakeholders :

- the **States**, traditionally monitoring international bodies, but having more and more difficulty setting and upholding rules ;
- the **private sector**, which has gradually taken over the roles of builders and strategists in the information society ;
- lastly, the **civil society**, a heterogeneous and scattered sum of actors focused on the defence of fundamental values (humans rights, access to culture...). Each of these components participates in the bodies under study in various ways.

All of the stakeholders must be associated in the elaboration process of the norms because **they all have shared responsibilities in defining and implementing them**. This cooperation process is not an addition of bilateral dialogues between the States and the two others. It should be a real balanced dialogue between the three.

The cooperation can work at different levels:

- the stakeholders can participate to the body itself that elaborate the norm;
- they can be consulted in the preparatory stage of the norms (right of initiative, participation within working groups);
- they can, eventually, be part of the decision-making process.

#### **4 Reaching for consensus : procedures need to seek acceptance of proposals by every participant.**

The Internet is a space where it is difficult to enforce rules. Each actor can easily bypass the constraint of a national obligation. One answer is that all the actors agree on the objectives of the rule and on the solutions to implement it. Therefore, each actor appropriates the rule and works at its enforcement.

If consensus is not reachable because of high political divisions, there is still an objective to pursue: establishing common information and understanding on the subjects concerned.

#### **5 Combining regulatory tools of each stakeholder: regulation, best practices, information and pedagogy...**

Public and private actors have specific regulatory tools they can use to foster their vision of the internet; none of these tools are entirely satisfying but they can be combined to draft effective solutions for internet policy issues. Depending of the subject, these latter will be based on more or less statutory interventions, codes of conducts, self-awareness...

#### **6 Combining the national and international dimension of the internet;**

The Internet is not a network which could be controlled at the local level. Many examples show that a regulation at least regional or international is necessary (spamming, child protection, etc.).

#### **7 Recognizing a specific role for public authorities**

Public authorities must be part of the open consultation process between all the stakeholders in order for it to take into account public policy concerns. In the decision phase, the States have full and specific competences in three ways:

- they are the only ones able to transform consultation process deliverables into legal norms;
- they can arbitrate between the parties if the consensus has not been reached;
- they are the natural vouchsafe of public interest.

#### **8 Recognizing the necessity of a cultural change**

Coregulation is not an easy path. It calls for a cultural change for all the stakeholders:

- the Governments, because a lot of them still consider internet as theirs; without challenging their specific role, they have to accept open dialogue with the other stakeholders, sometimes on an equal basis;
- the private sector has to understand that coregulation does not mean only regulated self-regulation, in other words, «regulation of their corporate interests»; they have to commit themselves to real discussions with all the actors involved, including the users;
- the civil society is very heterogeneous; this diversity is an asset as long as the actors work in a constructive way.

# Report on Protecting Minors from Exposure to Harmful Content on Mobile Phones

*Report of the European Internet Coregulation Network  
Published in July 2005*

## Introduction

The *Recommendation 98/560/EC* on the protection of minors and human dignity in audiovisual and information services, adopted on 24 September 1998, is in the process of being revised by the European institutions. As its first contribution to the on-going debate around this revision of EU policy, the European Internet Coregulation Network (EICN) recommended in its first policy statement that European policy makers, members of the industry and users should aim at making the next-generation mobile Internet a secure environment for children<sup>355</sup>. In issuing such a recommendation, the EICN designated child protection in multimedia online mobile services one of its priorities for action.

In order to build on this contribution, the EICN tasked the Oxford Internet Institute (OII) to lead a working group examining the child protection implications of Internet-enabled mobile phones and other new mobile devices, part phone and part handheld computer. The working group attempted to gather information on the best practices of local mobile phone operators, content providers and distributors on a European scale, in part using information provided by other EICN members and their contacts in response to a project questionnaire of August 2004. The researchers also conducted exploratory interviews with industry representatives from the major network operators in the UK and regulatory and Parliamentary actors.

Based on this original research and on previous work conducted at the University of Oxford for the Safer Internet project [www.selfregulation.info](http://www.selfregulation.info)<sup>356</sup>, the OII has elaborated a comprehensive project report on the «Implications of the Mobile Internet for the Protection of Minors», to be published soon after the release of this document.

The following report serves as a summary of that project, and concludes with the EICN's recommendations, which were unanimously adopted by the member organisations on 28 July 2005.

---

355. European Internet Coregulation Network. 2004. *Child Protection on the Internet. Preventing the Exposure of Children to Harmful Content. A Political Statement.*

356. Ahlert, Christian, Alexander, Marcus & Damian Tambini. 2003. European 3G Mobile Industry Self-Regulation: IAPCODE Background Paper, Paper delivered at the World Telemedia Conference, Prague.

## Background

The launch of third generation mobile networks (3G) across Europe in 2003/4<sup>357</sup> has highlighted the emergence of mobile Internet access, even though a more limited form of Internet access was previously possible under narrowband networks and in more developed mobile markets in East Asia. In the autumn of 2004 most of the major UK network operators began to offer handsets which are capable of using 3G for connecting to online services, a phenomenon mirrored elsewhere in Europe. More recently, further developments in handset technology brought new devices onto the market capable of seamless roaming. These handsets can switch automatically between different networks including wireless local area networks (LANs), a feature which further blurs the already muddy distinction between mobiles-accessed Internet and ordinary wireless access from a PC or PDA.

It is important to note that despite the fact that concerns about mobile content have been stimulated by the emergence of 3G and 'Internet-enabled handsets' for the purposes of this report, mobile content covers three different types of content: commercial content provided by mobile operators and largely purchased from third party suppliers; content available on the public Internet; and also content produced and passed through peer-to-peer communications such as photos. Differentiating between these three types of content is important as even if they are a source of common concern, different technical or regulatory responses are possible and potentially desirable in each case.

Mobile phones are thus becoming an ever more sophisticated device for accessing email, the Internet and other services. Such technological advances have however also led to the development of new business models for network operators, which focus largely on collecting revenue from online content. The models include:

- (1) network operators offering their own content,
- (2) network operators allowing third parties to provide content,
- (3) networks providing open access to the Internet.

Far from being mutually exclusive, these business models are increasingly combined by operators in a single strategy. Indeed, in the UK at least, mobile operator 3 is, as of June 2005, the only operator not offering *any* open access to the Internet, whether subscribers want it or not. It is important to recognize the existence of these different models however, as the possibilities for co – and self-regulation associated with the content delivery model will clearly vary according to the sources of content.

It is also important to remember that it is not just consumers who will benefit from these advances: most market forecasts see adult services, as well as gaming and gambling services, potentially offering a significant source of revenue for network operators. In this light any workable self or coregulatory framework must balance concerns for child protection with those of economic competitiveness.

---

357. The first European 3G networks were launched in the Isle of Man off the UK mainland in 2001, but national commercial roll-out was begun by 3 (Hutchison 3G) in Italy and the UK on 3rd March 2003: see <http://www.phonescoop.com/news/item.php?n=487>

## Mobile Content – the State of Play

### Mobiles vs PCs

Just because mobile technology has developed to the point where Internet and commercial content are easily accessible does not mean that such phones offer the same risks to children in terms of harmful material as access to such content via PCs. In particular, there are relevant differences in the way that the devices are designed, sold and used which need to be taken into account in order to understand the nature of public concerns and to design a policy response accordingly. These differences can be summarised as follows<sup>358</sup>:

1. **Ubiquity**: given the increasing pervasiveness of colour screen technology in even standard mobile phone models, many secondary and even primary school students are likely to have phones with colour screens at the birth of the wireless Internet, whilst most children have only gained access to the Internet via PCs at a later stage in that technology's development.<sup>359</sup> Although it is not yet clear that many children use their phones to access the Internet or commercial content (for example see Vincent 2004), the high levels of mobile phone ownership mean policymakers should not be complacent.

2. **Supervision**: unlike PC-based access to the Internet, mobile use is, by its very nature, more likely to be private and largely unsupervisable. This may be tempered to some extent by the possibility of parental monitoring of itemized phone bills, although in the UK as elsewhere in Europe, large numbers of mobile users have Pay-as-you-go accounts, with under-16s especially likely to have such accounts.

3. **Control**: with PCs, access to the Internet is provided and controlled by an Internet Service Provider (ISP) and users can choose which ISP they contract with after buying their PC. Such choice and competition amongst ISPs means that individuals could easily opt in or out of various filtering options by shopping around amongst ISPs. In the case of mobile-accessed Internet, however, a handset is usually bought as part of a contract with a particular operator. Even if it is practically possible to change network, this is not something which many customers would do on a regular basis. So long as this remains the case (and it may change) it is easier for network operators to adopt content controls, such as filters, as at any point in time they are the only gatekeeper to the Internet for individual users of their services. This feature, combined with the different models for content delivery described above means that mobile network operators can and do provide so-called 'walled gardens', which effectively limits Internet access to content approved by the network operator.

4. **Filtering Defaults**: it was widely expected that on mobile phones, filtering defaults when available would largely be opt-in, unlike opt-out Internet Explorer, AOL and

---

358. Categories adapted and extended from Marsden (2004).

359. Figures from the UK Department for Education and Skills show that in 2002 41% of children between 5 & 18 owning a mobile phone, a figure which is likely to have increased still further in the past two years (DfES 2002). A recent consumer survey suggested that mobile phones are owned by over 5 million under-16s in the UK (Mobile Youth 2005).



Google, meaning that 2.5/3G mobile phone users would by default have access to adult content. In the UK, this position has largely been reversed, in no small part due to lobbying by child protection groups, meaning that those purchasing new mobile phones will now usually need to opt out of filtering applications, which will only be possible after age verification.

**5. Convergence of Capture and Distribution in One Device:** most devices now offer digital image capture capabilities and also enable distribution of these images via the network, and locally at no cost by infrared and Bluetooth – picture messaging is an example of this. This means that in principle, the distribution of inappropriate pictures, or even pornography is only ‘One Click Away’ from digital image capturing; but in a way that cannot be controlled by filters at the network level.

**6. Peer-to-Peer File Sharing:** Given that 3G bandwidth is still much slower than standard broadband connections, p2p file-sharing of photos, movies or music is time consuming and costly. However, as operators are now starting to offer seamless roaming packages whereby mobile phones can be used at home with standard wireless broadband connections and on the move with wireless hotspots, P2P may further drive usage of mobile-accessed Internet by children.

## Harmful Content ?

One of the most difficult issues that arises in relation to the protection of minors from inappropriate content is at what age children should be able to access different types of content, or indeed what counts as ‘inappropriate’ or ‘harmful’ content for different groups of users. In many cases, for example, material might be deemed inappropriate and potentially harmful for a 7-year old, but harmless for a 16-year old. In addition what is deemed harmful in the UK for a 16-year old may be seen as entirely appropriate in the Netherlands, or Sweden. Any workable code of practice would have to address these issues within the context of its own cultural and regulatory norms, thus the Network has avoided making any statement as to what constitutes ‘harmful content’ for any particular country.

The Network has chosen to focus on harmful or inappropriate content, as illegal content, such as child pornography or hate speech, is (at least in Europe) less controversial because it is widely agreed to be unacceptable, and is explicitly prohibited by the national law of many EU member states and a corresponding network of resources, such as national hotlines, already exists to deal with it.

Inappropriate content for under-18s potentially includes, but is not limited to the following:

- Pornography
- Violent games
- Unmoderated chatroom services
- Music with sexually explicit lyrics or videos
- Spam containing adult content
- Gambling

Other concerns not relating to content may also be raised, for example, concerns about the cost of premium rate services which under-18s may choose to use such as interactive voting, or ringtone downloads but such concerns are beyond the scope of this report.

## Should children's access to mobile content be a policy concern?

As has been pointed out above, while mobile phone use by its very nature is less open to physical supervision than PC use, there are certain technical features of mobile phones which would suggest that the risks to children are potentially more controllable than those posed by PC-accessed content. The role of network operators as de facto gatekeepers means that there is a single bottleneck through which access to commercial content and the wider Internet can be controlled. This feature, combined with the fact that unlike most PCs, mobiles tend to be used or owned by a single individual, mean that in principle at least, there is more scope to sell or modify handsets in such a way that they are set to disallow access to material unsuitable for children. These caveats notwithstanding, the media have carried ever increasing numbers of sensationalized stories surrounding children's use of mobile phones since start-2004. In the UK, stories have included coverage of:

- schools and leisure centres banning the use of camera phones for fear of paedophile exploitation;
- the possibility of child abduction as the result of information provided by new location-aware handsets and
- accounts of a sex-offender who lured girls for underage sex through the use of Internet chat rooms (BBC news website, January-October 2004).

Market surveys have revealed potentially mixed feelings on the part of parents when it comes to their offspring's use of mobile phones. The National Children's Homes charity in the UK recently reported that 86% of Scottish parents feared that 3G mobile phones could threaten the safety of their children, whilst at the same time, the number of UK 7-10 year olds with mobile phones doubled in three years (2001-3), with parents' concerns about their child's safety being cited as one reason for this (source: Mintel survey, reported BBC news 28/4/04). With the advent of 2.5 and 3G phones, it would seem as if mobile phones might be perceived by parents as, on the one hand, helping to secure their children against abduction, yet exposing them to other new dangers of theft and inappropriate Internet content on the other. It is important to bear this trade-off in mind when looking at possible measures for child protection – the Internet potentially offers many benefits to children, educational, cultural and social, and any proposed solutions should work to ensure that access and information rights are preserved to the greatest extent possible whilst balancing for other concerns.

There is as yet little academic research on children's use of Internet-enabled mobile phones. One very recent study seems to offer little evidence to suggest that children make significant use of their mobile phones to access the Internet or download commercial content, and price sensitivity is cited as one important explanation for this (see for example Vincent 2004). But given that the technology and pricing plans are

changing rapidly, further research is needed to determine whether this will remain the case as 3G handsets face and pass their first anniversary in Europe.

Given the limitations of current research on mobile accessed content it is worth looking also at some of the studies of children's use of PCs. The European SAFT survey found that between a quarter and a third of 9-16 year olds had been accidentally exposed to violent, offensive, sexual or pornographic content in 2002/3. Sonia Livingstone's 2004 UK survey of children and Internet use backs this up, finding that 36% of 9-19 year olds have found themselves on a pornographic website when looking for something else and 25% say they have received pornographic material via junk mail (Livingstone 2004, p.29). Interestingly though, Livingstone's survey also examined parents' assessment of their children's online experiences, which showed that children report much higher levels of problematic experience online than their parents appear to be aware of. This would suggest that media and policy exhortations to parents to supervise their children's use of the Internet on home PCs may not be sufficient presently to deal with the problem of access to inappropriate material. Whilst there is clearly still room for effective and universal media literacy training, given that children's use of mobile phones is by its very nature so much harder to monitor and supervise, this finding also suggests that in the case of mobile content, technical and self – or coregulatory measures do indeed have a significant role to play in protecting children from inappropriate content, as will be outlined shortly. At the very least it also suggests that significant media literacy and awareness raising efforts should be directed at children, not just parents and carers.

## **Possible policy responses ?**

There are a range of different regulatory options available for dealing with these issues, each with their own advantages and disadvantages. Proponents of self-regulation claim that this is the most effective and efficient form of regulation in a fast-paced and complex market such as that enjoyed by the mobile phone and Internet industries. The «self» in self-regulation usually refers to an industry which is developing rules and codes of conduct for itself. Enforcement and monitoring of the regulatory environment in this model usually also lies with the industry itself. Observers of self-regulation usually cite the threat of government intervention as the main motivation for industry's development of self-regulatory codes, as this could make doing business much more costly. In reality, however, «pure» self-regulation, with little or no role for government, is almost never found. Even in the Internet and mobile industry where direct regulation of content is almost entirely absent, there is a multitude of national laws ranging from the protection of minors in general, to freedom of expression and copyright, which effectively regulate Internet content, or any content delivered to mobile Internet devices.

Throughout the 1990s self-regulation was heavily advocated by the European Commission, most notably under the Safer Internet Action Plan, but this approach seems to have fallen somewhat out of favour with recent measures promoting a more «coregulatory» approach. Whereas «self»-regulation implies a degree of independence from direct state regulation, «co»-regulation implies that the private

companies, the state and user-groups are involved in jointly developing rules and regulations. This might be thought more desirable to the extent that research on self-regulation has shown that some self-regulatory models in the Internet industry lacked proper procedures for oversight and enforcement, and amount to little more than declarations of good will.

Coregulation in this regard is a new process of elaborating rules in a world of «shared responsibilities» between all the actors. According to the European Internet Coregulation Network, coregulation aims at organizing a cooperation process on rights and usages issues between public authorities, the private sector and the civil society. Through this cooperation process, the actors have the opportunity to reach a consensus point on each subject. Coregulation allows to combine regulatory tools and preferences at the disposal of each actor (laws and decrees, codes of conduct, technical tools, self-awareness)<sup>360</sup>. Given the nature of this relationship, there are of course different possible models of coregulation which allow relatively greater or lesser degrees of freedom to industry, more or less involvement from consumer bodies and implication of the state. Thus, for example, as the OII observed in regards to mobile content, the United Kingdom's approach can be described as more self-regulatory as government involvement is fairly minimal, whereas in Germany and Italy for example it is stronger. It is also conceivable that a coregulatory process of consultation and negotiation might produce a framework such as a code of practice within which certain activities are left to be regulated by industry (such as provision of filtering tools or age verification processes) whilst others (such as the classification of commercial content) are subject to regulatory standards or the oversight of an independent monitoring body (as in the UK).

The European Commission has reported on Member States' regulation of mobile phone content and recommended a coregulatory approach where possible, although as that report indicates, some Member States do have applicable legislation which covers mobile content. It can be expected that the European Commission will return to the subject matter as part of the continuing Safer Internet Action Plan, which primarily aims at promoting awareness amongst member states of issues around child safety online, indeed a «Safer Internet Forum» on «Child Safety and Mobile Phones» bringing together stakeholders from all over Europe was held in Luxembourg on 14 June 2005.

The EICN's working group reported on several different strategies for dealing with child protection and mobile phones which are employed in Europe to regulate commercial content accessible via mobile phones and sometimes secure Internet-connectivity through mobile networks:

– *Germany*: introduction of legislation which establishes consistent standards for the evaluation of identical content across media sectors «irrespective of the mode of transmission». A single supervisory body – the «Commission for the protection of minors in the media» (*Kommission für Jugendmedienschutz* – KJM) – has been

---

360. See European Internet Coregulation Network, *Policy Statement on «Internet Governance»*, July 2005.

created for broadcasting, the Internet and other forms of digital media in regard to the protection of minors and human dignity.

– *United Kingdom*: establishment of a Code of Practice which all six mobile operators have signed up to which introduces specific measures to protect children from accessing harmful content inadvertently.

– *Italy & Ireland*: introduction of mobile codes of practice which include some measures to protect children amongst other commitments, although only in Italy did government play a significant role in helping to develop and promote the Code.

The UK Code of Conduct was of particular interest to the Network as it is so far the most detailed and thorough measure introduced to deal with the issue of child protection and harmful content accessed via mobile phones.

#### *The UK Code*

The UK Code was drafted by a committee including all six UK network operators and virtual operators (3, Vodafone, Orange, T-Mobile, Virgin Mobile, O2). Informal consultation with content providers, infrastructure and handset suppliers and government at national and European Commission levels took place. The six operators include all four of the largest pan-European operators<sup>361</sup>. Details of the Code's implementation (see below) were announced on 7 February 2005 with the launch of the Independent Mobile Classification Body (IMCB)<sup>362</sup>. The Code itself is unremarkable, but its ex ante adoption, prior to many adult services being known to the general public, is exceptional and reflects high awareness in the sector both of potential harms and of the value of self-regulation. In part, this can be attributed to the market size and regulatory resources of the four giant companies behind the drafting.

The main points of the code are:

- All commercial content unsuitable for under-18s will be classified as «18», and will only be made available to customers when the networks are satisfied that the customer is 18 or over.
- The classification framework will be comparable to those applied to other media, and will be created by a body independent of the mobile operators.
- Chat rooms available to under-18s will be moderated.
- Parents and carers will be able to apply filters to network operators'Internet access service to restrict the content available via a particular phone.
- Mobile operators will work to combat bulk and nuisance communications.

---

361. 56% of the 2000 European subscriber market was O2, Vodafone, T-Mobile and Orange – TIM and Telefonica Moviles, with less significant interest outside their domestic markets, are small in pan-European terms. See Ahlert et al (2003) at p4.

362. See Classification Framework at <http://www.imcb.org.uk/assets/documents/ClassificationFramework.pdf>

In addition, the Code observes the same 'notice and take-down' requirements with regard to illegal material as those applying to fixed-line ISPs. Thus Section 3 of the Code states:

*«Mobile operators will work with law enforcement agencies to deal with the reporting of content that may break the criminal law. Where a mobile operator is hosting content, including web or messaging content, it will put in place notify and take-down provisions.»*

There are, however, several restrictions on what the Code does or should cover. For example, the UK Code explains that:

*«The Code covers new types of content, including visual content, online gambling, mobile gaming, chat rooms and Internet access. It does not cover traditional premium rate voice or premium rate SMS (texting) services, which will continue to be regulated under the ICSTIS Code of Practice.<sup>363</sup>»*

This is explained by the fact that an effective code of practice and regulator (ICSTIS) have been in place to regulate such content for the last twenty years, so no new action on this is necessary.

Similarly, the Code refers to wider Internet content not directly supplied by third parties to the mobile operator but notes that operators do not have control over this, and as such cannot be held responsible for its classification or the availability of adult material. Instead it states:

*«Mobile operators will therefore offer parents and carers the opportunity to apply a filter to the mobile operator's Internet access service so that the Internet content thus accessible is restricted. The filter will be set at a level that is intended to filter out content approximately equivalent to commercial content with a classification of 18»*

Responsibilities here mirror those of fixed-line ISPs.

The code also does not seek to cover other issues which have already stimulated media concern such as the use of camera phones and Bluetooth technologies for content creation and distribution that does not require downloading from a website, or other forms of P2P file-sharing. To the extent that any form of regulation is possible with such content, this is already subject to nuisance call procedures and criminal laws which outlaw the transmission of illegal images and malicious communication.

Thus the Code covers the three different types of content outlined at the beginning of this paper, but ascribes very different responsibilities to mobile network operators in each case. In doing so, it covers most of the potential areas of concern for parents, and demonstrates to government that the industry has taken its corporate responsibility seriously, but does still leave unanswered some important questions. Issues include how to build a relationship of cooperation between mobile operators and commercial content providers, raising awareness of the code and the role of retailers. Also, the code is heavily dependent on age verification procedures which are still far from fool-proof and are open to fraud (although it could be argued that the primary

---

363. UK Code at p2.

responsibility of the mobile industry is to prevent accidental rather than deliberate access to adult material for minors.) It also still remains to be seen just how successful content rating systems will be. Content on the wider Internet will pose larger problems as it cannot be rated and restricted by mobile operators in the same way as commercial content. Therefore, it is likely that the most effective approach will be to combine the utilization of filtering software, content labels and URL block lists (Zittrain 2004).

It is also worth emphasising that in addition to the country-wide measures outlined above, there are many examples of self-regulation practiced by an individual network operator. In the UK, for example, both Vodafone and 3 have introduced additional measures: 3 by offering access only to a walled garden of rated content, and Vodafone by anticipating consumer concerns and introducing 'access control' measures which restrict access to adult content unless the user is over 18 and chooses to opt in. This self-regulating behaviour is particularly interesting in the context of large operators which operate in multiple national markets; thus Vodafone has introduced its content control systems not only in the UK where a code of practice exists but also in the Netherlands which lacks such a code.

It still remains to be seen whether child safety will become a key branding issue for mobile operators in the same way it has for fixed-line ISPs such as AOL, but it should at least be clear that business interests need not be harmed by the implementation of child protection measures; in fact there are tremendous gains to be made by operators who can show they have reduced the risks to children. With the global market for adult content on mobile handsets predicted to grow to around \$ 1 billion by 2008<sup>364</sup>, mobile operators who are trusted to prevent minors accessing harmful content will be free to capitalize on the opportunities offered by highly lucrative adult services.

## **Conclusions and recommendations from the EICN**

It is still 'early days' as far as control of harmful content accessed via mobile phones is concerned. Codes of practice have been introduced and limited public consultations held, but it remains to be seen how these solutions will work in practice, or how rigorously the codes will be applied by the mobile and content industries. Further, it is not yet clear how significant a risk will be posed to children by use of these phones, but it is important that policymakers be aware of the potential issues and are prepared to work with industry and consumers to prevent harm where appropriate.

On the basis of these various observations and against the backdrop of the analytical report prepared by the OII, the European Internet Coregulation Network draws the following conclusions concerning the regulation of commercial and Internet-based content:

---

364. Child Protection Unlocks Wireless Adult Content Market. Yankee Group study, released 25/10/2004.

1) That the various types of content and services which can be accessed via mobile phones may pose risks to minors and that policy responses to this issue should be considered.

2) That the European Commission and EU member states should monitor and learn from the operation of mobile codes of practice in the UK, Ireland and Italy & also fund or undertake research providing more information about children's use of mobile phones.

3) That coregulation, as the policy-making process involving industry, governments and user groups in the regulatory debate, is probably the most appropriate approach to this issue, as it offers the most scope for stakeholders' wishes to be taken into account, while also potentially offering more transparency in the application of the regulatory initiatives adopted than self-regulation alone. This leaves open the possibility that within an over-arching coregulatory framework, the different types of mobile content might be subject to differing levels of regulatory or self-regulatory control, as is the case in the UK.

4) That members of the Network should, in accordance with the principle of coregulation, engage with industry, government and user groups in their own countries to discuss the appropriateness of introducing measures for protecting minors from harmful content accessed via mobile phones, and that the European Commission should do the same. Where appropriate, members of the Network should further endeavour to develop and promote a Code of Practice as a contribution to the coregulatory process in their own states.

5) Further, as issues of child protection and Internet access are a source of concern in many European countries, and as several of the largest mobile operators have a presence in more than one country, policy debates should be undertaken at the European, not just national levels. This would still allow individual states to determine what content should be available to which age group according to their own cultural norms.

6) The introduction of codes of practice would seem to be a suitable policy response to this problem when arrived at in a genuinely coregulatory manner and backed up, as appropriate, by the introduction of an independent body for monitoring and ensuring application of the codes.

7) As the basis for an international framework for child protection and mobile phones, the Network propose a common set of principles which national codes of practice could be built on :

- The Internet and other forms of digital content are potentially of huge benefit to children for educational, recreational and cultural reasons. In order for this potential benefit to be maximised, children's inadvertent access to harmful content should be minimised, and this applies to content accessed via mobile phones as well as PCs.

- Awareness-raising and media literacy training are key to empowering parents and children to use the Internet safely; both government and industry have responsibilities to bear on this issue.



- In order to support the restriction of certain content to users of particular age groups in accordance with countries' own standards of decency and appropriateness, content classification and age rating should be employed to control access to commercial content, and site blocking and filtering tools should be employed to limit access to wider Internet content.
- Independent rating bodies could have a role to play in classifying any content offered by the operators as premium services according to national standards and in adjudicating resultant disputes.
- Interactive services used by minors, such as chatrooms, should be moderated where appropriate.
- Handset manufacturers and network operators should continue to undertake research looking at new, more accurate and non-intrusive ways of managing access to content by minors through mobile phones, especially on the wider Internet.

## References

- Ahlert, Christian, Alexander, Marcus & Damian Tambini. 2003. *European 3G Mobile Industry Self-Regulation: IAPCODE Background Paper*, Paper delivered at the World Telemedia Conference, Prague. Available online at: <http://www.selfregulation.info/iapcoda/031106-mobiles-revised-bckgrd.pdf>
- DfES, 2002. *Young People and ICT 2002*, London: DfES. Available online at: [http://www.dfes.gov.uk/ictinschools/uploads/genericdocs/Young\\_People\\_ICT\\_2002.pdf](http://www.dfes.gov.uk/ictinschools/uploads/genericdocs/Young_People_ICT_2002.pdf)
- European Internet Coregulation Network. 2004. *Child Protection on the Internet. Preventing the Exposure of Children to Harmful Content. A Political Statement*. Available online at: <http://network.foruminternet.org/IMG/pdf/childprotection-policystatement.pdf>
- Livingstone, Sonia. 2004. *UK Children Go Online*, ESRC. Available online at: <http://www.children-go-online.net/>
- Marsden, Chris. 2004. Is Peer to Peer the Next Mobile Regulation Challenge? Editorial for PCMLP Self Regulation Review, February 2004. Available online at: <http://www.selfregulation.info/iapcoda/0402xx-selfregulation-review.htm>
- Vincent, Jane. 2005: *Examining mobile phone and ICT use amongst children aged 11 to 16*, Digital World Research Centre, University of Surrey, available online at: <http://www.surrey.ac.uk/dwrc/People/Vincent.htm>
- Zittrain, J. and Edelman, B. 2004. 'Documentation of Internet Filtering Worldwide', pp137-148 in Hardy, C. and Moller, C. eds *Spreading the Word on the Internet: 16 Answers to 4 Questions*, Vienna, OSCE

Cinquième partie

# **Les perspectives de l'année 2006**

# **Les perspectives de l'année 2006**

par Isabelle Falque-Pierrotin

La montée en puissance du Wi-fi, le développement de l'internet mobile et de la voix sur IP sont autant d'avancées technologiques qui aident l'internet à s'installer encore davantage dans notre vie quotidienne, dans la sphère professionnelle comme personnelle. Au-delà de la technique, c'est par l'usage que les bouleversements de fond se font jour. Qui aurait pu prédire le raz de marée des blogs? Le développement du téléchargement de musique et de films en ligne? L'explosion de la téléphonie sur l'internet? Les internautes modèlent l'internet au quotidien, façonnant ainsi les enjeux de demain.

En France, le cadre juridique est en place sur la plupart des questions liées à l'internet. 2006 devrait être une nouvelle année record en matière de commerce électronique en France. La mise en place de moyens permettant d'assurer la protection des mineurs sur l'internet sera effective en 2006 en France, sous l'action conjointe de la responsabilisation des acteurs et de la prise de conscience des familles sur ce sujet sensible, sous l'impulsion des pouvoirs publics. Sur tous ces sujets, le Forum pourra se prévaloir de jouer son rôle dans ces évolutions, de par ses travaux de concertation et ses actions d'information sur ces questions.

De surcroît, son entrée progressive dans le domaine des labels lui donne de nouvelles possibilités de réflexion et d'action au sein du secteur des communications électroniques.

## **Les objectifs 2006 du Forum des droits sur l'internet**

### La concertation

Les groupes de travail créés en 2005 sont en cours et remettront leurs travaux courant 2006 sur les thèmes suivants :

#### **Certificat citoyen**

Ce groupe de travail finalisera ses conclusions début 2006. Celles-ci définiront un référentiel commun de pratiques pour les fournisseurs d'accès et de services matérialisé par un label. Le Forum postule à la gestion de ce label.

#### **Classification des contenus multimédias mobiles**

Les résultats des travaux sur la classification des contenus multimédias mobiles seront communiqués au cours de l'année 2006. Le Forum assura le suivi de ses propositions auprès des opérateurs de téléphonie mobile et des éditeurs de services.

De nouveaux groupes de travail verront le jour en 2006 :

### **Application du droit de la consommation à la vente sur l'internet**

L'objectif de ce groupe sera, à partir de l'ensemble des problématiques référencées, de faire des propositions adressées aux pouvoirs publics (modification législative ou réglementaire) ou aux acteurs eux-mêmes (interprétations de règles existantes, etc.) tendant à assurer une adaptation du droit de la vente à distance aux éventuelles spécificités de l'internet.

### **Vente de médicaments sur l'internet**

Ce groupe de travail analysera les problématiques liées à l'accessibilité sur le territoire français des officines étrangères, l'importation de produits pharmaceutiques commercialisés illégalement et la création d'officines électroniques en France.

### **Accès public à l'internet**

Un groupe de travail devrait être mis en place sur l'accès public à l'internet, avec pour mission à clarifier les définitions et le cadre réglementaire applicables à l'ensemble des usages (accès à l'internet depuis les points d'accès public – cybercafés, associations, collectivités publiques – et accès à l'internet en entreprise).

D'autres groupes de travail pourront être créés, en fonction de l'actualité, de la saisine des pouvoirs publics ou des demandes des membres.

## L'information et la sensibilisation

### **Les sites**

La refonte du site institutionnel Foruminternet.org est prévue en 2006.

Les différents sites du Forum, Foruminternet.org, le site d'information grand public Droitdunet.fr, ou encore le site du service de médiation Mediateurdunet.fr devraient continuer de connaître un accroissement significatif de leur trafic.

### **De nouveaux guides pratiques**

Les guides de sensibilisation au bon usage de l'internet destinés aux parents et aux enfants devraient faire l'objet d'une nouvelle édition.

Un guide d'information des cyber-consommateurs sur les achats en ligne sera élaboré fin 2006, pour la troisième année consécutive.

Un guide sur l'utilisation d'internet au travail est envisagé, à destination des salariés et des entreprises.

## Programme d'événements

En 2006, le Forum continuera de développer des événements, notamment à destination de ses membres. De nouveaux événements ouverts au public verront le jour dans une optique de sensibilisation aux enjeux sociétaux de l'internet.

### La médiation

Le succès enregistré par le service de médiation depuis sa création en 2004 devrait permettre à celui-ci de continuer son développement en 2006. Le soutien du service par le ministère de la Justice démontre tout l'intérêt de ce ministère pour le déploiement de la médiation dans notre pays. Quant aux entreprises, une prise de conscience s'opère quant à l'efficacité de la méthode et la nécessité pour elles de soutenir une telle démarche, complémentaire de leur service client.

Le Forum avec son service de médiation a montré le chemin à suivre. Il continuera son action sur le terrain en 2006 et formalisera, par ailleurs, ses échanges avec les pouvoirs publics et les acteurs économiques pour assurer la pérennité de son service.

### La coopération internationale

Les membres du Réseau européen de corégulation de l'internet (EICN) continueront de se réunir sur une base régulière en 2006 et programmeront de nouveaux travaux. De nouveaux pays, comme l'Espagne, devraient rejoindre le réseau.

Dans le cadre de son rapport «*Protecting Minors from Exposure to Harmful Content on Mobile Phones*», remis en juillet 2005 à la Commissaire européenne Viviane Reding, le Réseau recommandait l'élaboration, dans les pays qui n'en sont par encore dotés, de codes de conduite suivant le principe de corégulation, sur la base de bonnes pratiques (classification des contenus commerciaux, modération des services interactifs...). Le Forum des droits sur l'internet a mis en œuvre cette recommandation en France en créant un groupe de travail sur la classification des contenus mobiles. D'autres membres du Réseau développeront de tels codes de conduite en concertation avec les acteurs concernés (utilisateurs, industriels, pouvoirs publics) dans chacun de leurs pays.

En outre, le réseau EICN a proposé à la Commission européenne, à la suite du Sommet de Tunis, de mettre en place une infrastructure européenne multi-acteurs, permettant à l'Europe d'apporter une contribution concrète au projet de Forum sur la gouvernance de l'internet qui doit se dérouler en Grèce au printemps 2006. Ce projet est à l'étude au sein des services de la Commission.

# Table des matières

<b>Préface</b>	5
<b>Internet: la sortie de l'enfance</b>	7
<b>Le Forum des droits sur l'internet en 2005</b>	9
Fonctionnement du Forum en 2005	9
<i>Un renforcement de l'équipe de médiation</i>	9
<i>Un budget stable</i>	9
<i>Renouvellement au sein des organes dirigeants</i>	9
Missions du Forum des droits sur l'internet	10
Les actions de concertation entre les acteurs publics et privés sur les enjeux juridiques de l'internet	10
<i>Les recommandations des groupes de travail</i>	10
Les actions d'information et de sensibilisation	13
La médiation	14
La coopération internationale à travers le réseau européen de corégulation de l'internet	15
Annexes	
<i>Composition du Conseil d'orientation</i>	16
<i>Composition du Conseil de surveillance</i>	17
<i>L'équipe du Forum des droits sur l'internet</i>	17
<i>Les adhérents du Forum des droits sur l'internet (décembre 2005)</i>	18
<i>Barème des cotisations 2005</i>	19
<b>Les enjeux de droit et de société en 2005</b>	21
Lutte contre la cybercriminalité	21
<i>La conservation des données de connexion</i>	21
<i>La responsabilisation des intermédiaires techniques</i>	26
<i>La responsabilité de l'éditeur du site</i>	28
Protection de l'enfance	29
<i>L'accompagnement des familles dans leur usage des nouvelles technologies</i>	29

<i>La systématisation de l'offre de logiciels de filtrage</i>	30
<i>La responsabilité des créateurs de sites pornographiques accessibles aux mineurs</i>	31
Propriété intellectuelle	32
<i>Les poursuites diligentées à l'encontre des éditeurs de logiciels d'échange de fichiers</i>	33
<i>Les poursuites diligentées à l'encontre des utilisateurs des réseaux peer-to-peer</i>	34
<i>Les questions relatives aux liens hypertextes</i>	35
<i>Les enjeux de la protection d'une œuvre dans le contexte international</i>	37
Commerce électronique	38
<i>L'encadrement de la tacite reconduction des contrats de consommation</i>	39
<i>L'archivage des contrats électroniques</i>	39
<i>La nouvelle responsabilité civile des transporteurs postaux</i>	40
<i>La dématérialisation de certaines formalités et procédures contractuelles</i>	41
<i>La lutte contre les pratiques commerciales illicites ou abusives</i>	44
<i>Le régime de responsabilité de l'affilié et de l'affilieur</i>	46
<i>La vente de produits pharmaceutiques et para-pharmaceutiques en ligne</i>	47
Droit du travail	48
<i>La vie privée numérique du salarié</i>	48
<i>La liberté d'expression des syndicats</i>	49
<i>La diffusion d'offres d'emploi en ligne</i>	51
Administration électronique	51
<i>La fixation du nouveau régime d'accès aux documents administratifs et de diffusion des données publiques</i>	51
<i>Le renforcement de l'accessibilité des personnes handicapées</i>	53
<i>La création du service public de changement d'adresse</i>	54
<i>Le développement du vote électronique</i>	54
Première partie	
<b>LA CONCERTATION</b>	
LES RECOMMANDATIONS DU FORUM DES DROITS SUR L'INTERNET PUBLIÉES EN 2005	57
<b>Les enfants du net (II) : pédo-pornographie et pédophilie sur l'internet</b>	59
Introduction	59

<i>Champ des recommandations</i>	60
<i>Méthodologie</i>	60
La diffusion et le recel de pédo-pornographie sur l'internet	61
<i>Évaluation générale du phénomène</i>	62
<i>État des moyens en vue de combattre la diffusion et le recel de pornographie enfantine sur l'internet, et des limites de ces moyens</i>	69
L'utilisation de l'internet aux fins de préparer une atteinte sexuelle sur un mineur	94
<i>Perception et réalités des risques associés à certains usages de l'internet</i>	94
<i>L'action des parties concernées et ses limites</i>	101
Recommandations	112
<i>Mieux connaître les usages et les risques</i>	112
<i>Sensibiliser les jeunes internautes et les adultes</i>	115
<i>Développer les outils favorisant la maîtrise des usages de l'internet</i>	118
<i>Engager une réflexion spécifique sur le droit et l'organisation du dispositif répressif</i>	121
<i>Renforcer la coopération internationale policière et judiciaire</i>	124
Conclusion	
Poursuivre la réflexion sur les réseaux mobiles et les nouveaux supports d'accès à l'internet	125
Annexe 1	
Composition du groupe de travail	127
Annexe 2	
Auditions et entretiens par le groupe de travail	128
Annexe 3	
Bibliographie	129
<b>Liens commerciaux :</b>	
<b>prévenir et résoudre les atteintes aux droits des tiers</b>	132
Introduction	132
<i>Contexte et objectifs</i>	132
<i>Fonctionnement des liens commerciaux et rôle des acteurs dans la sélection des mots-clés</i>	133
Recommandation aux personnes s'estimant victimes d'une atteinte portée à leurs droits	134
Recommandation aux annonceurs	135



Recommandation aux fournisseurs de liens commerciaux	135
Annexe 1	
Composition du groupe de travail	137
Annexe 2	
Auditions réalisées par le groupe de travail	138
<b>Commerce entre particuliers sur l'internet: quelles obligations pour les vendeurs et les plates-formes de mise en relation ?</b>	139
Introduction	139
<i>Méthodologie suivie</i>	140
<i>Plan du rapport</i>	140
Le cadre général de la vente par un particulier sur l'internet	141
<i>Les plates-formes de mise en relation: une relation tripartite aux contours juridiques difficiles</i>	141
<i>Le régime de responsabilité des plates-formes de mise en relation</i>	143
<i>Les principaux acteurs de la mise en relation</i>	149
Le régime juridique de la vente par un particulier sur l'internet	153
<i>Les règles applicables à tout vendeur sur l'internet</i>	153
<i>Les règles spécifiques applicables au vendeur professionnel</i>	168
<i>Le régime fiscal et social</i>	181
Conclusion	183
Annexe 1	
Composition du groupe de travail	185
Annexe 2	
Auditions réalisées par le groupe de travail	186
Annexe 3	
Schémas synthétiques du processus contractuel	187
<b>La conservation électronique des documents</b>	188
Introduction	188
<i>Plan du rapport</i>	190
La conservation électronique des documents: état des lieux	190
<i>Le cadre juridique de la conservation des documents</i>	190
<i>Le cadre technique entourant la conservation électronique des documents</i>	196

Mettre en place un environnement de confiance	202
<i>Les modalités d'une conservation de l'écrit électronique</i>	203
<i>Les moyens complémentaires de garantir la mise en place d'un environnement de confiance</i>	211
<i>Pistes de prospective pour la confiance dans l'environnement électronique</i>	215
<b>Annexe 1</b>	
Synthèse des recommandations	223
<i>Modalités d'une conservation électronique des documents</i>	223
<i>Les moyens complémentaires de garantir la mise en place d'un environnement de confiance</i>	224
<i>Pistes de prospective pour la confiance dans l'économie numérique</i>	224
<b>Annexe 2</b>	
Composition du groupe de travail	225
<b>Annexe 3</b>	
Auditions	226
<b>Deuxième partie</b>	
<b>L'INFORMATION ET LA SENSIBILISATION</b>	229
<b>Rapport sur le projet de carte nationale d'identité électronique (CNIE)</b>	231
Introduction	231
Les points forts du débat public	232
<i>Sur les questions centrales</i>	232
<i>Sur les questions plus générales</i>	253
Analyse critique du processus du débat	257
<i>Le débat est-il efficient ?</i>	259
<i>Le débat public est-il fiable ?</i>	261
Analyse et recommandations du Forum des droits sur l'internet	262
<i>Les enjeux de sécurité sont essentiels aux yeux des Français mais les arguments avancés à l'appui du projet n'ont pas convaincu</i>	263
<i>La protection de la vie privée est une préoccupation majeure à laquelle le projet doit apporter des garanties complémentaires</i>	264
<i>Des incertitudes à lever en termes de sécurité</i>	265
<i>L'articulation entre le projet INES et celui de dématérialisation de l'état civil</i>	266
<i>Une attente mitigée par rapport à une carte de services</i>	266
	335

<i>Des réticences sur le caractère payant et obligatoire de la carte nationale d'identité électronique</i>	267
<i>Un débat devant le Parlement sur le caractère obligatoire</i>	267
<i>La sensibilité de l'enjeu territorial</i>	267
<i>Le contexte européen</i>	268
Conclusion	268
Annexe 1	
Lettre de mission	269
Annexe 2	
Experts intervenus aux débats en ligne et en région	271
Annexe 3	
Comptes rendus des débats en régions et en ligne et les contributions des experts en ligne	273
<i>Liens vers les comptes rendus des débats itinérants</i>	273
<i>Liens vers les comptes rendus des débats en ligne (du 1<sup>er</sup> février au 7 juin 2005)</i>	274
<i>Liens vers les contributions des experts en ligne</i>	274
Annexe 4	
Le sondage Ipsos / Forum des droits sur l'internet 20 et 21 mai 2005	275
<b>Les autres publications du Forum des droits sur l'internet</b>	277
<b>Troisième partie</b>	
<b>LA MÉDIATION</b>	279
Bilan d'activité 2004-2005	281
Bilan quantitatif du service	282
<i>Les chiffres clés du service</i>	282
<i>Profil des utilisateurs et montant des différends</i>	284
<i>Efficacité du service</i>	285
<i>Comportements à risque</i>	287
Le déroulement de la médiation	289
<i>Un processus de traitement en cinq étapes</i>	289
<i>Règlement de médiation</i>	294
<i>Organisation du service</i>	295
Conclusion	297

Annexe 1	
Les chiffres clés du service de médiation	298
Annexe 2	
Règlement de médiation	299
<b>Quatrième partie</b>	
<b>LA COOPÉRATION INTERNATIONALE</b>	305
<b>Policy Statement on Internet Governance</b>	307
<i>EICN philosophy of regulation</i>	308
<i>Recommendations for a good « internet governance »</i>	310
<b>Report on Protecting Minors from Exposure to Harmful Content on Mobile Phones</b>	313
Introduction	313
Background	314
Mobile Content – the State of Play	315
<i>Mobiles vs PCs</i>	314
<i>Harmful Content ?</i>	316
<i>Should children’s access to mobile content be a policy concern ?</i>	317
Possible policy responses ?	318
Conclusions and recommendations from the EICN	322
<b>Cinquième partie</b>	
<b>LES PERSPECTIVES DE L’ANNÉE 2006</b>	
par Isabelle Falque-Pierrotin	325
Les objectifs 2006 du Forum des droits sur l’internet	327
<i>La concertation</i>	327
<i>L’information et la sensibilisation</i>	328
<i>La médiation</i>	329
<i>La coopération internationale</i>	329