N° 608

(2ère partie)

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 février 2003.

AVIS

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 (n° 528) *pour la* **confiance** *dans l'***économie numérique,**

PAR MME MICHÈLE TABAROT,

Député.

Voir le numéro :

Assemblée nationale : **612.**

Audiovisuel et communication.

SOMMAIRE

Pages

Article 16

(art. L. 134-2 [nouveau] du code de la consommation)

Conservation de la preuve du contrat conclu par voie électronique

L'article 16 introduit un nouvel article L. 134-2 dans le code de la consommation, qui met à la charge du contractant professionnel l'obligation de conserver l'écrit qui constate le contrat pendant un certain délai, déterminé par décret, et en garantit l'accès à tout moment à son cocontractant si celui-ci en fait la demande, dès lors que le contrat conclu par voie électronique porte sur une somme supérieure ou égale à un certain montant, à fixer par ce même décret.

L'article 16 recouvre des enjeux de première importance. Dans la mesure où il est peu probable que des parties ayant contracté par voie numérique doublent le contrat de documents papiers, la question de la conservation du contrat devient dès lors cruciale. Comme le souligne fort justement Maître Eric Caprioli, non seulement elle intervient, le cas échéant, dans l'administration de la preuve auprès des tribunaux, mais elle est également déterminante dans la production de pièces justificatives aux agents de diverses administrations (douanes, impôts, caisses sociales et de retraite).

Cette disposition pose ainsi la question, toujours complexe, de l'archivage des contrats. Elle rejoint le problème similaire soulevé par l'article 1316-1 du code civil : « *Comment conserver des données numériques tenant lieu de documents à valeur juridique, lesquels restent soumis, ne l'oublions pas, à des règles formulées le plus souvent pour l'archivage sur des supports papier ? L'archivage ne correspond-il pas à l'idée de pérennité de l'information avec la possibilité de la restituer intacte ?* » [(1)]. Nul besoin d'ajouter que cette question recouvre, qui plus est, une dimension économique importante, la mise en œuvre de modalités de conservation efficaces du contrat requérant l'acquisition de moyens techniques spécialement dédiés (double disque, disque amovible, réseau spécifique, etc.).

Dans cette perspective, la question des montants concernés et des délais envisagés apparaît comme cruciale, ces deux paramètres pouvant, selon la combinaison qui est retenue, déterminer l'importance du matériel technique requis pour le stockage des données.

Concernant le montant, s'agira-t-il du seuil de 800 euros défini par le décret n° 80-533 du 15 juillet 1980 – modifié par le décret n° 2001-476 du 30 mai 2001 portant adaptation de la valeur en euros du montant exprimé en francs – pris pour l'application de l'article 1341 du code civil, selon lequel « *il doit être passé acte devant notaires ou signatures privées de toutes choses excédant une somme ou une valeur fixée par décret* » ? Interrogé sur ce point par votre rapporteur pour avis, le gouvernement n'est pas en mesure d'apporter de réponse à ce stade.

---

(1) Eric Caprioli, « Variations sur le thème du droit de l'archivage dans le commerce électronique *», Petites affiches, 18-19 août 1999, n° 164.*

La question des délais appelle un préalable méthodologique nécessaire à la compréhension de l'ensemble des données du problème : en effet, « *une distinction fondamentale s'impose, qui concerne les délais de conservation obligatoires des documents archivés et les délais de prescriptions relatifs aux droits et obligations y afférant* » (1), même s'il est vrai que cette distinction présente un intérêt relatif au vu de l'identité des délais. Sur cette question non plus, votre rapporteur pour avis n'a pas obtenu d'informations précises.

Le gouvernement souhaite en effet se donner le temps de la réflexion sur ces questions et mener une concertation étroite avec tous les acteurs concernés, qui devrait débuter au cours de la présente année, sous l'égide de la mission pour l'économie numérique créée en mars 2001 au sein du ministère de l'économie et des finances. Comme l'a indiqué à votre rapporteur pour avis M. Gilles Brégant, secrétaire général de la mission pour l'économie numérique, le Gouvernement est totalement ouvert aux propositions des utilisateurs et des professionnels des services en ligne et s'est fixé pour objectif de parvenir à un accord qui satisfasse l'ensemble des intérêts en présence.

La Commission a *émis un avis favorable* à l'adoption de cet article sans modification.

Article 24

Pouvoirs des agents spécialisés en matière de constatation des infractions au régime de la cryptologie

Parce que la cryptologie est un instrument technologique hautement sophistiqué, il importe que les personnels chargés de veiller au respect de son régime d'emploi, qui est déterminé par le présent projet, soient spécialisés en cette matière. Le présent article a précisément pour objet de prévoir la création d'une telle catégorie d'agents, ainsi que les modalités de leur intervention.

• ***La création d'une nouvelle catégorie d'agents spécialisés dotés de pouvoirs de police judiciaire***

Le premier alinéa de cet article prévoit que les agents compétents pour constater par procès verbal les infractions aux dispositions des articles 18, 19, 22 et 23 du présent projet tendant à la libéralisation de l'usage de la cryptologie, sont « *habilités à cet effet par le Premier ministre* » et « *assermentés dans des conditions fixées par décret en Conseil d'État* ».

Bien évidemment, cette compétence ne doit pas avoir pour effet d'interdire l'intervention des autres agents investis de pouvoirs de police judiciaire et le début du premier alinéa le précise expressément. En effet, on rappellera que la mission de la police judiciaire de droit commun est de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs tant qu'une information n'est pas ouverte (article 14 du code de procédure pénale). Celle-ci peut donc être amenée à conduire des investigations en matière de fraude au régime légal de la

(1) *Eric Caprioli, «* Variations sur le thème du droit de l'archivage dans le commerce électronique *», Petites affiches, 18-19 août 1999, n° 164.*

cryptologie sans devoir pour autant se dessaisir de l'affaire au profit des agents habilités. De même, il ne saurait être question de priver les agents des douanes des prérogatives qu'ils détiennent en application des dispositions de l'article 64 du code des douanes, qui les autorisent à rechercher et à constater les infractions aux dispositions du code des douanes dont l'application en matière d'importation ou d'exportation illégales de matériel de cryptologie n'est pas à exclure. Là aussi, la rédaction du présent article préserve leurs compétences.

En raison de leur statut d'agents habilités bénéficiant de pouvoirs de police judiciaire, les prérogatives qui leur sont attribuées doivent être strictement déterminées par la loi. Le deuxième alinéa de cet article s'y emploie en précisant qu'ils peuvent accéder *« aux locaux, terrains ou moyens de transport à usage professionnel en vue de rechercher et de constater les infractions, demander la communication de tous les documents professionnels et en prendre copie, recueillir, sur convocation ou sur place, les renseignements et justifications »*. En outre, il est indiqué qu'ils ne peuvent accéder à ces locaux que pendant leurs heures d'ouvertures au public et, à défaut, entre 8 heures et 20 heures. On observera qu'à la différence des officiers de police judiciaire de droit commun auxquels est reconnue la possibilité, sous certaines conditions prévues par le code de procédure pénale, de procéder à des visites domiciliaires, les agents habilités au titre du présent article *« ne peuvent accéder aux locaux qui servent de domicile »* à l'intéressé. Cette restriction n'est pas sans rappeler celle opposable à d'autres agents spécialisés dotés de pouvoirs de police judiciaire, à l'instar des inspecteurs du travail qui, en application des dispositions de l'article L. 611-8 du code du travail, ne peuvent pénétrer dans les locaux qui servent de domicile qu'après en avoir reçu l'autorisation des occupants.

- ***Des investigations placées sous le contrôle de magistrats qui peuvent autoriser la confiscation des matériels de cryptologie***

Le droit commun, en particulier l'article 12 du code de procédure pénale, place la police judiciaire sous la direction du procureur de la République. Le dispositif proposé par le présent article ne retient pas formellement cette solution mais aboutit à un régime juridique qui s'en approche. En effet, le troisième alinéa du présent article dispose que le procureur de la République est *« préalablement informé des opérations envisagées en vue de la recherche des infractions »* et qu'il peut s'opposer à celles-ci. Dans ces conditions, ce magistrat exerce bien, de fait, la direction des investigations menées par les agents habilités. De surcroît, il est destinataire dans les cinq jours des procès verbaux dressés par les agents dont une copie est d'ailleurs remise à l'intéressé.

A ce contrôle exercé par un magistrat du parquet, s'ajoute l'intervention d'un juge du siège lorsque les agents habilités désirent procéder à la saisie de moyens de cryptologie. Ainsi, le quatrième alinéa du présent article prévoit que les agents habilités peuvent saisir de tels moyens sur autorisation judiciaire donnée par ordonnance du président du tribunal de grande instance ou du juge des libertés et de la détention. A cet égard, il est quelque peu surprenant que des agents dotés de pouvoirs de police judiciaire, placés de fait sous le contrôle du procureur de la République, soient autorisés à s'adresser directement à un magistrat du siège aux fins de saisie de matériel de cryptologie. Il semblerait en effet préférable, notamment

en termes d'efficacité de la réponse pénale, de prévoir que la demande de saisie est transmise aux magistrats du siège par l'intermédiaire du procureur de la République qui pourra, compte tenu de ses résultats, décider de mettre en œuvre ou non l'action publique conformément aux dispositions de l'article 31 du code de procédure pénale. A titre d'illustration, on fera observer que la procédure de saisie conservatoire en matière de terrorisme prévue par l'article 706-24-2 du même code est ordonnée par le juge des libertés et de la détention sur requête du procureur de la République.

S'agissant de la demande de saisie, il est prévu qu'elle doit comporter « *tous les éléments d'information* » de nature à la justifier. Sur le fond, l'intervention de juges du siège, inamovibles ainsi que le prévoit l'article 64 de la Constitution, constitue une garantie essentielle et nécessaire dans le cadre d'une procédure susceptible de conduire à la saisie de biens privés. Il demeure toutefois que l'on peut s'interroger sur l'opportunité d'offrir au procureur de la République, le choix de saisir le président du tribunal de grande instance ou le juge des libertés et de la détention qui a lui-même le rang de président, de premier vice-président ou de vice-président ainsi que le précise l'article 137-1 du code de procédure pénale. En effet, dans un souci de simplification procédurale et afin de prévenir d'inévitables divergences de jurisprudences au sein d'une même juridiction, il semblerait préférable d'unifier dans les mains d'un seul des deux magistrats du siège précités le pouvoir d'autoriser la saisie de moyens de cryptologie.

Après avoir *adopté* un amendement du rapporteur pour avis, corrigeant une erreur de référence (**amendement n° 52**), la Commission a *adopté* un amendement du même auteur prévoyant que la demande de saisie des matériels de cryptologie présentée par les agents spécialisés doit être transmise par l'intermédiaire du procureur de la République au seul président du tribunal de grande instance ou au juge du siège délégué par lui (**amendement n° 53**).

A supposer que lesdits magistrats du siège autorisent les agents habilités à procéder à la saisie de moyens de cryptologie, cette opération s'effectuera sous leur contrôle et leur autorité ainsi que le précise la dernière phrase du quatrième alinéa du présent article. Comme le prévoit le texte, les matériels saisis feront immédiatement l'objet d'un inventaire qui sera annexé au procès-verbal dressé sur les lieux, les originaux de ces documents étant transmis au juge ayant ordonné la saisie. Enfin, en contrepartie de ce pouvoir, le présent article confère aux magistrats du siège le droit à tout moment, d'office ou sur la demande de l'intéressé, d'ordonner la mainlevée de la saisie.

On observera néanmoins que le dispositif proposé par le présent article n'indique pas ce qu'il advient des pièces saisies. Sont-elles confisquées sans aucune limite de durée, constituent-elles des pièces susceptibles d'être versées au dossier de la procédure si le procureur de la République décide de mettre en œuvre l'action publique ? Cette dernière solution semble préférable et mériterait d'être précisée. A l'initiative de son rapporteur pour avis, la Commission a *adopté* un amendement en ce sens (**amendement n° 54**).

Puis la Commission a *émis un avis favorable* à l'adoption de cet article ainsi modifié.

Article 25

(art. 132-76 [nouveau] du code pénal)

Aggravation des sanctions pénales en cas d'utilisation d'un moyen de cryptologie pour préparer ou commettre une infraction

La libéralisation de la cryptologie proposée par l'article 18 du présent projet doit, corrélativement, s'accompagner du renforcement des sanctions pénales encourues par les personnes qui l'utiliseront à des fins criminelles. Tel est précisément l'objet du présent article, qui fait de l'usage de la cryptologie une circonstance aggravante lorsque ce procédé *« a été utilisé pour préparer ou commettre un crime ou un délit ou pour en faciliter la préparation ou la commission ».* Toutefois, lorsque le législateur est désireux d'aggraver les sanctions pénales à raison du recours à un procédé particulier, deux méthodes s'offrent à lui.

La première, dont la 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 mineurs, est une bonne illustration, constitue à insérer dans chaque incrimination la référence particulière à l'usage dudit procédé. En l'espèce, la loi du 17 juin 1998 a souhaité entraver le développement du réseau Internet en matière d'exploitation sexuelle en faisant de *« l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunications »* une circonstance aggravante pour un certain nombre de crimes et délits qu'elle a modifiés à cet effet. Il en est ainsi, à titre d'exemple, de la pédo-pornographie (troisième alinéa de l'article 227-23 du code pénal) ou du proxénétisme (10° de l'article 225-7 du même code). Or, cette démarche emporte le risque d'omettre un certain nombre d'incriminations, sachant qu'il en existerait dans notre droit, selon certaines estimations, près de 15 000, dont les auteurs échapperont, de ce fait, au renforcement de la répression souhaité par le législateur, ce qui n'est pas satisfaisant.

C'est pourquoi la méthode suivie par le présent article est différente et tend, à l'inverse, à prévoir une disposition de portée générale aggravant les peines encourues dans tous les cas d'utilisation d'un moyen de cryptologie. A cet effet, le présent article insère dans le code pénal, au sein du titre III, relatif aux peines, du livre premier, regroupant les dispositions générales, un article 132-76 nouveau qui aggrave les sanctions pénales en se référant au quantum de la peine encourue lorsque le crime ou le délit a été commis de façon ordinaire, sans avoir recours à un moyen de cryptologie. Cette méthode est également celle qui a été retenue en matière de terrorisme, comme le montre l'article 421-3 du code pénal.

Ainsi, le 1° de l'article 132-76 dispose que lorsque le crime est puni de trente ans de réclusion criminelle, la peine est portée à la réclusion à perpétuité dans l'hypothèse où un moyen de cryptologie a été utilisé pour sa préparation ou sa commission. Le 2° procède la même manière et porte la peine à trente ans de réclusion criminelle lorsque l'infraction est punie de vingt ans de réclusion. Le 3° porte la peine d'emprisonnement à vingt ans de réclusion criminelle lorsque l'infraction est punie de quinze ans de réclusion ; le 4° la porte à quinze ans de réclusion criminelle lorsque l'infraction est punie de dix ans d'emprisonnement ; le 5° la porte à dix ans d'emprisonnement lorsque les faits sont passibles de cinq ans d'emprisonnement et le 6° porte à sept ans d'emprisonnement la peine encourue

lorsque l'infraction est punie de cinq ans d'emprisonnement. Enfin, s'agissant des délits punis de trois ans d'emprisonnement au plus, le 7° dispose que le maximum de la peine privative de liberté est porté au double lorsqu'un moyen de cryptologie a été utilisé.

Au-delà de cette légitime aggravation des sanctions pénales, le dispositif proposé introduit néanmoins une rare novation dans notre droit pénal, qu'il convient de relever. En effet, le dernier alinéa de l'article 132-76 nouveau dispose que ces sanctions ne sont pas applicables à *« l'auteur ou au complice de l'infraction qui, à la demande des autorités judiciaires, leur a remis la version en clair des messages chiffrés ainsi que les conventions secrètes nécessaires au déchiffrement ».*

Ce faisant, il s'agit d'introduire la notion, aujourd'hui étrangère au droit français, de « repenti » qui soulève certaines interrogations. En effet, si l'objectif poursuivi est d'améliorer l'interpellation des auteurs d'une infraction grâce à la protection offerte à l'un d'entre eux désireux de coopérer avec les autorités judiciaires, ce que l'on peut comprendre, la portée générale du dispositif proposé n'emporte pas pleinement l'adhésion de votre rapporteur pour avis. En effet, est-il envisageable, de renoncer à l'aggravation des peines à l'endroit d'un auteur de crime, un terroriste par exemple, ayant recouru à la cryptologie et qui fournirait ensuite les moyens de déchiffrer les messages qu'il a envoyés ? A tout le moins, le champ de l'exception prévue par le dernier alinéa de cet article, devrait, pour les infractions les plus graves, être limité aux seuls complices.

Après avoir *adopté* un amendement rédactionnel du rapporteur pour avis (**amendement n° 55**), la Commission a *adopté* un amendement du même auteur limitant le champ d'application de la procédure d'atténuation des peines en prévoyant d'exclure de son bénéfice les auteurs des infractions punies d'une peine supérieure à quinze ans d'emprisonnement (**amendement n° 56**). La Commission a ensuite *émis un avis favorable* à l'adoption de cet article ainsi modifié.

Article 26

(art. 11-1 [nouveau] de la loi n° 91-646 du 10 juillet 1991
et art. 434-15-2 [nouveau] du code pénal)

Interceptions de sécurité de messages cryptés - sanctions pénales en cas de refus de communiquer leur convention de déchiffrement

A la suite des attentats commis le 11 septembre 2001, les investigations menées par les services de police américains et européens ont révélé que les terroristes avaient largement eu recours aux réseaux numériques et à des messages cryptés pour échanger des informations et préparer leurs crimes. C'est pourquoi, nombre de gouvernements ont décidé d'adopter des dispositions spécifiques afin de renforcer l'efficacité de la lutte contre le terrorisme.

S'agissant de la France, des dispositions en ce sens ont été introduites dans la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne mais leur validité est limitée à une durée « *allant jusqu'au 31 décembre 2003* », ainsi que le prévoit son article 22. Or, chacun conviendra que la menace terroriste n'a nullement disparue et qu'il n'est pas souhaitable, ni prudent, de se priver d'un certain nombre d'instruments juridiques à partir du 31 décembre prochain.

C'est pourquoi le présent article a pour objet de pérenniser les dispositions introduites par l'article 31 de la loi du 15 novembre 2001 précitée et qui sont relatives aux interceptions de sécurité et aux sanctions pénales encourues par les personnes refusant de remettre aux autorités judiciaires la convention de déchiffrement des messages. A cet effet, le paragraphe I du présent article abroge l'article 31 de la loi du 15 novembre 2001, tandis que ses deux paragraphes suivants reprennent littéralement son dispositif pour l'insérer de façon pérenne dans notre droit positif.

• ***La possibilité de procéder à des interceptions de sécurité de messages cryptés est prévue***

Le paragraphe II du présent article tend à insérer un article 11-1 nouveau dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. Son dispositif prévoit que les personnes assurant des prestations de cryptologie sont tenues de remettre aux agents « *autorisés dans les conditions prévues à l'article 4* », sur leur demande, les conventions permettant le déchiffrement des données cryptées au moyen des prestations qu'elles ont fournies.

On rappellera que l'article 3 de la loi du 10 juillet 1991 qui détermine les conditions autorisant le recours aux interceptions de sécurité prévoit qu'elles sont autorisées « à titre exceptionnel » et doivent avoir pour objet de « *rechercher les renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, ou la prévention du terrorisme, de la criminalité ou de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous en application de la loi du 10 janvier 1936 sur les groupes de combat et les milices privées* ». S'agissant des autorités

compétentes pour autoriser ces interceptions, l'article 4 précité prévoit que seul le Premier ministre, ou l'une des deux personnes spécialement déléguées par lui, peuvent ordonner une telle mesure par une « *décision écrite et motivée* ». Cette autorisation n'est valable que pour une durée maximale de quatre mois, mais est renouvelable dans les mêmes conditions de forme et de durée, ainsi que le prévoit l'article 6 de la même loi. Enfin, l'on observera que les renseignements ainsi recueillis ne peuvent servir à d'autres fins que celles énumérées à l'article 3 mais ne font pas obstacle à l'application des dispositions du deuxième alinéa de l'article 40 du code de procédure pénale qui, rappelons-le, oblige toute autorité constituée, tout officier public ou fonctionnaire d'informer sans délai le procureur de la République des crimes ou délits dont il acquiert la connaissance dans l'exercice de ses fonctions.

La cryptologie étant une discipline hautement complexe, le dispositif proposé par l'article 11-1 nouveau prévoit, fort prudemment, que les agents autorisés peuvent demander aux fournisseurs de prestations de cryptologie de « *mettre eux-mêmes en œuvre ces conventions* » de déchiffrement, sauf si ceux-ci démontrent qu'ils ne sont pas en mesure de satisfaire à ces réquisitions. Afin de garantir l'efficacité des réquisitions adressées par les agents habilitées, le deuxième alinéa de l'article 11-1 nouveau punit d'une peine de deux ans d'emprisonnement et de 30 000 euros d'amende le fait de ne pas y déférer. Pour sa part, le dernier alinéa de cet article renvoie à un décret en Conseil d'État le soin de préciser les procédures suivant lesquelles l'obligation de transmettre les conventions de déchiffrement est mise en œuvre et les conditions de sa prise en charge financière par l'État.

- ***Des sanctions pénales en cas de refus de communiquer aux autorités judiciaires la convention de déchiffrement ayant servi à la préparation ou à la commission d'une infraction sont introduites***

Le paragraphe III du présent article insère au sein de la deuxième section, relative aux entraves à l'exercice de la justice, du chapitre IV du titre III du livre IV du code pénal, un article 434-15-2 nouveau qui punit de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie « *susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit* », de refuser de la mettre à la disposition des autorités judiciaires, procureur de la République ou juge d'instruction, qui en font la demande. Le second alinéa de cet article aggrave la sanction en la portant à cinq ans d'emprisonnement et 75 000 euros d'amende si ce refus « *aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets* ».

Ces dispositions complètent utilement le droit en vigueur qui ne permet pas de sanctionner ce type de comportement. En effet, les différentes dispositions de la deuxième section précitée sanctionnent, notamment, la menace commise envers un magistrat ou un juré (article 234-8 du code pénal), leur tentative de subornation (234-9), le fait, pour quiconque connaissant la preuve de l'innocence d'une personne, de refuser de témoigner (article 234-11), le témoignage mensonger (article 234-13) ou encore la subornation d'un interprète ou d'un expert (articles 434-19 et 434-21) mais non l'usage de la cryptologie qui peut, indéniablement, constituer une entrave à l'exercice de la justice.

La Commission a *émis un avis favorable* à l'adoption de cet article sans modification.

Section 5

Saisine des moyens de l'État pour la mise au clair de données chiffrées

Article 27

(titre IV [nouveau] du code de procédure pénale)

Réquisition des moyens de décryptage

A l'instar du précédent, le présent article a pour objet de pérenniser des dispositions de la loi du 15 novembre 2001, et plus précisément celles figurant à l'article 30, relatives à la « *mise au clair des données chiffrées nécessaires à la manifestation de la vérité* ». A cette fin, le paragraphe I du présent article abroge l'article 30 précité dont les dispositions sont insérées dans le code de procédure pénale par le paragraphe II qui introduit, après l'article 230 dudit code, un titre IV nouveau qui regroupe les articles 230-1 à 230-5 nouveaux.

Sur le fond, l'article 230-1 nouveau prévoit que, lorsqu'il apparaît que des données saisies ou obtenues au cours d'une enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'y accéder en clair, le procureur de la République ou, le cas échéant, le juge d'instruction peut « *désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire* ».

Ces dispositions spécifiques aux messages cryptés s'appliquent sans préjudice de l'application des dispositions de droit commun du code de procédure pénale (articles 60, 77-1 et 156), qui confèrent aux officiers de police judiciaire, au procureur de la République ou au juge d'instruction, le droit de recourir à « *toutes personnes qualifiées* » s'il y a lieu de procéder à des constatations ou à des examens techniques ou scientifiques, ainsi que le rappelle le premier alinéa de l'article 230-1 nouveau.

Toutefois, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, le juge d'instruction mais également la juridiction de jugement saisie de l'affaire peuvent « *prescrire le recours aux moyens de l'État soumis au secret de la défense nationale* » selon les modalités prévues par les articles 230-2 et 230-3 nouveaux du code de procédure pénale. Il s'agit de permettre, dans les affaires les plus graves et les plus complexes, de renforcer l'efficacité des poursuites et des investigations judiciaires en facilitant l'accès des magistrats à des moyens particulièrement sophistiqués, aujourd'hui réservés aux seules forces en charge de la défense nationale.

A supposer que les magistrats ou les juridictions précités décident de recourir auxdits moyens, il est nécessaire d'en prévoir les modalités pratiques. Tel est précisément l'objet de l'article 230-2 nouveau qui dispose que ce recours doit prendre la forme d'une réquisition écrite « *adressée au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information* » et accompagnée du support physique contenant les données à mettre au clair. La réquisition doit préciser les délais dans lesquels les opérations de mise au clair doivent être réalisées, sachant que l'autorité judiciaire requérante peut ordonner l'interruption des opérations prescrites.

En l'état actuel de l'organisation administrative des services de la police judiciaire, l'organisme compétent pour traiter de ces réquisitions est l'Office central de lutte contre la criminalité liée aux technologies de l'information (OCLCTIC) créé par le décret n° 2000-405 du 15 mai 2000. Toutefois, on observera que la rédaction proposée par le présent article est formulée en des termes suffisamment neutres pour ne pas désigner uniquement l'OCLCTIC et permettra, en conséquence, à son dispositif de ne pas devenir inapplicable en raison d'une modification ultérieure des structures administratives du ministère de l'intérieur.

Une fois saisi, le service de police judiciaire transmet sans délai la réquisition à un organisme technique soumis au secret de la défense nationale et désigné par décret. En effet, l'OCLCTIC, office central à vocation interministérielle et à compétence nationale a, certes, pour mission de réaliser des enquêtes judiciaires technologiquement complexes et d'assister techniquement d'autres services de police judiciaires, par exemple en matière de pédophilie sur Internet ou de trafic de stupéfiants, mais il n'a pas vocation à mettre en œuvre directement l'ensemble des moyens technologiques nécessaires, qui exigent des compétences extrêmement variées (des ingénieurs et des informaticiens) et des moyens humains considérables.

Toutefois, le dernier alinéa de l'article 230-2 indique que les données protégées au titre du secret de la défense nationale ne peuvent être communiquées que dans les conditions prévues par la loi n° 98-567 du 8 juillet 1998 instituant une Commission consultative du secret défense. On rappellera que cette commission est une autorité administrative indépendante qui a pour objet de donner un avis à la suite de la demande d'une juridiction française tendant à la déclassification et la communication d'informations ayant fait l'objet d'une classification en application des dispositions de l'article 413-9 du code pénal. Ce dernier définit les données présentant un « *caractère de secret de la défense nationale* » comme les renseignements, procédés, objets, documents, données informatiques ou fichiers « *dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale* ».

Pour sa part, l'article 230-3 nouveau précise les modalités de transmission des résultats des opérations tendant à la mise au clair des données. Ainsi, dès leur achèvement, ou dès qu'il apparaît que ces opérations sont impossibles, ou à l'expiration du délai prescrit par l'autorité judiciaire, les résultats sont retransmis au service national de la police judiciaire, qui les remet « *immédiatement* » à l'autorité requérante. Fort logiquement, ces résultats sont accompagnés des indications techniques utiles à leur compréhension, ainsi que d'une attestation visée par le responsable de l'organisme technique « *certifiant la sincérité des résultats*

transmis ». Enfin, le dernier alinéa de cet article dispose que les éléments ainsi obtenus font l'objet d'un procès verbal et sont versés au dossier de la procédure. Cette précision est d'importance puisqu'elle garantit que les éventuels éléments de preuve ainsi obtenus seront accessibles aux parties et pourront, le cas échéant, être contestés selon les voies de recours de droit commun. En revanche, les décisions judiciaires de recourir aux moyens permettant la mise au clair des données ne doivent pas pouvoir faire l'objet de contestations car elles constituent des mesures d'investigations ne revêtant pas le caractère juridictionnel. L'article 230-4 nouveau le prévoit expressément et peut d'ailleurs être rapproché des dispositions du second alinéa de l'article 100 du même code, qui indique que la décision du juge d'instruction de prescrire l'interception des correspondances émises par la voie des télécommunications « *n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours* ».

Enfin, l'article 230-5 nouveau se borne à préciser que, sans préjudice des obligations découlant du secret de la défense nationale, les agents requis en application des dispositions des articles 230-1 et suivants sont tenus d'apporter leur concours à la justice.

En conclusion, les dispositions du présent article, ainsi que celles figurant à l'article précédent constituent le juste corollaire de la libéralisation du régime de la cryptologie prévue par l'article 18 du présent projet. En effet, si la libéralisation de ces moyens a pour principal objet de sécuriser les échanges d'informations sur les réseaux en garantissant leur confidentialité, ce qui devrait sans conteste améliorer la confiance des acteurs en la matière et contribuer au développement économique de ce secteur, elle ne saurait avoir pour effet d'amoindrir la capacité d'élucidation des services de police judiciaire. En renforçant les moyens technologiques au service de la police et des autorités judiciaires tout en sanctionnant pénalement le refus de mettre à leur disposition les conventions de déchiffrement ayant servi à préparer ou à commettre une infraction, le texte propose un juste équilibre entre ces deux exigences.

La Commission a *émis un avis favorable* à l'adoption de cet article sans modification.

CHAPITRE II

Lutte contre la cybercriminalité

Le développement des technologies de l'information, et tout particulièrement d'Internet, constitue indéniablement un progrès dans le droit reconnu à chacun d'accéder librement aux informations qu'il recherche, mais représente également un facteur considérable de gains de productivité pour les entreprises et de croissance pour l'ensemble de l'économie, qu'il convient d'encourager. Quelques données statistiques illustrent clairement cette dimension. Ainsi, le nombre des foyers possédant un PC est passé de 4,074 millions en 2001 (soit 16,7 % d'entre eux) à près de 5,40 millions au premier trimestre 2002 (soit 22 % des foyers). S'agissant du commerce électronique entre les entreprises et les

consommateurs (dit « B to C »), son montant a atteint 2 350 millions d'euros en 2002 contre 685 millions seulement en 2000, soit une progression de 343 % [1].

Les graphiques suivants illustrent clairement l'impact macroéconomique croissant des technologies de l'information et de la communication (TIC). Ainsi, la part de l'investissement en TIC dans l'investissement productif est passée, en France, de 6,8 % en 1980 à 14,4 % en 2000.

PART DE L'INVESTISSEMENT EN TIC DANS L'INVESTISSEMENT PRODUCTIF

En % (calculs sur données en valeur [1])

Types d'investissement en TIC	Années	France	Etats-Unis
Équipements de communication	1980	2,5	5,1
	1990	3,5	7,0
	1995	3,9	8,7
	2000	4,4	8,3
Logiciels	1980	1,3	3,0
	1990	2,6	8,0
	1995	3,5	10,1
	2000	6,1	13,6
Équipements de communication	1980	2,9	7,1
	1990	3,2	7,5
	1995	3,5	7,3
	2000	3,9	8,0
Total TIC	1980	6,8	15,2
	1990	9,4	22,5
	1995	10,8	26,1
	2000	14,4	29,9

(1) Les données en valeur ont plus de sens que les données en volume à cause de l'utilisation d'indices chaînes.

Source : Colecchia-Schreyer (2001), tableau 2, in *Le contre-choc de la « nouvelle économie », une étude de cas sur cinq pays de l'OCDE, La revue de l'OFCE, octobre 2002, p. 254.*

La conséquence économique de cette part croissante des investissements en TIC se traduit dans l'augmentation de leur contribution annuelle moyenne à la croissance du PIB. En effet, celle-ci s'établissait en France, producteurs et utilisateurs de TIC confondus, à 0,8 point de PIB entre 1996 et 1999, soit 42 % de l'ensemble de la croissance obtenue, contre seulement 0,3 % entre 1990 et 1995, soit 33 % du total de celle-ci (voir le tableau ci-contre)

CONTRIBUTION ANNUELLE MOYENNE À LA CROISSANCE DU PIB

Points de pourcentage

	Producteurs de TIC		Utilisateurs de TIC		Croissance du PIB	
	1990-1995	1996-1999	1990-1995	1996-1999	1990-1995	1996-1999
Finlande	0,3	1,5	– 0,5	1,0	– 0,5	5,1
France	0,2	0,5	0,1	0,3	0,9	1,9
Pays-Bas	0,1	0,6	0,5	1,3	2,1	3,7
États-Unis	0,4	0,8	0,5	1,9	2,3	4,7

Les contributions sont calculées en pondérant la variation annuelle du PIB en volume de chaque secteur par la part du PIB de ce secteur en (t-1) dans le PIB total.
Le total n'est pas égal à la somme des composantes du fait des arrondis.

Source : Van Ark (2001), in *Le contre-choc de la « nouvelle économie », une étude de cas sur cinq pays de l'OCDE, La revue de l'OFCE, octobre 2002, p. 254.*

(1) Source : www.journaldunet.com

Cependant, comme toute innovation, les technologies de l'information ont également généré de nouveaux types de comportements délictueux dont le développement altère la confiance des acteurs dans la sécurité des réseaux et entrave son expansion. L'ampleur de la « cybercriminalité » semble néanmoins difficile à évaluer puisque les statistiques recensent les infractions selon leur nature et non en fonction des moyens techniques utilisés par leurs auteurs. Dès lors, toutes les estimations de ce phénomène criminel sont nécessairement fondées sur des extrapolations des données existantes ce qui les rend contestables. De surcroît, s'agissant des atteintes aux systèmes de traitement automatisé de données (STAD), qui sont pourtant des infractions spécifiques, ni les statistiques de la délinquance établies par le ministère de l'intérieur selon la nomenclature de « l'état 4001 », ni celles figurant au sein de l'annuaire statistique de la justice ne les font apparaître distinctement, ce qui est regrettable. Il serait d'ailleurs tentant, vraisemblablement à tort, d'en déduire leur caractère non significatif. En effet, il est probable que les entreprises ou les administrations victimes de ces délits sont réticentes à les déclarer afin de ne pas altérer la confiance des internautes ou de leurs clients dans la sûreté de leur réseau. Cependant, selon les informations communiquées à votre rapporteur pour avis, les faits de cybercriminalité seraient passés de moins d'une dizaine en 1988 à près de 2 000 en l'an 2000.

Sur le plan juridique, la cybercriminalité regroupe principalement deux catégories de crimes et délits : ceux de droit commun commis à l'aide ou exclusivement sur les réseaux numériques, et les atteintes spécifiques aux systèmes informatiques ou aux données personnelles. Or, la répression de ces infractions est aujourd'hui imparfaitement assurée par les dispositions en vigueur en raison de l'inadaptation des incriminations aux spécificités des délits numériques. Ainsi, la répression des infractions de droit commun commises à l'aide de, ou exclusivement sur, les réseaux numériques, à l'instar de la diffusion de contenus illicites, relève de l'application de la loi pénale générale, mais très peu d'incriminations ont été adaptées aux spécificités des réseaux numériques, ce qui n'est pas satisfaisant. On mentionnera toutefois, que constitue une circonstance aggravante le fait de commettre le délit de proxénétisme *« grâce à l'utilisation, pour la diffusion de message à destination d'un public non déterminé, d'un réseau de télécommunications »* [(1)], ce qui désigne, sans ambiguïté, l'hypothèse du recours à Internet [(2)] mais il s'agit là d'un exemple isolé.

Quant aux infractions spécifiques contre les biens, le nouveau code pénal comporte, au sein du chapitre III du titre II du livre troisième, les articles 321–1 à 323–7 réprimant les atteintes aux systèmes de traitement automatisé des données (STAD), mais ces dispositions, introduites par la loi dite « Godfrain » du 5 janvier 1988, n'ont pas été actualisées pour prendre en considération le développement d'Internet et notamment l'introduction d'un « virus » informatique.

Si le droit pénal semble incomplet, il en est de même des règles du code de procédure pénale En effet, les instruments dont disposent les officiers de police

---

(1) Cf. 9° de l'article 225-7 du code pénal introduit par la loi n° 98-468 du 17 juin 1998.

(2) De même, l'article 227-23 du code pénal, qui punit de trois ans d'emprisonnement et de 45 000 € d'amende le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation à caractère pornographique d'un mineur, porte les peines à 5 ans d'emprisonnement et 75 000 € d'amende lorsqu'un réseau de télécommunications a été utilisé pour la diffusion de ces images à destination d'un public non déterminé.

judiciaire dans la recherche des preuves des infractions n'ont pas été conçus au temps de l'univers numérique et dématérialisé, ni même adaptés à celui-ci. Il en est ainsi de la nature des pièces susceptibles d'être saisies dans le cadre des perquisitions. ou des horaires pendant lesquels elles peuvent avoir lieu. Dès lors, si l'on est fondé à plaider en faveur d'un « toilettage formel » de certaines dispositions du code de procédure pénale, d'autres modifications, plus substantielles, doivent être également envisagées afin d'améliorer la réactivité des services en charge des enquêtes.

Le Gouvernement et sa majorité sont déterminés à s'engager dans cette voie. D'ores et déjà, à l'initiative du rapporteur du projet de loi pour la sécurité intérieure (1), l'Assemblée nationale a adopté des dispositions permettant le recours à des perquisitions en ligne ou facilitant la mise à disposition, par la voie numérique, des données nécessaires à l'enquête et qui sont requises par les officiers de police judiciaire auprès des opérateurs de télécommunications. Par ailleurs, le Garde des Sceaux prépare un projet de loi renforçant les instruments juridiques destinés à la lutte contre la criminalité organisée, qui devrait également prendre en considération les spécificités de la cybercriminalité en l'attente de l'introduction dans notre droit interne des obligations qui découlent de la signature par la France de la convention du Conseil de l'Europe sur la cybercriminalité.

Pour leur part, les articles du présent chapitre du projet de loi constituent l'une des premières étapes de la nécessaire adaptation des règles du droit pénal et de la procédure pénale à la délinquance numérique qui, au-delà de l'actualisation formelle des pièces susceptibles d'être saisies dans le cadre des perquisitions ou de l'exécution d'une commission rogatoire délivrée par le juge d'instruction (articles 30 à 32), renforcent le quantum des peines encourues en matière d'atteinte aux STAD (article 33) et introduisent une nouvelle incrimination permettant de sanctionner le recours aux « virus informatiques » (article 34).

Article 30

(art. 56 du code de procédure pénale)

Perquisitions en flagrant délit - Modification des pièces susceptibles d'être saisies et des modalités de leur conservation

Introduit par la loi n° 57-1426 du 31 décembre 1957, le premier alinéa de l'article 56 du code de procédure pénale dispose que, si la nature du crime est telle que la preuve en puisse être acquise par la *« saisie de papiers, documents ou autres objets »* en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte *« sans désemparer »* au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal. Inchangée depuis son introduction dans le code de procédure pénale, cette disposition ne mentionne pas les données informatiques dont l'invention et le développement lui sont postérieurs.

Or, cette situation n'est pas satisfaisante car elle ne correspond pas aux investigations effectivement menées par les services de police judiciaire, qui sont

(1) Cf. rapport n° 508, du 26 décembre 2002.

parfois contraints de saisir l'ensemble du support informatique, qui constitue un « objet », alors que seules quelques données précises sont nécessaires à la manifestation de la vérité. C'est pourquoi les deux premiers alinéas du présent article ont pour objet de compléter la liste des pièces susceptibles d'être saisies par les officiers de police judiciaire (OPJ) en insérant la référence, d'une part, aux « *données informatiques* » en la possession des personnes qui paraissent avoir participé au crime et, d'autre part, aux « *informations* » relatives aux faits incriminés.

Au-delà de ces adaptations strictement formelles, le présent article a également pour objet d'adapter les modalités de saisie et de conservation desdites données informatiques. En effet, le droit en vigueur est silencieux en matière de reproduction de données informatiques, alors même que l'une de leurs principales caractéristiques est la facilité et la rapidité avec laquelle cette tâche peut être réalisée.

C'est pourquoi, le 3° du présent article substitue au cinquième alinéa de l'article 56 précité trois nouveaux alinéas qui permettent aux OPJ de placer sous main de justice une copie des données informatiques dont la saisie est nécessaire à la manifestation de la vérité. Toutefois, afin de garantir l'authenticité et la non-altération des données copiées par rapport aux originales, le dispositif proposé prévoit que cette opération ne peut être réalisée *« qu'en présence des personnes qui assistent à la perquisition »*. En conséquence, dans l'hypothèse où ces dernières seraient absentes, seul le support physique contenant les données pourrait être saisi et placé sous scellé comme le prévoit le droit en vigueur.

A supposer que les données saisies soient copiées, il ne saurait pour autant être question de les laisser à la disposition des auteurs de l'infraction. En effet, il n'est pas concevable que les détenteurs d'images pornographiques de mineurs numérisées, qui entrent dans le champ des sanctions prévues par l'article 227-23 du code pénal, soient laissés en possession de celles-ci une fois la copie réalisée par les OPJ. C'est pourquoi, le deuxième alinéa du 3° du présent article prévoit que, sur instruction du procureur de la République, il peut être procédé à l'effacement définitif des données sur le support physique qui n'a pas été placé sous main de justice et dont la *« détention ou l'usage est illégal ou dangereux pour la sécurité des personnes et des biens »*.

Enfin, le dernier alinéa du présent article, reprend pour l'essentiel les dispositions de l'actuel cinquième alinéa de l'article 56 du code de procédure pénale qui prévoit que, avec l'accord du procureur de la République, l'officier de police judicaire ne maintient que la saisie des objets, documents et *« données informatiques »* utiles à la manifestation de la vérité. Il convient de préciser que les modifications ainsi introduites en matière de perquisition dans le cadre des enquêtes de flagrance s'appliqueront également à celles menées au cours d'une enquête préliminaire en application des dispositions de l'article 76 du code de procédure pénale. En effet, le dernier alinéa de cet article renvoie, s'agissant des « formes » de la perquisition et donc des pièces susceptibles d'être saisies, à celles figurant à l'article 56 du code de procédure pénale, précisément modifié par le présent article du projet.

La Commission a *émis un avis favorable* à l'adoption de cet article sans modification.

Articles 31 et 32

(art. 94 et 97 du code de procédure pénale)

Perquisitions dans le cadre d'une instruction – Modification des pièces susceptibles d'être saisies et des modalités de leur conservation

Par coordination avec les modifications apportées par le précédent article à l'article 56 du code de procédure pénale, l'article 31 du projet a pour seul objet de prévoir expressément la possibilité de saisie de *« données informatiques »* dans le cadre des perquisitions ordonnées par le juge d'instruction en application des dispositions de l'article 94 du code de procédure pénale.

Pour sa part, l'article 32 du présent projet modifie l'article 97 du même code, dont le premier alinéa prévoit que le juge d'instruction, ou l'officier de police judiciaire qu'il a commis à cet effet, peuvent rechercher et prendre connaissance des *« documents »* nécessaire à l'instruction. De même, le deuxième alinéa de cet article dispose que « *tous les objets et documents »* placés sous main de justice sont immédiatement inventoriés et placés sous scellés. Enfin, le cinquième alinéa du même article prévoit que, si les nécessités de l'instruction ne s'y opposent pas, *« copie ou photocopie des documents »* placés sous main de justice peuvent être délivrés à leurs frais aux intéressés qui en font la demande. Là encore, afin de prendre en considération les conséquences du développement de l'informatique, il est proposé de compléter la liste des documents et objets susceptibles d'être saisis ou reproduits par la référence aux « *données informatiques* ».

Par ailleurs et à l'instar des modifications proposées par l'article 30 du projet de loi, le 5° de l'article 32 autorise la réalisation d'une copie des données informatiques saisies, qui doit également être réalisée « *en présence des personnes qui assistent à la perquisition* ». Par coordination, le juge d'instruction ayant fait procéder à la copie de données informatiques peut ordonner leur effacement du support initial qui n'a pas été placé sous main de justice lorsque leur détention ou usage est *« illégal ou dangereux pour la sécurité des personnes et des biens ».*

La Commission a *émis un avis favorable* à l'adoption de ces articles sans modification.

Article 33

(art. 323-1 à 323-3 du code pénal)

Aggravation des peines encourues par les auteurs des atteintes aux systèmes de traitement automatisé de données

Introduits par la loi du 5 janvier 1988, dite loi « Godfrain », les articles 323-1 à 323-7 du code pénal répriment les atteintes aux systèmes de traitement automatisé de données (STAD). Ainsi, le premier alinéa de l'article 323–1 punit d'un an d'emprisonnement et de 15 000 € d'amende le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un STAD sachant que, lorsqu'il en est résulté

la suppression ou la modification de données qui y sont contenues ou l'altération de son fonctionnement, les peines sont portées à deux ans d'emprisonnement et 30 000 € d'amende par les dispositions du deuxième alinéa du même article. En outre, le fait d'entraver ou de fausser le fonctionnement d'un STAD est puni de trois ans d'emprisonnement et de 45 000 € d'amende, comme le prévoit l'article 323-2. Enfin, l'article 323-3 sanctionne d'une peine de trois ans d'emprisonnement et de 45 000 € d'amende le fait d'introduire frauduleusement des données dans un STAD ou de supprimer ou de modifier frauduleusement les données qu'il contient.

Bien que novatrices lors de leur introduction dans notre code pénal, ces dispositions n'ont pas été modifiées depuis et le quantum des peines encourues ne semble manifestement plus en rapport avec les dommages subis par les victimes des infractions précédemment décrites. En effet, selon certaines études (1) menées sur la base d'un échantillon de 3 286 entreprises américaines et européennes, les pertes moyennes engendrées par l'effacement de données ou l'attaque du réseau depuis l'extérieur seraient, respectivement, de l'ordre de 24 625 euros et de 54 380 euros. Ces montants particulièrement élevés démontrent la nocivité économique des atteintes aux STAD et incitent le législateur à renforcer les sanctions encourues par les auteurs de ces infractions.

Tel est précisément l'objet du présent article, qui aggrave l'ensemble des peines encourues par les auteurs des infractions précitées. Ainsi, il est proposé que les peines prévues par l'article 323-1 du code pénal soient désormais de deux ans d'emprisonnement et de 30 000 euros d'amende et soient portées à trois ans d'emprisonnement et 45 000 euros d'amende lorsqu'il en est résulté la suppression, la modification de données ou l'altération du fonctionnement du STAD. S'agissant des peines encourues par les auteurs des délits prévus à l'article 323-2, le paragraphe II du présent article les porte à cinq ans d'emprisonnement et 75 000 euros d'amende. Enfin, les auteurs d'un délit sanctionné par les dispositions de l'article 323-3 seront désormais passibles d'une peine de cinq ans d'emprisonnement et de 75 000 euros d'amende.

La Commission a *émis un avis favorable* à l'adoption de cet article sans modification.

Article 34

(art. 323-3-1 [nouveau], 323-4 et 323-7 du code pénal)

Création d'une nouvelle incrimination en matière de droit de l'informatique

Ils ont souvent des noms suggestifs comme « Tchernobyl », voire aguicheurs tels que « I love you » ou « Melissa », pour ne citer que les plus connus, mais leurs conséquences sont ravageuses pour les systèmes informatiques qui en sont les victimes. Les virus informatiques sont, en effet, l'un des avatars les plus néfastes du développement des réseaux numériques. Selon une étude menée sur un vaste échantillon d'entreprises américaines et européennes (2), l'introduction d'un

(1) Source : OMNI Consulting Group cité par le journal du net, www.journaldunet.com
(2) Source : OMNI Consulting Group, cité par le journal électronique : www.journaldunet.com

virus dans le système informatique entraîne une perte moyenne de plus de 26 000 euros pour les sociétés qui en sont victimes.

Or, face au développement de ces pratiques hostiles, le droit pénal français n'apporte pas de réponse pleinement satisfaisante. En effet, l'article 323-1 du code pénal réprime l'accès frauduleux dans tout ou partie d'un système de traitement automatisé de données (STAD), alors même que, dans bien des cas, les virus y sont introduits d'une façon régulière, par l'intermédiaire des messageries personnelles des salariés par exemple. De même, l'article 323-3 qui sanctionne le fait d'introduire frauduleusement des données dans un STAD, ne permet pas de réprimer l'introduction non frauduleuse de telles données par un virus. Pour sa part, l'article 323-2 du même code punit le fait d'entraver ou de fausser le fonctionnement d'un STAD. Or, cette incrimination sanctionne davantage les conséquences de l'introduction d'un virus dans un STAD que le fait de détenir ou de concevoir un tel programme informatique, ce qui peut sembler paradoxal, voire insuffisant en termes d'efficacité de la réponse pénale.

C'est pourquoi, le présent article tend à insérer un article 323-3-1 nouveau du code pénal, qui a pour objet de réprimer le fait de *« détenir, d'offrir, de céder ou de mettre à disposition un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés »* pour commettre les infractions prévues par les articles 323-1 à 323-3. Les peines encourues par les détenteurs ou les fabricants de virus informatiques sont celles prévues par l'infraction commise à l'aide de leur programme. Si l'on prend en considération l'aggravation des peines proposée à l'article précédent du projet de loi, les détenteurs, vendeurs ou pourvoyeurs de programmes informatiques ayant permis la commission des infractions prévues à l'article 323-1 seront désormais passibles d'une peine de trois ans d'emprisonnement de 45 000 euros d'amende, tandis que les auteurs des délits prévus aux articles 323-2 et 323-3 encourront cinq ans d'emprisonnement et 75 000 euros d'amende.

On observera que cette nouvelle incrimination n'est pas sans rappeler celle prévue par les dispositions de l'article L. 163–4–1 du code monétaire et financier [(1)] qui punit de sept ans d'emprisonnement et de 750 000 € d'amende le fait *« de fabriquer, de détenir, de céder, d'offrir ou de mettre à disposition des équipements, instruments, programmes informatiques ou toutes données conçus ou spécialement adaptés »* pour commettre les délits de contrefaçon ou de falsification de cartes de paiement. Cette incrimination tend, notamment, à réprimer le recours à des logiciels de fabrication de faux numéros de cartes de paiement ou de piratage de ceux-ci à l'occasion d'une transaction sur Internet, qui sont ensuite exploités frauduleusement ou mis à la disposition du public sur des sites spécialisés dits de « carding ».

Pour autant, le dispositif du second alinéa de l'article 323-3-1 nouveau du code pénal comporte une différence substantielle par rapport à celui prévu à l'article L. 163-4-1 du code monétaire et financier. En effet, il prévoit que les sanctions pénales ne sont pas applicables lorsque la détention, l'offre, la cession et la mise à disposition sont *« justifiés par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communication électronique et*

(1) Cette disposition a été introduite par la loi du 15 novembre 2001 relative à la sécurité quotidienne.

des systèmes d'information ». Cette exclusion du champ d'application de la sanction pénale a pour premier objet de permettre aux laboratoires scientifiques en informatique, y compris ceux qui travaillent en matière militaire, de poursuivre leurs nécessaires travaux en ce domaine. Elle se justifie également au regard des pratiques des sociétés chargées de concevoir des programmes informatiques de veille, de sécurisation ou de défense des systèmes informatiques et qui ont besoin de concevoir des virus afin de tester la fiabilité de leur propre programme anti-virus.

Toutefois, sur le plan juridique, cette exclusion du champ de la responsabilité pénale soulève certaines interrogations. En effet, il est quelque peu curieux de prévoir une irresponsabilité pénale absolue pour des organismes ou des personnes physiques qui ont détenu ou conçu des programmes « spécialement adaptés » pour commettre une infraction. Au regard du principe constitutionnel de la légalité et de la nécessité des peines, une dérogation aussi générale semble d'ailleurs contestable. C'est pourquoi, il semblerait préférable de prévoir que ces organismes ne sont pas responsables lorsqu'ils détiennent ou conçoivent des programmes spécialement adaptés pour commettre « les faits » prévus aux articles précités du code pénal et non les « infractions » réprimées par ces mêmes articles. Cette distinction peut d'ailleurs se justifier sur le fondement du principe général de droit pénal figurant à l'article 121-3 du code pénal selon lequel *« il n'est point de crime ou de délit sans l'intention de le commettre »* puisque, tant les laboratoires de recherche que les sociétés chargées de la veille ou de la sécurisation des systèmes informatiques sont, *a priori*, exempts de toute intention de commettre un crime ou un délit à l'aide de leurs outils informatiques.

Par ailleurs, votre rapporteur pour avis juge le champ de l'exclusion de la responsabilité pénale proposée excessivement large. En effet, les notions de *« besoins de la recherche scientifique et technique »* ou de *« protection et de la sécurité des réseaux de communication »* sont particulièrement imprécises, susceptibles de recouvrir des organismes irréprochables et d'autres qui le seraient moins, certains pouvant être tentés de développer des virus informatiques en excipant de leur mission de sécurisation des réseaux. C'est pourquoi, afin de renforcer les garanties juridiques quant au bon usage des virus informatiques, il serait préférable de prévoir que les organismes, publics et privés, qui sont habilités à mettre en œuvre de tels programmes informatiques procèdent préalablement à une déclaration auprès des services du Premier ministre. Suivant son rapporteur pour avis, la Commission a *adopté* un amendement du rapporteur pour avis en ce sens (**amendement n° 57**).

Enfin, le dernier alinéa du présent article a pour objet, par coordination avec l'introduction de ce nouveau délit, d'insérer dans les articles 323-4 et 323-7, respectivement relatifs à la commission des infractions au STAD en groupement ou à l'aide d'une entente et à la répression de la tentative de commettre ces délits, la référence à l'article 323-3-1.

La Commission a ensuite *émis un avis favorable* à l'adoption de cet article ainsi modifié.

AMENDEMENTS ADOPTES OU POUR LESQUELS LA COMMISSION A ÉMIS UN AVIS FAVORABLE

Article 2

Amendement n° 31 de la Commission :

Rédiger ainsi le I de cet article :

« I. — L'article 17 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication est complété par un alinéa ainsi rédigé :

« Les dispositions du présent article ne s'appliquent pas aux services visés au chapitre VI du titre II. »

(art. 43-8 de la loi n° 86-1067 du 30 septembre 1986)

Amendements n^{os} 32 et 33 de la Commission :

• A la fin de cet article, substituer aux mots : « avec promptitude », les mots : « dans les meilleurs délais ».

• Compléter cet article par l'alinéa suivant :

« Le fait, par quiconque, de caractériser de façon abusive une apparence d'illicéité aux fins d'obtenir le retrait de données ou d'en rendre l'accès impossible est constitutif d'une entrave à la liberté d'expression, du travail, d'association, de réunion ou de manifestation au sens du premier alinéa de l'article 431-1 du code pénal. »

(art. 43-9 de la loi n° 86-1067 du 30 septembre 1986)

Amendement n° 34 de la Commission :

Après les mots : « n'ont pas agi », rédiger ainsi la fin de cet article : « dans les meilleurs délais pour faire cesser la diffusion d'une information ou d'une activité manifestement illicite. »

(art. 43-10 de la loi n° 86-1067 du 30 septembre 1986)

Amendement n° 35 de la Commission :

Au début de cet article, substituer aux mots : « prestataires techniques mentionnés », les mots : « personnes mentionnées ».

(art. 43-11 de la loi n° 86-1067 du 30 septembre 1986)

Amendement n° 36 de la Commission :

Au début de cet article, substituer aux mots : « prestataires techniques mentionnés », les mots : « personnes mentionnées ».

(art. 43-12 de la loi n° 86-1067 du 30 septembre 1986)

Amendement n° 37 de la Commission :

Dans cet article, substituer aux mots : « tout prestataire technique mentionné », les mots : « toute personne mentionnée ».

(art. 43-14 de la loi n° 86-1067 du 30 septembre 1986)

Amendement n° 38 de la Commission :

Dans le premier alinéa du I de cet article, substituer aux mots : « tiennent à la disposition », les mots : « mettent à disposition ».

Amendements n^os^ 39 et 40 de la Commission :

• Compléter cet article par le paragraphe suivant :

« Après l'article 79-6 de la même loi, sont insérés deux articles 79-7 et 79-8 ainsi rédigés :

« *Art. 79-7.* — Est puni de 3 750 euros d'amende le fait, pour une personne physique ou le dirigeant de droit ou de fait d'une personne morale exerçant l'une des activités définies aux articles 43-7 et 43-8, de ne pas avoir conservé les éléments d'information visés à l'article 43-13 ou de ne pas déférer à la demande d'une autorité judiciaire d'avoir communication desdits éléments.

« Les personnes morales peuvent être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du code pénal. Elles encourent une peine d'amende suivant les modalités prévues par l'article 131-38 du code pénal. »

« *Art. 79-8.* — Est puni de 3 750 euros d'amende toute personne physique ou tout dirigeant de droit ou de fait d'une personne morale exerçant l'activité définie à l'article 43-14 qui n'aurait pas respecté les prescriptions de ce même article.

« Les personnes morales peuvent être déclarées pénalement responsables de cette infraction dans les conditions prévues à l'article 121-2 du code pénal. Elles encourent une peine d'amende suivant les modalités prévues par l'article 131-38 du code pénal. »

• Compléter cet article par le paragraphe suivant :

« V. — Dans le dernier alinéa du paragraphe I de l'article 26 de la loi n° 1067 du 30 septembre 1986 relative à la liberté de communication, la référence : "43-16" est substituée à la référence "43-11".

« Il est procédé à la même substitution dans le premier alinéa de l'article 33-1, dans le dernier alinéa du paragraphe I de l'article 44, dans l'article 44-1 et dans le deuxième alinéa du paragraphe I de l'article 53 de la même loi. »

Article 5

(art. L. 34-11 de code des postes et télécommunications)

Amendements n^os^ 41, 42 et 43 et de la Commission :

• Dans la première phrase du premier alinéa du I de cet article, après les mots : « d'attribuer », insérer les mots : « et de gérer ».

• Après les mots : « rendues publiques et qui », rédiger ainsi la fin du deuxième alinéa du I de cet article :

« veillent au respect, par le demandeur, des droits de la propriété intellectuelle. »

• I. — Avant la dernière phrase de l'avant-dernier alinéa du I de cet article, insérer la phrase suivante : « La décision du ministre chargé des télécommunications tendant à la désignation, ou au retrait de la désignation, d'un organisme peut faire l'objet d'un recours devant le Conseil d'État. »

II. — En conséquence, rédiger ainsi la dernière phrase du même alinéa : « Chaque organisme adresse au ministre chargé des télécommunications un rapport d'activité annuel. »

Amendement n° 17 présenté par M. Jean Dionis du Séjour :

Avant le dernier alinéa du I de cet article, insérer l'alinéa suivant :

« L'attribution et la gestion des adresses rattachées à chaque domaine de premier niveau sont centralisées par un organisme unique ».

Après l'article 5

Amendements n^{os} 11, 9, 10 et 8 présentés par M. Patrice Martin-Lalande :

• Insérer l'article suivant :

« I. — A la fin du quatrième alinéa (3°) de l'article 42-1 de la loi du 30 septembre 1986 précitée, les mots : ", si le manquement n'est pas constitutif d'une infraction pénale", sont supprimés.

« II. — Après le premier alinéa de l'article 42-2 de la loi du 30 septembre 1986 précitée, sont insérés deux alinéa ainsi rédigés :

« Lorsque le manquement est constitutif d'une infraction pénale, le montant de la section pécuniaire ne peut excéder celui prévu pour l'amende pénale.

« Lorsque le Conseil supérieur de l'audiovisuel a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que la sanction pécuniaire s'impute sur l'amende qu'il prononce. »

• Insérer l'article suivant :

« L'article 42-4 de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication est ainsi modifié :

« I. — Dans la première phrase, les mots : "titulaires d'autorisation pour l'exploitation d'un service de communication audiovisuelle" sont remplacés par les mots : "éditeurs de services de radiodiffusion sonore ou de télévision".

« II. — Après la première phrase sont insérées deux phrases ainsi rédigées : "Le Conseil supérieur de l'audiovisuel demande à l'intéressé de lui présenter ses observations dans un délai de deux jours francs à compter de la réception de cette demande. La décision est ensuite prononcée sans que soit mise en œuvre la procédure prévue à l'article 42-7."

« III. — La dernière phrase est complétée par les mots : "dans les conditions fixées à l'article 42-2."

• Insérer l'article suivant :

« A la fin de l'article 48-2 de la loi du 30 septembre 1986 précitée, les mots : "et à la condition que le manquement ne soit pas constitutif d'une infraction pénale" sont supprimés. »

• Insérer la division et l'intitulé suivants :

« Chapitre III
« Régulation de la communication ».

Article 7

Amendements n^os^ 44, 45 et 46 de la Commission :

• Avant le I de cet article, insérer le paragraphe suivant :

« I A. — L'activité définie à l'article 6, lorsqu'elle est assurée par des personnes établies en France, s'exerce librement sur le territoire national dans le respect des lois et règlements en vigueur.

« Sont exclus des dispositions de l'alinéa précédent :

« 1° Les jeux d'argent, y compris sous forme de paris et de loteries, légalement autorisés ;

« 2° Les activités de représentation et d'assistance en justice ;

« 3° Les activités des notaires exercées pour l'application des dispositions de l'article 1^er^ de l'ordonnance n° 45-2590 du 2 novembre 1945 relative au statut du notariat. »

• Dans le premier alinéa du I de cet article, après les mots : « sur le territoire national », insérer les mots : « à l'exclusion des activités visées aux 1° à 3° du paragraphe précédent et ».

• Compléter la première phrase du 1° du II de cet article par les mots : « , conformément aux engagements internationaux souscrits par la France ».

Avant l'article 14

Amendement n° 47 de la Commission :

Rédiger ainsi l'intitulé du chapitre III :

« Les obligations souscrites sous forme électronique ».

Article 14
(art. 1369-1 du code civil)

Amendements n^os^ 48 et 49 de la Commission :

• Dans la première phrase du premier alinéa de cet article, après les mots : « Quiconque propose », insérer les mots : « à titre professionnel ».

• Dans la première phrase du premier alinéa de cet article, substituer aux mots : « générales et particulières », le mot : « contractuelles ».

Amendement n^o^ 18 présenté par M. Jean Dionis du Séjour:

Compléter la dernière phrase du premier alinéa de cet article par les mots : « de son fait ».

Amendement n° 50 de la Commission :

Rédiger ainsi le deuxième alinéa de cet article :

« L'offre énonce en outre : ».

(art. 1369-3 du code civil)

Amendement n° 51 de la Commission :

• Rédiger ainsi le début du premier alinéa de cet article :

« Il est fait exception aux obligations visées aux 1° à 5° de l'article 1369-1 et aux deux premiers alinéas ... *(le reste sans changement)* ».

Article 24

Amendements nos 52, 53 et 54 de la Commission :

• A la fin du premier alinéa de cet article, substituer aux mots : « , 22 et 23 », les mots : « et 22 ».

• I. — Après les mots : « du président du tribunal de grande instance », rédiger ainsi la fin de la première phrase du quatrième alinéa de cet article : « ou d'un magistrat du siège délégué par lui, préalablement saisi par le procureur de la République. ».

II. — En conséquence, dans l'avant-dernier alinéa de cet article, substituer aux mots : « le juge des libertés et de la détention », les mots : « ou le magistrat du siège délégué par lui ».

• Compléter le cinquième alinéa de cet article par la phrase suivante : « Ils sont versés au dossier de la procédure. »

Article 25

(art. 132-76 du code pénal)

Amendements nos 55 et 56 de la Commission :

• Dans le premier alinéa de cet article, substituer aux mots : « relative à la communication électronique », les mots : « pour la confiance dans l'économie numérique ».

• Dans le dernier alinéa de cet article, substituer aux mots : « à l'auteur ou au complice de l'infraction qui, », les mots : « au complice d'une infraction punie de plus de quinze ans d'emprisonnement ou à l'auteur ou au complice d'une infraction punie d'une peine inférieure ou égale à quinze ans d'emprisonnement qui, ».

Article 34

(art. 323-3-1 du code pénal)

Amendement n° 57 de la Commission :

I. — Dans le premier alinéa de cet article, substituer aux mots : « une ou plusieurs des infractions prévues », les mots : « les faits prévus ».

II. — En conséquence :

1° Dans le dernier alinéa de cet article, après les mots : « mise à disposition », insérer les mots : « de l'instrument, du programme informatique, ou de toute donnée, » ;

2° Compléter le dernier alinéa de cet article par les mots : « et lorsqu'elles sont mises en œuvre par des organismes publics ou privés ayant procédé à une déclaration préalable auprès du Premier ministre selon les modalités prévues par les dispositions du III de l'article 18 de la loi n° du pour la confiance dans l'économie numérique. »

AMENDEMENTS POUR LESQUELS LA COMMISSION A EMIS UN AVIS DEFAVORABLE

Article premier

Amendement n° 12 présenté par M. Jean Dionis du Séjour :

Rédiger ainsi cet article :

« On entend par communication publique en ligne toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, qui s'appuie sur un procédé de télécommunication permettant un échange réciproque d'information entre l'émetteur et le récepteur.

« On entend par courrier électronique, tout message de correspondance privée, sous forme de texte, de voix, de son ou d'image, envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère.

« La communication publique en ligne est libre.

« L'exercice de cette liberté ne peut être limité que dans la mesure requise, d'une part, par le respect de la dignité de la personne humaine, de la protection de l'enfance et de l'adolescence, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et, d'autre part, par la sauvegarde de l'ordre public, par les besoins de la défense nationale, par les exigences de service public, par les contraintes techniques inhérentes aux moyens de communication.

« Il est institué un Conseil supérieur de la communication publique en ligne.

« Un décret prévoit sa composition, son mode de fonctionnement, ainsi que les conditions dans lesquelles il peut adresser aux éditeurs et distributeurs de services de communication publique en ligne des recommandations relatives au respect des principes énoncés dans la présente loi. Ces recommandations sont publiées au *Journal officiel* de la République française. »

Après l'article premier

Amendement n° 13 présenté par M. Jean Dionis du Séjour :

Insérer l'article suivant :

« Le chapitre VI du titre II de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication est abrogé. »

Article 2

Amendement n° 14 présenté par M. Jean Dionis du Séjour :

Rédiger ainsi cet article :

« I. — Les personnes dont l'activité est d'offrir un accès à des services de communication publique en ligne sont tenues d'informer leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et de leur proposer au moins un de ces moyens.

« II. — Les prestataires techniques mentionnés aux paragraphes III et IV 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.

« Toutefois, les prestataires techniques mentionnés au paragraphe III mettent en œuvre les moyens conformes à l'état de l'art pour prévenir la diffusion de données constitutives 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.

« III. — Les personnes qui assurent, même à titre gratuit, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par des services de communication publique en ligne, ne peuvent voir leur responsabilité civile engagée du fait de la diffusion de ces informations ou activités que si, dès le moment où elles ont eu la connaissance effective de leur caractère manifestement illicite, ou de faits et circonstances faisant apparaître ce caractère manifestement illicite, elles n'ont pas agi avec promptitude pour retirer ces données ou rendre l'accès à celles-ci impossible.

« IV. — Les personnes désignées au paragraphe II ne peuvent voir leur responsabilité pénale engagée que si, en connaissance de cause, elles n'ont pas agi avec promptitude pour faire cesser la diffusion d'une information ou d'une activité dont elles ne pouvaient ignorer le caractère manifestement illicite.

« V. — La personne physique ou morale qui a caractérisé une apparence d'illicéité aux fins d'obtenir le retrait de données ou de rendre leur accès impossible engage sa responsabilité pénale au titre de l'article 431-1 du code pénal, et sa responsabilité civile envers la personne dont les données ont été retirées ou rendues inaccessibles.

« VI. — L'autorité judiciaire peut prescrire sur requête, à tout prestataire technique mentionné aux paragraphes III et IV, toutes mesures propres à faire cesser un dommage occasionné par le contenu d'un service de communication publique en ligne, telles que celles visant à cesser de stocker ce contenu ou, à défaut, à cesser d'en permettre l'accès. »

(art. 43-8 de la loi n° 86-1067 du 30 septembre 1986)

Amendements n^{os} 4 et 5 présentés par M. Patrice Martin-Lalande :

• Rédiger ainsi le début de cet article :

« Les personnes qui fournissent, même à titre gratuit, un service à la société de l'information consistant à stocker des informations fournies par un destinataire du service, pour mise à disposition du public de signaux, d'écrits, d'images, de sons ou de messages de toute nature accessibles par des services de communication publique en ligne, ne peuvent voir leur responsabilité civile engagée… *(le reste sans changement)* »

• Compléter cet article par le paragraphe suivant :

« II. — Une procédure de notification à laquelle pourront, d'une part, les personnes physiques ou morales ayant un intérêt à agir et s'étant identifiées ou, d'autre part, le parquet, est instaurée.

« Cette notification comprend, sous peine de nullité :

« – L'identification de l'auteur de la notification

« – La description des faits litigieux

« – L'emplacement exact du contenu litigieux

« – Les motifs pour lesquels le contenu doit être retiré comprenant la mention dispositions légales et des justifications de fait

« – La copie du courrier électronique envoyé simultanément à l'auteur/éditeur du contenu objet du différend, pour l'informer de la notification ou la justification de ce que l'auteur n'a pu être contacté.

« L'incrimination pénale de dénonciation calomnieuse prévue à l'article 226-10 du code pénal s'étend à la notification abusive. »

(art. 43-12 de la loi n° 86-1067 du 30 septembre 1986)

Amendement n° 6 présenté par M. Patrice Martin-Lalande :

Supprimer cet article.

Après l'article 2

Amendements n^os^ 15 et 16 présentés par M. Jean Dionis du Séjour :

• Insérer l'article suivant :

« Les personnes mentionnées aux paragraphes III et IV de l'article 2 de la présente loi sont tenues de détenir et de 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.

« Elles sont également tenues de fournir aux personnes qui éditent un service de communication publique en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 2 *ter*.

« L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux paragraphes III et IV de l'article 2 des données mentionnées au premier alinéa.

« Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.

« Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation. »

• Insérer l'article suivant :

« I. — Les personnes dont l'activité est d'éditer un service de communication publique en ligne tiennent à la disposition du public :

« *a)* S'il s'agit de personnes physiques, leurs nom, prénom, domicile et numéro de téléphone ;

« *b)* S'il s'agit de personnes morales, leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre du commerce et des sociétés ou au répertoire des métiers, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;

« *c)* Le nom du directeur ou du codirecteur de la publication et, le cas échéant, celui du responsable de la rédaction au sens de l'article 93-2 de la loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle ;

« *d)* Le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone du prestataire mentionné au paragraphe III de l'article 2.

« II. — Les personnes éditant à titre non professionnel un service de communication publique en ligne peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire mentionné au paragraphe III de l'article 2, sous réserve de lui avoir communiqué les éléments d'identification personnelle prévus au I. »

Article 3

Amendement n° 7 présenté par M. Patrice Martin-Lalande :

Supprimer le I de cet article.

ANNEXE 1

DIRECTIVE 2000/31/CE DU PARLEMENT EUROPEEN ET DU CONSEIL DU 8 JUIN 2000 RELATIVE A CERTAINS ASPECTS JURIDIQUES DES SERVICES DE LA SOCIETE DE L'INFORMATION, ET NOTAMMENT DU COMMERCE ELECTRONIQUE, DANS LE MARCHE INTERIEUR ("DIRECTIVE SUR LE COMMERCE ELECTRONIQUE")

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 47, paragraphe 2, son article 55 et son article 95,

vu la proposition de la Commission [(1)],

vu l'avis du Comité économique et social [(2)], statuant conformément à la procédure visée à l'article 251 du traité [(3)], considérant ce qui suit :

(1) L'Union européenne vise à établir des liens toujours plus étroits entre les États et les peuples européens et à assurer le progrès économique et social.

Conformément à l'article 14, paragraphe 2, du traité, le marché intérieur comporte un espace sans frontières intérieures dans lequel la libre circulation des marchandises et des services ainsi que la liberté d'établissement sont assurées. Le développement des services de la société de l'information dans l'espace sans frontières intérieures est un moyen essentiel pour éliminer les barrières qui divisent les peuples européens.

(2) Le développement du commerce électronique dans la société de l'information offre des opportunités importantes pour l'emploi dans la Communauté, en particulier dans les petites et moyennes entreprises. Il facilitera la croissance économique des entreprises européennes ainsi que leurs investissements dans l'innovation et il peut également renforcer la compétitivité des entreprises européennes, pour autant que tout le monde puisse accéder à l'Internet.

(3) Le droit communautaire et les caractéristiques de l'ordre juridique communautaire constituent un atout essentiel pour que les citoyens et les opérateurs européens puissent bénéficier pleinement, sans considération de frontières, des possibilités offertes par le commerce électronique. La présente directive a ainsi pour objet d'assurer un niveau élevé d'intégration juridique communautaire afin d'établir un réel espace sans frontières intérieures pour les services de la société de l'information.

---

(1) JO C 30 du 5.2.1999, p. 4.
(2) JO C 169 du 16.6.1999, p. 36.
(3) Avis du Parlement européen du 6 mai 1999 (JO C 279 du 1.10.1999, p. 389), position commune du Conseil du 28 février 2000 (JO C 128 du 8.5.2000, p. 32) et décision du Parlement européen du 4 mai 2000 (non encore parue au Journal officiel).

(4) Il est important de veiller à ce que le commerce électronique puisse bénéficier dans sa globalité du marché intérieur et donc que, au même titre que pour la directive 89/552/CEE du Conseil du 3 octobre 1989 visant à la coordination de certaines dispositions législatives, réglementaires et administratives des États membres relatives à l'exercice d'activités de radiodiffusion télévisuelle [(1)], un niveau élevé d'intégration communautaire soit obtenu.

(5) Le développement des services de la société de l'information dans la Communauté est limité par un certain nombre d'obstacles juridiques au bon fonctionnement du marché intérieur qui sont de nature à rendre moins attrayant l'exercice de la liberté d'établissement et de la libre prestation des services. Ces obstacles résident dans la divergence des législations ainsi que dans l'insécurité juridique des régimes nationaux applicables à ces services. En l'absence d'une coordination et d'un ajustement des législations dans les domaines concernés, des obstacles peuvent être justifiés au regard de la jurisprudence de la Cour de justice des Communautés européennes. Une insécurité juridique existe sur l'étendue du contrôle que les États membres peuvent opérer sur les services provenant d'un autre État membre.

(6) Il convient, au regard des objectifs communautaires, des articles 43 et 49 du traité et du droit communautaire dérivé, de supprimer ces obstacles par une coordination de certaines législations nationales et par une clarification au niveau communautaire de certains concepts juridiques, dans la mesure nécessaire au bon fonctionnement du marché intérieur. La présente directive, en ne traitant que certaines questions spécifiques qui soulèvent des problèmes pour le marché intérieur, est pleinement cohérente avec la nécessité de respecter le principe de subsidiarité tel qu'énoncé à l'article 5 du traité.

(7) Pour garantir la sécurité juridique et la confiance du consommateur, il y a lieu que la présente directive établisse un cadre général clair pour couvrir certains aspects juridiques du commerce électronique dans le marché intérieur.

(8) L'objectif de la présente directive est de créer un cadre juridique pour assurer la libre circulation des services de la société de l'information entre les États membres et non d'harmoniser le domaine du droit pénal en tant que tel.

(9) Dans bien des cas, la libre circulation des services de la société de l'information peut refléter spécifiquement, dans la législation communautaire, un principe plus général, à savoir la liberté d'expression, consacrée par l'article 10, paragraphe 1, de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui a été ratifiée par tous les États membres. Pour cette raison, les directives couvrant la fourniture de services de la société de l'information doivent assurer que cette activité peut être exercée librement en vertu de l'article précité, sous réserve uniquement des restrictions prévues au paragraphe 2 du même article et à l'article 46, paragraphe 1, du traité. La présente directive n'entend pas porter atteinte aux règles et principes fondamentaux nationaux en matière de liberté d'expression.

---

(1) JO L 298 du 17.10.1989, p. 23. Directive modifiée par la directive 97/36/CE du Parlement européen et du Conseil (JO L 202 du 30.7.1997, p. 60).

(10) Conformément au principe de proportionnalité, les mesures prévues par la présente directive se limitent strictement au minimum requis pour atteindre l'objectif du bon fonctionnement du marché intérieur. Là où il est nécessaire d'intervenir au niveau communautaire, et afin de garantir un espace qui soit réellement sans frontières intérieures pour le commerce électronique, la directive doit assurer un haut niveau de protection des objectifs d'intérêt général, en particulier la protection des mineurs, de la dignité humaine, du consommateur et de la santé publique. Conformément à l'article 152 du traité, la protection de la santé publique est une composante essentielle des autres politiques de la Communauté.

(11) La présente directive est sans préjudice du niveau de protection existant notamment en matière de protection de la santé publique et des intérêts des consommateurs, établi par les instruments communautaires. Entre autres, la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs [(1)] et la directive 97/7/CE du Parlement européen et du Conseil du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance [(2)] constituent un élément fondamental pour la protection des consommateurs en matière contractuelle. Ces directives sont également applicables, dans leur intégralité, aux services de la société de l'information. Ce même acquis communautaire, qui est pleinement applicable aux services de la société de l'information, englobe aussi notamment la directive 84/450/CEE du Conseil du 10 septembre 1984 relative à la publicité trompeuse et comparative [(3)], la directive 87/102/CEE du Conseil du 22 décembre 1986 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de crédit à la consommation [(4)], la directive 93/22/CEE du Conseil du 10 mai 1993 concernant les services d'investissement dans le domaine des valeurs mobilières [(5)], la directive 90/314/CEE du Conseil du 13 juin 1990 concernant les voyages, vacances et circuits à forfait [(6)], la directive 98/6/CE du Parlement européen et du Conseil du 16 février 1998 relative à la protection des consommateurs en matière d'indication des prix des produits offerts aux consommateurs [(7)], la directive 92/59/CEE du Conseil du 29 juin 1992 relative à la sécurité générale des produits [(8)], la directive 94/47/CE du Parlement européen et du Conseil du 26 octobre 1994 concernant la protection des acquéreurs pour certains aspects des contrats portant sur l'acquisition d'un droit d'utilisation à temps partiel de biens immobiliers [(9)], la directive 98/27/CE du Parlement européen et du Conseil du 19 mai 1998 relative aux actions en cessation en matière de protection des intérêts des consommateurs [(10)], la directive 85/374/CEE du Conseil du 25 juillet 1985 relative à la responsabilité du fait des produits défectueux [(11)], la directive 1999/44/CE du Parlement européen et du Conseil du 25 mai 1999 relative à certains

---

(1) JO L 95 du 21.4.1993, p. 29.
(2) JO L 144 du 4.6.1997, p. 19.
(3) JO L 250 du 19.9.1984, p. 17. Directive modifiée par la directive 97/55/CE du Parlement européen et du Conseil (JO L 290 du 23.10.1997, p. 18).
(4) JO L 42 du 12.2.1987, p. 48. Directive modifiée en dernier lieu par la directive 98/7/CE du Parlement européen et du Conseil (JO L 101 du 1.4.1998, p. 17).
(5) JO L 141 du 11.6.1993, p. 27. Directive modifiée en dernier lieu par la directive 97/9/CE du Parlement européen et du Conseil (JO L 84 du 26.3.1997, p. 22).
(6) JO L 158 du 23.6.1990, p. 59.
(7) JO L 80 du 18.3.1998, p. 27.
(8) JO L 228 du 11.8.1992, p. 24.
(9) JO L 280 du 29.10.1994, p. 83.
(10) JO L 166 du 11.6.1998, p. 51. Directive modifiée par la directive 1999/44/CE (JO L 171 du 7.7.1999, p. 12).
(11) JO L 210 du 7.8.1985, p. 29. Directive modifiée par la directive 1999/34/CE (JO L 141 du 4.6.1999, p. 20).

aspects de la vente et aux garanties des biens de consommation [1], la future directive du Parlement européen et du Conseil concernant la vente à distance de services financiers aux consommateurs et la directive 92/28/CEE du Conseil du 31 mars 1992 concernant la publicité faite à l'égard des médicaments [2]. La présente directive doit être sans préjudice de la directive 98/43/CE du Parlement européen et du Conseil du 6 juillet 1998 concernant le rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de publicité et de parrainage en faveur des produits du tabac [3] adoptée dans le cadre du marché intérieur ou des directives relatives à la protection de la santé publique. La présente directive complète les exigences d'information établies par les directives précitées et en particulier la directive 97/7/CE.

(12) Il est nécessaire d'exclure du champ d'application de la présente directive certaines activités compte tenu du fait que la libre prestation des services dans ces domaines ne peut être, à ce stade, garantie au regard du traité ou du droit communautaire dérivé existant. Cette exclusion doit être sans préjudice des éventuels instruments qui pourraient s'avérer nécessaires pour le bon fonctionnement du marché intérieur. La fiscalité, notamment la taxe sur la valeur ajoutée frappant un grand nombre des services visés par la présente directive, doit être exclue du champ d'application de la présente directive.

(13) La présente directive n'a pas pour but d'établir des règles en matière d'obligations fiscales ni ne préjuge de l'élaboration d'instruments communautaires relatifs aux aspects fiscaux du commerce électronique.

(14) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est uniquement régie par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [4] et par la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications [5], qui sont pleinement applicables aux services de la société de l'information. Ces directives établissent d'ores et déjà un cadre juridique communautaire dans le domaine des données à caractère personnel et, par conséquent, il n'est pas nécessaire de traiter cette question dans la présente directive afin d'assurer le bon fonctionnement du marché intérieur, et notamment la libre circulation des données à caractère personnel entre les États membres. La mise en oeuvre et l'application de la présente directive devraient être conformes aux principes relatifs à la protection des données à caractère personnel, notamment pour ce qui est des communications commerciales non sollicitées et de la responsabilité des intermédiaires. La présente directive ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet.

---

(1) JO L 171 du 7.7.1999, p. 12.
(2) JO L 113 du 30.4.1992, p. 13.
(3) JO L 213 du 30.7.1998, p. 9.
(4) JO L 281 du 28.11.1995, p. 31.
(5) JO L 24 du 30.1.1998, p. 1.

(15) Le secret des communications est garanti par l'article 5 de la directive 97/66/CE. Conformément à cette directive, les États membres doivent interdire tout type d'interception illicite ou la surveillance de telles communications par d'autres que les expéditeurs et les récepteurs, sauf lorsque ces activités sont légalement autorisées.

(16) L'exclusion des activités de jeux d'argent du champ d'application de la présente directive couvre uniquement les jeux de hasard, les loteries et les transactions portant sur des paris, qui supposent des enjeux en valeur monétaire. Elle ne couvre pas les concours ou jeux promotionnels qui ont pour but d'encourager la vente de biens ou de services et pour lesquels les paiements, s'ils ont lieu, ne servent qu'à acquérir les biens ou les services en promotion.

(17) La définition des services de la société de l'information existe déjà en droit communautaire. Elle figure dans la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information [(1)] et dans la directive 98/84/CE du Parlement européen et du Conseil du 20 novembre 1998 concernant la protection juridique des services à accès conditionnel et des services d'accès conditionnel [(2)]. Cette définition couvre tout service fourni, normalement contre rémunération, à distance au moyen d'équipement électronique de traitement (y compris la compression numérique) et de stockage des données, à la demande individuelle d'un destinataire de services. Les services visés dans la liste indicative figurant à l'annexe V de la directive 98/34/CE qui ne comportent pas de traitement et de stockage des données ne sont pas couverts par la présente définition.

(18) Les services de la société de l'information englobent un large éventail d'activités économiques qui ont lieu en ligne. Ces activités peuvent consister, en particulier, à vendre des biens en ligne. Les activités telles que la livraison de biens en tant que telle ou la fourniture de services hors ligne ne sont pas couvertes. Les services de la société de l'information ne se limitent pas exclusivement aux services donnant lieu à la conclusion de contrats en ligne, mais, dans la mesure où ils représentent une activité économique, ils s'étendent à des services qui ne sont pas rémunérés par ceux qui les reçoivent, tels que les services qui fournissent des informations en ligne ou des communications commerciales, ou ceux qui fournissent des outils permettant la recherche, l'accès et la récupération des données. Les services de la société de l'information comportent également des services qui consistent à transmettre des informations par le biais d'un réseau de communication, à fournir un accès à un réseau de communication ou à héberger des informations fournies par un destinataire de services. Les services de télévision au sens de la directive 89/552/CEE et de radiodiffusion ne sont pas des services de la société de l'information car ils ne sont pas fournis sur demande individuelle. En revanche, les services transmis de point à point, tels que les services de vidéo à la demande ou la fourniture de communications commerciales par courrier électronique constituent des services de la société de l'information. L'utilisation du courrier électronique ou d'autres moyens de communication individuels équivalents par des personnes

(1) JO L 204 du 21.7.1998, p. 37. Directive modifiée par la directive 98/48/CE (JO L 217 du 5.8.1998, p. 18).
(2) JO L 320 du 28.11.1998, p. 54.

physiques agissant à des fins qui n'entrent pas dans le cadre de leurs activités commerciales ou professionnelles, y compris leur utilisation pour la conclusion de contrats entre ces personnes, n'est pas un service de la société de l'information. La relation contractuelle entre un employé et son employeur n'est pas un service de la société de l'information. Les activités qui, par leur nature, ne peuvent pas être réalisées à distance ou par voie électronique, telles que le contrôle légal des comptes d'une société ou la consultation médicale requérant un examen physique du patient, ne sont pas des services de la société de l'information.

(19) Le lieu d'établissement d'un prestataire devrait être déterminé conformément à la jurisprudence de la Cour de justice, selon laquelle le concept d'établissement implique l'exercice effectif d'une activité économique au moyen d'une installation stable et pour une durée indéterminée. Cette exigence est également remplie lorsqu'une société est constituée pour une période donnée. Le lieu d'établissement d'une société fournissant des services par le biais d'un site Internet n'est pas le lieu où se situe l'installation technologique servant de support au site ni le lieu où son site est accessible, mais le lieu où elle exerce son activité économique. Dans le cas où un prestataire a plusieurs lieux d'établissement, il est important de déterminer de quel lieu d'établissement le service concerné est presté. Dans les cas où il est difficile de déterminer, entre plusieurs lieux d'établissement, celui à partir duquel un service donné est fourni, le lieu d'établissement est celui dans lequel le prestataire a le centre de ses activités pour ce service spécifique.

(20) La définition du "destinataire d'un service" couvre tous les types d'utilisation des services de la société de l'information, tant par les personnes qui fournissent l'information sur les réseaux ouverts tels que l'Internet que par celles qui recherchent des informations sur l'Internet pour des raisons privées ou professionnelles.

(21) La portée du domaine coordonné est sans préjudice d'une future harmonisation communautaire concernant les services de la société de l'information et de futures législations adoptées au niveau national conformément au droit communautaire. Le domaine coordonné ne couvre que les exigences relatives aux activités en ligne, telles que l'information en ligne, la publicité en ligne, les achats en ligne, la conclusion de contrats en ligne et ne concerne pas les exigences juridiques des États membres relatives aux biens telles que les normes en matière de sécurité, les obligations en matière d'étiquetage ou la responsabilité du fait des produits, ni les exigences des États membres relatives à la livraison ou au transport de biens, y compris la distribution de médicaments. Le domaine coordonné ne couvre pas l'exercice du droit de préemption par les pouvoirs publics concernant certains biens tels que les oeuvres d'art.

(22) Le contrôle des services de la société de l'information doit se faire à la source de l'activité pour assurer une protection efficace des objectifs d'intérêt général. Pour cela, il est nécessaire de garantir que l'autorité compétente assure cette protection non seulement pour les citoyens de son propre pays, mais aussi pour l'ensemble des citoyens de la Communauté. Pour améliorer la confiance mutuelle entre les États membres, il est indispensable de préciser clairement cette responsabilité de l'État membre d'origine des services. En outre, afin d'assurer efficacement la libre prestation des services et une sécurité juridique pour les

prestataires et leurs destinataires, ces services de la société de l'information doivent être soumis en principe au régime juridique de l'État membre dans lequel le prestataire est établi.

(23) La présente directive n'a pas pour objet d'établir des règles supplémentaires de droit international privé relatives aux conflits de loi ni de traiter de la compétence des tribunaux. Les dispositions du droit applicable désigné par les règles du droit international privé ne doivent pas restreindre la libre prestation des services de la société de l'information telle que prévue par la présente directive.

(24) Dans le cadre de la présente directive et nonobstant le principe du contrôle à la source de services de la société de l'information, il apparaît légitime, dans les conditions prévues par la présente directive, que les États membres prennent des mesures tendant à limiter la libre circulation des services de la société de l'information.

(25) Les juridictions nationales, y compris les juridictions civiles, statuant sur les différends de droit privé peuvent déroger à la libre prestation des services de la société de l'information, conformément aux conditions définies dans la présente directive.

(26) Les États membres peuvent, conformément aux conditions définies dans la présente directive, appliquer leurs règles nationales de droit pénal et de procédure pénale pour engager toutes les mesures d'enquêtes et autres nécessaires pour détecter et poursuivre les infractions en matière pénale, sans qu'il soit besoin de notifier ces mesures à la Commission.

(27) La présente directive, en liaison avec la future directive du Parlement européen et du Conseil concernant la vente à distance de services financiers aux consommateurs, contribue à la création d'un cadre juridique pour la prestation en ligne de services financiers. La présente directive ne préjuge pas de futures initiatives dans le domaine des services financiers, notamment en ce qui concerne l'harmonisation des règles de conduite dans ce domaine. La possibilité pour les États membres, établie par la présente directive, de restreindre, dans certaines circonstances, la libre prestation des services de la société de l'information aux fins de protection des consommateurs couvre également les mesures dans le domaine des services financiers, notamment des mesures visant à protéger les investisseurs.

(28) L'obligation faite aux États membres de ne pas soumettre l'accès à l'activité d'un prestataire de services de la société de l'information à une autorisation préalable ne concerne pas les services postaux couverts par la directive 97/67/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant des règles communes pour le développement du marché intérieur des services postaux de la Communauté et l'amélioration de la qualité du service [(1)], consistant dans la remise physique d'un message imprimé par courrier électronique et n'affecte pas les régimes d'accréditation volontaire, notamment pour les prestataires de services de signature électronique et de certification.

---

(1) JO L 15 du 21.1.1998, p. 14.

(29) Les communications commerciales sont essentielles pour le financement des services de la société de l'information et le développement d'une large variété de nouveaux services gratuits. Dans l'intérêt de la protection des consommateurs et de la loyauté des transactions, les communications commerciales, y compris les rabais, les offres, concours et jeux promotionnels, doivent respecter un certain nombre d'obligations relatives à la transparence. Ces obligations sont sans préjudice de la directive 97/7/CE. La présente directive ne doit pas affecter les directives existantes concernant les communications commerciales, en particulier la directive 98/43/CE.

(30) L'envoi par courrier électronique de communications commerciales non sollicitées peut être inopportun pour les consommateurs et pour les fournisseurs de services de la société de l'information et susceptible de perturber le bon fonctionnement des réseaux interactifs. La question du consentement du destinataire pour certaines formes de communication commerciale non sollicitée n'est pas traitée dans la présente directive, mais a déjà été traitée, en particulier, dans la directive 97/7/CE et dans la directive 97/66/CE. Dans les États membres qui autorisent l'envoi par courrier électronique de communications commerciales non sollicitées, la mise en place de dispositifs de filtrage approprié par les entreprises doit être encouragée et facilitée. Il faut en outre, en toute hypothèse, que les communications commerciales non sollicitées soient clairement identifiables en tant que telles afin d'améliorer la transparence et de faciliter le fonctionnement de tels dispositifs mis en place par les entreprises. L'envoi par courrier électronique de communications commerciales non sollicitées ne saurait entraîner de frais supplémentaires pour le destinataire.

(31) Les États membres qui autorisent l'envoi par courrier électronique, par des prestataires établis sur leur territoire, de communications commerciales non sollicitées sans le consentement préalable du destinataire, doivent veiller à ce que les prestataires consultent régulièrement les registres "opt-out" où les personnes physiques qui ne souhaitent pas recevoir ce type de communications commerciales peuvent s'inscrire, et respectent le souhait de ces personnes.

(32) Pour supprimer les entraves au développement des services transfrontaliers dans la Communauté que les membres des professions réglementées pourraient proposer sur l'Internet, il est nécessaire que le respect des règles professionnelles prévues pour protéger notamment le consommateur ou la santé publique soit garanti au niveau communautaire. Les codes de conduite au niveau communautaire constituent le meilleur instrument pour déterminer les règles déontologiques applicables à la communication commerciale. Il convient d'encourager leur élaboration ou, le cas échéant, leur adaptation, sans préjudice de l'autonomie des organismes et des associations professionnels.

(33) La présente directive complète le droit communautaire et le droit national relatif aux professions réglementées en maintenant un ensemble cohérent de règles applicables dans ce domaine.

(34) Chaque État membre doit ajuster sa législation qui contient des exigences, notamment de forme, susceptibles de gêner le recours à des contrats par voie électronique. Il convient que l'examen des législations nécessitant cet ajustement se fasse systématiquement et porte sur l'ensemble des étapes et des actes nécessaires au

processus contractuel, y compris l'archivage du contrat. Il convient que le résultat de cet ajustement soit de rendre réalisables les contrats conclus par voie électronique. L'effet juridique des signatures électroniques fait l'objet de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques [1], l'accusé de réception par un prestataire peut être constitué par la fourniture en ligne d'un service payé.

(35) La présente directive n'affecte pas la possibilité pour les États membres de maintenir ou d'établir pour les contrats des exigences juridiques générales ou spécifiques qui peuvent être satisfaites par des moyens électroniques, notamment des exigences en matière de sécurité des signatures électroniques.

(36) Les États membres peuvent maintenir des restrictions à l'utilisation de contrats électroniques en ce qui concerne les contrats pour lesquels la loi requiert l'intervention de tribunaux, d'autorités publiques ou de professions exerçant une autorité publique. Cette possibilité couvre également les contrats requérant l'intervention de tribunaux, d'autorités publiques ou de professions exerçant une autorité publique afin de produire des effets à l'égard des tiers, aussi bien que les contrats requérant une certification juridique ou une attestation par un notaire.

(37) L'obligation faite aux États membres d'éliminer les obstacles à l'utilisation des contrats électroniques ne concerne que les obstacles résultant d'exigences juridiques et non pas les obstacles d'ordre pratique résultant d'une impossibilité d'utiliser les moyens électroniques dans certains cas.

(38) L'obligation faite aux États membres d'éliminer les obstacles à l'utilisation des contrats électroniques est mise en oeuvre dans le respect des exigences juridiques pour les contrats, consacrées par le droit communautaire.

(39) Les exceptions aux dispositions relatives aux contrats passés exclusivement au moyen du courrier électronique ou au moyen de communications individuelles équivalentes prévues dans la présente directive, en ce qui concerne les informations à fournir et la passation d'une commande, ne sauraient avoir comme conséquence de permettre le contournement de ces dispositions par les prestataires de services de la société de l'information.

(40) Les divergences existantes et émergentes entre les législations et les jurisprudences des États membres dans le domaine de la responsabilité des prestataires de services agissant en qualité d'intermédiaires empêchent le bon fonctionnement du marché intérieur, en particulier en gênant le développement des services transfrontaliers et en produisant des distorsions de concurrence. Les prestataires des services ont, dans certains cas, le devoir d'agir pour éviter les activités illégales ou pour y mettre fin. La présente directive doit constituer la base adéquate pour l'élaboration de mécanismes rapides et fiables permettant de retirer les informations illicites et de rendre l'accès à celles-ci impossible. Il conviendrait que de tels mécanismes soient élaborés sur la base d'accords volontaires négociés entre toutes les parties concernées et qu'ils soient encouragés par les États membres. Il est dans l'intérêt de toutes les parties qui participent à la fourniture de services de

(1) JO L 13 du 19.1.2000, p. 12.

la société de l'information d'adopter et d'appliquer de tels mécanismes. Les dispositions de la présente directive sur la responsabilité ne doivent pas faire obstacle au développement et à la mise en oeuvre effective, par les différentes parties concernées, de systèmes techniques de protection et d'identification ainsi que d'instruments techniques de surveillance rendus possibles par les techniques numériques, dans le respect des limites établies par les directives 95/46/CE et 97/66/CE.

(41) La présente directive instaure un équilibre entre les différents intérêts en jeu et établit des principes qui peuvent servir de base aux normes et aux accords adoptés par les entreprises.

(42) Les dérogations en matière de responsabilité prévues par la présente directive ne couvrent que les cas où l'activité du prestataire de services dans le cadre de la société de l'information est limitée au processus technique d'exploitation et de fourniture d'un accès à un réseau de communication sur lequel les informations fournies par des tiers sont transmises ou stockées temporairement, dans le seul but d'améliorer l'efficacité de la transmission. Cette activité revêt un caractère purement technique, automatique et passif, qui implique que le prestataire de services de la société de l'information n'a pas la connaissance ni le contrôle des informations transmises ou stockées.

(43) Un prestataire de services peut bénéficier de dérogations pour le "simple transport" et pour la forme de stockage dite "caching" lorsqu'il n'est impliqué en aucune manière dans l'information transmise. Cela suppose, entre autres, qu'il ne modifie pas l'information qu'il transmet. Cette exigence ne couvre pas les manipulations à caractère technique qui ont lieu au cours de la transmission, car ces dernières n'altèrent pas l'intégrité de l'information contenue dans la transmission.

(44) Un prestataire de services qui collabore délibérément avec l'un des destinataires de son service afin de se livrer à des activités illégales va au-delà des activités de "simple transport" ou de "caching" et, dès lors, il ne peut pas bénéficier des dérogations en matière de responsabilité prévues pour ce type d'activité.

(45) Les limitations de responsabilité des prestataires de services intermédiaires prévues dans la présente directive sont sans préjudice de la possibilité d'actions en cessation de différents types. Ces actions en cessation peuvent notamment revêtir la forme de décisions de tribunaux ou d'autorités administratives exigeant qu'il soit mis un terme à toute violation ou que l'on prévienne toute violation, y compris en retirant les informations illicites ou en rendant l'accès à ces dernières impossible.

(46) Afin de bénéficier d'une limitation de responsabilité, le prestataire d'un service de la société de l'information consistant dans le stockage d'informations doit, dès qu'il prend effectivement connaissance ou conscience du caractère illicite des activités, agir promptement pour retirer les informations concernées ou rendre l'accès à celles-ci impossible. Il y a lieu de procéder à leur retrait ou de rendre leur accès impossible dans le respect du principe de la liberté d'expression et des procédures établies à cet effet au niveau national. La présente directive n'affecte pas la possibilité qu'ont les États membres de définir des exigences spécifiques

auxquelles il doit être satisfait promptement avant de retirer des informations ou d'en rendre l'accès impossible.

(47) L'interdiction pour les États membres d'imposer aux prestataires de services une obligation de surveillance ne vaut que pour les obligations à caractère général. Elle ne concerne pas les obligations de surveillance applicables à un cas spécifique et, notamment, elle ne fait pas obstacle aux décisions des autorités nationales prises conformément à la législation nationale.

(48) La présente directive n'affecte en rien la possibilité qu'ont les États membres d'exiger des prestataires de services qui stockent des informations fournies par des destinataires de leurs services qu'ils agissent avec les précautions que l'on peut raisonnablement attendre d'eux et qui sont définies dans la législation nationale, et ce afin de détecter et d'empêcher certains types d'activités illicites.

(49) Les États membres et la Commission doivent encourager l'élaboration de codes de conduite. Cela ne porte pas atteinte au caractère volontaire de ces codes et à la possibilité, pour les parties intéressées, de décider librement si elles adhèrent ou non à ces codes.

(50) Il est important que la proposition de directive sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information et la présente directive entrent en vigueur au même moment afin d'établir un cadre réglementaire clair en ce qui concerne la responsabilité des intermédiaires en cas de violation du droit d'auteur et des droits voisins au niveau communautaire.

(51) Il doit incomber à chaque État membre, le cas échéant, de modifier toute législation susceptible de gêner l'utilisation des mécanismes de règlement extrajudiciaire des litiges par les voies électroniques. Le résultat de cette modification doit être de rendre réellement et effectivement possible, en droit et dans la pratique, le fonctionnement de tels mécanismes, y compris dans des situations transfrontalières.

(52) L'exercice effectif des libertés du marché intérieur nécessite de garantir aux victimes un accès efficace aux règlements des litiges. Les dommages qui peuvent se produire dans le cadre des services de la société de l'information se caractérisent à la fois par leur rapidité et leur étendue géographique. En raison de cette spécificité et de la nécessité de veiller à ce que les autorités nationales ne mettent pas en cause la confiance qu'elles doivent s'accorder mutuellement, la présente directive invite les États membres à faire en sorte que les recours juridictionnels appropriés soient disponibles. Les États membres doivent évaluer la nécessité de fournir un accès aux procédures juridictionnelles par les moyens électroniques appropriés.

(53) La directive 98/27/CE, applicable aux services de la société de l'information, prévoit un mécanisme relatif aux actions en cessation visant à protéger les intérêts collectifs des consommateurs. Ce mécanisme contribuera à la libre circulation des services de la société de l'information en assurant un niveau élevé de protection des consommateurs.

(54) Les sanctions prévues dans le cadre de la présente directive sont sans préjudice de toute autre sanction ou voie de droit prévue par le droit national. Les États membres ne sont pas tenus de prévoir des sanctions pénales pour la violation des dispositions nationales adoptées en application de la présente directive.

(55) La présente directive ne porte pas atteinte au droit applicable aux obligations contractuelles relatives aux contrats conclus par les consommateurs. En conséquence, la présente directive ne saurait avoir pour effet de priver le consommateur de la protection que lui procurent les règles impératives relatives aux obligations contractuelles prévues par le droit de l'État membre dans lequel il a sa résidence habituelle.

(56) En ce qui concerne la dérogation prévue par la présente directive pour les obligations contractuelles dans les contrats conclus par les consommateurs, celles-ci doivent être interprétées comme comprenant les informations sur les éléments essentiels du contenu du contrat, y compris les droits du consommateur, ayant une influence déterminante sur la décision de contracter.

(57) Conformément à une jurisprudence constante de la Cour de justice, un État membre conserve le droit de prendre des mesures à l'encontre d'un prestataire établi dans un autre État membre, mais dont l'activité est entièrement ou principalement tournée vers le territoire du premier État membre, lorsque le choix de cet établissement a été fait en vue de se soustraire aux règles qui seraient applicables à ce prestataire s'il s'était établi sur le territoire du premier État membre.

(58) La présente directive ne doit pas s'appliquer aux services fournis par des prestataires établis dans un pays tiers. Compte tenu de la dimension mondiale du service électronique, il convient toutefois d'assurer la cohérence des règles communautaires avec les règles internationales. La présente directive est sans préjudice des résultats des discussions en cours sur les aspects juridiques dans les organisations internationales (entre autres, OMC, OCDE, Cnudci).

(59) En dépit de la nature planétaire des communications électroniques, la coordination au niveau de l'Union européenne des mesures réglementaires nationales est nécessaire afin d'éviter la fragmentation du marché intérieur et d'établir un cadre réglementaire européen approprié. Cette coordination doit également contribuer à l'établissement d'une position de négociation commune et forte dans les enceintes internationales.

(60) Pour permettre un développement sans entrave du commerce électronique, le cadre juridique doit être clair et simple, prévisible et cohérent avec les règles applicables au niveau international, de sorte qu'il ne porte pas atteinte à la compétitivité de l'industrie européenne et qu'il ne fasse pas obstacle à l'innovation dans ce secteur.

(61) Si le marché doit réellement fonctionner par des moyens électroniques dans un contexte mondialisé, l'Union européenne et les grands ensembles non européens ont besoin de se concerter pour rendre leurs législations et leurs procédures compatibles.

(62) La coopération avec les pays tiers doit être renforcée dans le domaine du commerce électronique, notamment avec les pays candidats, les pays en développement et les autres partenaires commerciaux de l'Union européenne.

(63) L'adoption de la présente directive ne saurait empêcher les États membres de prendre en compte les différentes implications sociales, sociétales et culturelles inhérentes à l'avènement de la société de l'information. En particulier, elle ne devrait pas porter atteinte aux mesures destinées à atteindre des objectifs sociaux, culturels et démocratiques que les États membres pourraient adopter, conformément au droit communautaire, en tenant compte de leur diversité linguistique, des spécificités nationales et régionales ainsi que de leurs patrimoines culturels, et à assurer et à maintenir l'accès du public à un éventail le plus large possible de services de la société de l'information. Le développement de la société de l'information doit assurer, en tout état de cause, l'accès des citoyens de la Communauté au patrimoine culturel européen fourni dans un environnement numérique.

(64) La communication électronique constitue pour les États membres un excellent moyen de fournir un service public dans les domaines culturel, éducatif et linguistique.

(65) Le Conseil, dans sa résolution du 19 janvier 1999 sur la dimension consumériste de la société de l'information [(1)], a souligné que la protection des consommateurs méritait une attention particulière dans le cadre de celle-ci. La Commission étudiera la mesure dans laquelle les règles de protection des consommateurs existantes fournissent une protection insuffisante au regard de la société de l'information et identifiera, le cas échéant, les lacunes de cette législation et les aspects pour lesquels des mesures additionnelles pourraient s'avérer nécessaires. En cas de besoin, la Commission devrait faire des propositions spécifiques additionnelles visant à combler les lacunes qu'elle aurait ainsi identifiées,

A ARRÊTÉ LA PRÉSENTE DIRECTIVE :

CHAPITRE I^er^
DISPOSITIONS GÉNÉRALES

Article premier
Objectif et champ d'application

1. La présente directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres.

2. La présente directive rapproche, dans la mesure nécessaire à la réalisation de l'objectif visé au paragraphe 1, certaines dispositions nationales applicables aux services de la société de l'information et qui concernent le marché intérieur, l'établissement des prestataires, les communications commerciales, les contrats par voie électronique, la responsabilité des intermédiaires, les codes de conduite, le

(1) JO C 23 du 28.1.1999, p. 1.

règlement extrajudiciaire des litiges, les recours juridictionnels et la coopération entre États membres.

3. La présente directive complète le droit communautaire applicable aux services de la société de l'information sans préjudice du niveau de protection, notamment en matière de santé publique et des intérêts des consommateurs, établi par les instruments communautaires et la législation nationale les mettant en oeuvre dans la mesure où cela ne restreint pas la libre prestation de services de la société de l'information.

4. La présente directive n'établit pas de règles additionnelles de droit international privé et ne traite pas de la compétence des juridictions.

5. La présente directive n'est pas applicable:

a) au domaine de la fiscalité;

b) aux questions relatives aux services de la société de l'information couvertes par les directives 95/46/CE et 97/66/CE;

c) aux questions relatives aux accords ou pratiques régis par le droit sur les ententes;

d) aux activités suivantes des services de la société de l'information:

— les activités de notaire ou les professions équivalentes, dans la mesure où elles comportent une participation directe et spécifique à l'exercice de l'autorité publique,

— la représentation d'un client et la défense de ses intérêts devant les tribunaux,

— les activités de jeux d'argent impliquant des mises ayant une valeur monétaire dans des jeux de hasard, y compris les loteries et les transactions portant sur des paris.

6. La présente directive ne porte pas atteinte aux mesures prises au niveau communautaire ou au niveau national, dans le respect du droit communautaire, pour promouvoir la diversité culturelle et linguistique et assurer la défense du pluralisme.

Article 2
Définitions

Aux fins de la présente directive, on entend par:

a) "services de la société de l'information": les services au sens de l'article 1er, paragraphe 2, de la directive 98/34/CE, telle que modifiée par la directive 98/48/CE;

b) "prestataire": toute personne physique ou morale qui fournit un service de la société de l'information;

c) "prestataire établi": prestataire qui exerce d'une manière effective une activité économique au moyen d'une installation stable pour une durée indéterminée. La présence et l'utilisation des moyens techniques et des technologies requis pour fournir le service ne constituent pas en tant que telles un établissement du prestataire;

d) "destinataire du service": toute personne physique ou morale qui, à des fins professionnelles ou non, utilise un service de la société de l'information, notamment pour rechercher une information ou la rendre accessible;

e) "consommateur": toute personne physique agissant à des fins qui n'entrent pas dans le cadre de son activité professionnelle ou commerciale;

f) "communication commerciale": toute forme de communication destinée à promouvoir, directement ou indirectement, des biens, des services, ou l'image d'une entreprise, d'une organisation ou d'une personne ayant une activité commerciale, industrielle, artisanale ou exerçant une profession réglementée. Ne constituent pas en tant que telles des communications commerciales:

— les informations permettant l'accès direct à l'activité de l'entreprise, de l'organisation ou de la personne, notamment un nom de domaine ou une adresse de courrier électronique,

— les communications relatives aux biens, aux services ou à l'image de l'entreprise, de l'organisation ou de la personne élaborées d'une manière indépendante, en particulier lorsqu'elles sont fournies sans contrepartie financière;

g) "profession réglementée": toute profession au sens, soit de l'article 1er, point d), de la directive 89/49/CEE du Conseil du 21 décembre 1988 relative à un système général de reconnaissance des diplômes d'enseignement supérieur qui sanctionne des formations professionnelles d'une durée minimale de trois ans [(1)], soit au sens de l'article 1er, point f), de la directive 92/51/CEE du Conseil du 18 juin 1992 relative à un deuxième système général de reconnaissance des formations professionnelles, qui complète la directive 89/48/CEE [(2)] ;

h) "domaine coordonné": les exigences prévues par les systèmes juridiques des États membres et applicables aux prestataires des services de la société de l'information ou aux services de la société de l'information, qu'elles revêtent un caractère général ou qu'elles aient été spécifiquement conçues pour eux.

i) Le domaine coordonné a trait à des exigences que le prestataire doit satisfaire et qui concernent:

— l'accès à l'activité d'un service de la société de l'information, telles que les exigences en matière de qualification, d'autorisation ou de notification,

— l'exercice de l'activité d'un service de la société de l'information, telles que les exigences portant sur le comportement du prestataire, la qualité ou le contenu du

(1) JO L 19 du 24.1.1989, p. 16.
(2) JO L 209 du 24.7.1992, p. 25. Directive modifiée en dernier lieu par la directive 97/38/CE (JO L 184 du 12.7.1997, p. 31).

service, y compris en matière de publicité et de contrat, ou sur la responsabilité du prestataire.

ii) Le domaine coordonnée ne couvre pas les exigences telles que:

— les exigences applicables aux biens en tant que tels,

— les exigences applicables à la livraison de biens,

— les exigences applicables aux services qui ne sont pas fournis par voie électronique.

Article 3
Marché intérieur

1. Chaque État membre veille à ce que les services de la société de l'information fournis par un prestataire établi sur son territoire respectent les dispositions nationales applicables dans cet État membre relevant du domaine coordonné.

2. Les État membres ne peuvent, pour des raisons relevant du domaine coordonné, restreindre la libre circulation des services de la société de l'information en provenance d'un autre État membre.

3. Les paragraphes 1 et 2 ne sont pas applicables aux domaines visés à l'annexe.

4. Les États membres peuvent prendre, à l'égard d'un service donné de la société de l'information, des mesures qui dérogent au paragraphe 2 si les conditions suivantes sont remplies:

a) les mesures doivent être:

i) nécessaires pour une des raisons suivantes:

— l'ordre public, en particulier la prévention, les investigations, la détection et les poursuites en matière pénale, notamment la protection des mineurs et la lutte contre l'incitation à la haine pour des raisons de race, de sexe, de religion ou de nationalité et contre les atteintes à la dignité de la personne humaine,

— la protection de la santé publique,

— la sécurité publique, y compris la protection de la sécurité et de la défense nationales,

— la protection des consommateurs, y compris des investisseurs;

ii) prises à l'encontre d'un service de la société de l'information qui porte atteinte aux objectifs visés au point i) ou qui constitue un risque sérieux et grave d'atteinte à ces objectifs;

iii) proportionnelles à ces objectifs;

b) l'État membre a préalablement et sans préjudice de la procédure judiciaire, y compris la procédure préliminaire et les actes accomplis dans le cadre d'une enquête pénale:

— demandé à l'État membre visé au paragraphe 1 de prendre des mesures et ce dernier n'en a pas pris ou elles n'ont pas été suffisantes,

— notifié à la Commission et à l'État membre visé au paragraphe 1 son intention de prendre de telles mesures.

5. Les États membres peuvent, en cas d'urgence, déroger aux conditions prévues au paragraphe 4, point b). Dans ce cas, les mesures sont notifiées dans les plus brefs délais à la Commission et à l'État membre visé au paragraphe 1, en indiquant les raisons pour lesquelles l'État membre estime qu'il y a urgence.

6. Sans préjudice de la faculté pour l'État membre de prendre et d'appliquer les mesures en question, la Commission doit examiner dans les plus brefs délais la compatibilité des mesures notifiées avec le droit communautaire; lorsqu'elle parvient à la conclusion que la mesure est incompatible avec le droit communautaire, la Commission demande à l'État membre concerné de s'abstenir de prendre les mesures envisagées ou de mettre fin d'urgence aux mesures en question.

CHAPITRE II
PRINCIPES

Section 1: Exigences en matière d'établissement et d'information

Article 4
Principe de non-autorisation préalable

1. Les États membres veillent à ce que l'accès à l'activité d'un prestataire de services de la société de l'information et l'exercice de celle-ci ne puissent pas être soumis à un régime d'autorisation préalable ou à toute autre exigence ayant un effet équivalent.

2. Le paragraphe 1 est sans préjudice des régimes d'autorisation qui ne visent pas spécifiquement et exclusivement les services de la société de l'information ou qui sont couverts par la directive 97/13/CE du Parlement européen et du Conseil du 10 avril 1997 relative à un cadre commun pour les autorisations générales et les licences individuelles dans le secteur des services des télécommunications [(1)].

Article 5
Informations générales à fournir

1. Outre les autres exigences en matière d'information prévues par le droit communautaire, les États membres veillent à ce que le prestataire rende possible un accès facile, direct et permanent, pour les destinataires du service et pour les autorités compétentes, au moins aux informations suivantes:

---

(1) JO L 117 du 7.5.1997, p. 15.

a) le nom du prestataire de services;

b) l'adresse géographique à laquelle le prestataire de services est établi;

c) les coordonnées du prestataire, y compris son adresse de courrier électronique, permettant d'entrer en contact rapidement et de communiquer directement et efficacement avec lui;

d) dans le cas où le prestataire est inscrit dans un registre de commerce ou dans un autre registre public similaire, le registre de commerce dans lequel il est inscrit et son numéro d'immatriculation, ou des moyens équivalents d'identification figurant dans ce registre;

e) dans le cas où l'activité est soumise à un régime d'autorisation, les coordonnées de l'autorité de surveillance compétente;

f) en ce qui concerne les professions réglementées:

— tout ordre professionnel ou organisme similaire auprès duquel le prestataire est inscrit,

— le titre professionnel et l'État membre dans lequel il a été octroyé,

— une référence aux règles professionnelles applicables dans l'État membre d'établissement et aux moyens d'y avoir accès;

g) dans le cas où le prestataire exerce une activité soumise à la TVA, le numéro d'identification visé à l'article 22, paragraphe 1, de la sixième directive 77/388/CEE du Conseil du 17 mai 1977 en matière d'harmonisation des législations des États membres relatives aux taxes sur le chiffre d'affaires - Système commun de taxe sur la valeur ajoutée: assiette uniforme [1].

2. Outre les autres exigences en matière d'information prévues par le droit communautaire, les États membres veillent au moins à ce que, lorsque les services de la société de l'information mentionnent des prix, ces derniers soient indiqués de manière claire et non ambiguë et précisent notamment si les taxes et les frais de livraison sont inclus.

Section 2: Communications commerciales

Article 6
Informations à fournir

Outre les autres exigences en matière d'information prévues par le droit communautaire, les États membres veillent à ce que les communications commerciales qui font partie d'un service de la société de l'information ou qui constituent un tel service répondent au moins aux conditions suivantes:

a) la communication commerciale doit être clairement identifiable comme telle;

---

(1) JO L 145 du 13.6.1977, p. 1. Directive modifiée en dernier lieu par la directive 1999/85/CE (JO L 277 du 28.10.1999, p. 34).

b) la personne physique ou morale pour le compte de laquelle la communication commerciale est faite doit être clairement identifiable;

c) lorsqu'elles sont autorisées dans l'État membre où le prestataire est établi, les offres promotionnelles, telles que les rabais, les primes et les cadeaux, doivent être clairement identifiables comme telles et les conditions pour en bénéficier doivent être aisément accessibles et présentées de manière précise et non équivoque;

d) lorsqu'ils sont autorisés dans l'État membre où le prestataire est établi, les concours ou jeux promotionnels doivent être clairement identifiables comme tels et leurs conditions de participation doivent être aisément accessibles et présentées de manière précise et non équivoque.

Article 7
Communications commerciales non sollicitées

1. Outre les autres exigences prévues par le droit communautaire, les États membres qui autorisent les communications commerciales non sollicitées par courrier électronique veillent à ce que ces communications commerciales effectuées par un prestataire établi sur leur territoire puissent être identifiées de manière claire et non équivoque dès leur réception par le destinataire.

2. Sans préjudice de la directive 97/7/CE et de la directive 97/66/CE, les États membres prennent des mesures visant à garantir que les prestataires qui envoient par courrier électronique des communications commerciales non sollicitées consultent régulièrement les registres "opt-out" dans lesquels les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces dernières.

Article 8
Professions réglementées

1. Les États membres veillent à ce que l'utilisation de communications commerciales qui font partie d'un service de la société de l'information fourni par un membre d'une profession réglementée, ou qui constituent un tel service, soit autorisée sous réserve du respect des règles professionnelles visant, notamment, l'indépendance, la dignité et l'honneur de la profession ainsi que le secret professionnel et la loyauté envers les clients et les autres membres de la profession.

2. Sans préjudice de l'autonomie des organismes et associations professionnels, les États membres et la Commission encouragent les associations et les organismes professionnels à élaborer des codes de conduite au niveau communautaire pour préciser les informations qui peuvent être données à des fins de communications commerciales dans le respect des règles visées au paragraphe 1.

3. Lors de l'élaboration de propositions relatives à des initiatives communautaires qui peuvent s'avérer nécessaires pour assurer le bon fonctionnement du marché intérieur au regard des informations visées au paragraphe 2, la Commission tient dûment compte des codes de conduite applicables au niveau communautaire et agit en étroite coopération avec les associations et organismes professionnels concernés.

4. La présente directive s'applique en sus des directives communautaires régissant l'accès aux activités des professions réglementées et l'exercice de celles-ci.

Section 3: Contrats par voie électronique

Article 9
Traitement des contrats

1. Les États membres veillent à ce que leur système juridique rende possible la conclusion des contrats par voie électronique. Les États membres veillent notamment à ce que le régime juridique applicable au processus contractuel ne fasse pas obstacle à l'utilisation des contrats électroniques ni ne conduise à priver d'effet et de validité juridiques de tels contrats pour le motif qu'ils sont passés par voie électronique.

2. Les États membres peuvent prévoir que le paragraphe 1 ne s'appliquent pas à tous les contrats ou à certains d'entre eux qui relèvent des catégories suivantes:

a) les contrats qui créent ou transfèrent des droits sur des biens immobiliers, à l'exception des droits de location;

b) les contrats pour lesquels la loi requiert l'intervention des tribunaux, des autorités publiques ou de professions exerçant une autorité publique;

c) les contrats de sûretés et garanties fournis par des personnes agissant à des fins qui n'entrent pas dans le cadre de leur activité professionnelle ou commerciale;

d) les contrats relevant du droit de la famille ou du droit des successions.

3. Les États membres indiquent à la Commission les catégories visées au paragraphe 2 auxquelles ils n'appliquent pas le paragraphe 1. Ils soumettent tous les cinq ans à la Commission un rapport sur l'application du paragraphe 2 en expliquant les raisons pour lesquelles ils estiment nécessaire de maintenir les catégories visées au paragraphe 2, point b), auxquelles ils n'appliquent pas le paragraphe 1.

Article 10
Informations à fournir

1. Outre les autres exigences en matière d'information prévues par le droit communautaire, les États membres veillent à ce que, sauf si les parties qui ne sont pas des consommateurs en ont convenu autrement, le prestataire de services fournisse au moins les informations mentionnées ci-après, formulées de manière claire, compréhensible et non équivoque et avant que le destinataire du service ne passe sa commande:

a) les différentes étapes techniques à suivre pour conclure le contrat;

b) si le contrat une fois conclu est archivé ou non par le prestataire de services et s'il est accessible ou non;

c) les moyens techniques pour identifier et corriger des erreurs commises dans la saisie des données avant que la commande ne soit passée;

d) les langues proposées pour la conclusion du contrat.

2. Les États membres veillent à ce que, sauf si les parties qui ne sont pas des consommateurs en ont convenu autrement, le prestataire indique les éventuels codes de conduite pertinents auxquels il est soumis ainsi que les informations sur la façon dont ces codes peuvent être consultés par voie électronique.

3. Les clauses contractuelles et les conditions générales fournies au destinataire doivent l'être d'une manière qui lui permette de les conserver et de les reproduire.

4. Les paragraphes 1 et 2 ne sont pas applicables à des contrats conclus exclusivement par le biais d'un échange de courriers électroniques ou par des communications individuelles équivalentes.

Article 11
Passation d'une commande

1. Les États membres veillent, sauf si les parties qui ne sont pas des consommateurs en ont convenu autrement, à ce que, dans les cas où un destinataire du service passe sa commande par des moyens technologiques, les principes suivants s'appliquent:

— le prestataire doit accuser réception de la commande du destinataire sans délai injustifié et par voie électronique,

— la commande et l'accusé de réception sont considérés comme étant reçus lorsque les parties auxquelles il sont adressés peuvent y avoir accès.

2. Les États membres veillent, sauf si les parties qui ne sont pas des consommateurs en ont convenu autrement, à ce que le prestataire mette à la disposition du destinataire du service des moyens techniques appropriés, efficaces et accessibles lui permettant d'identifier les erreurs commises dans la saisie des données et de les corriger, et ce avant la passation de la commande.

3. Le paragraphe 1, premier tiret, et le paragraphe 2 ne sont pas applicables à des contrats conclus exclusivement au moyen d'un échange de courriers électroniques ou au moyen de communications individuelles équivalentes.

Section 4: Responsabilité des prestataires intermédiaires

Article 12
Simple transport ("Mere conduit")

1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou à fournir un accès au réseau de communication, le prestataire de services ne soit pas responsable des informations transmises, à condition que le prestataire:

a) ne soit pas à l'origine de la transmission;

b) ne sélectionne pas le destinataire de la transmission

et

c) ne sélectionne et ne modifie pas les informations faisant l'objet de la transmission.

2. Les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation.

Article 13
Forme de stockage dite "caching"

1. Les États membre veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à transmettre, sur un réseau de communication, des informations fournies par un destinataire du service, le prestataire ne soit pas responsable au titre du stockage automatique, intermédiaire et temporaire de cette information fait dans le seul but de rendre plus efficace la transmission ultérieure de l'information à la demande d'autres destinataires du service, à condition que:

a) le prestataire ne modifie pas l'information;

b) le prestataire se conforme aux conditions d'accès à l'information;

c) le prestataire se conforme aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue et utilisées par les entreprises;

d) le prestataire n'entrave pas l'utilisation licite de la technologie, largement reconnue et utilisée par l'industrie, dans le but d'obtenir des données sur l'utilisation de l'information

et

e) le prestataire agisse promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il a effectivement connaissance du fait que l'information à l'origine de la transmission a été retirée du réseau ou du fait que l'accès à l'information a été rendu impossible, ou du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible.

2. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette fin à une violation ou qu'il prévienne une violation.

Article 14
Hébergement

1. 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 connaissances, agisse promptement pour retirer les informations ou rendre l'accès à celles-ci impossible.

2. Le paragraphe 1 ne s'applique pas lorsque le destinataire du service agit sous l'autorité ou le contrôle du prestataire.

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible.

Article 15
Absence d'obligation générale en matière de surveillance

1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, 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.

2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement.

CHAPITRE III
MISE EN ŒUVRE

Article 16
Codes de conduite

1. Les États membres et la Commission encouragent:

a) l'élaboration, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs, de codes de conduite au niveau communautaire, destinés à contribuer à la bonne application des articles 5 à 15;

b) la transmission volontaire à la Commission des projets de codes de conduite au niveau national ou communautaire;

c) l'accessibilité par voie électronique des codes de conduite dans les langues communautaires;

d) la communication aux États membres et à la Commission, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs, de leurs évaluations de l'application de leurs codes de conduite et de leur impact sur les pratiques, les us ou les coutumes relatifs au commerce électronique;

e) l'établissement de codes de conduite pour ce qui a trait à la protection des mineurs et de la dignité humaine.

2. Les États membres et la Commission encouragent les associations ou les organisations représentant les consommateurs à participer à l'élaboration et à l'application des codes de conduite ayant des incidences sur leurs intérêts et élaborés en conformité avec le paragraphe 1, point a). Le cas échéant, les associations représentant les personnes souffrant d'un handicap visuel et, de manière générale, les personnes handicapées devraient être consultées afin de tenir compte de leurs besoins spécifiques.

Article 17
Règlement extrajudiciaire des litiges

1. Les États membres veillent à ce que, en cas de désaccord entre un prestataire de services de la société de l'information et le destinataire du service, leur législation ne fasse pas obstacle à l'utilisation des mécanismes de règlement extrajudiciaire pour le règlement des différends, disponibles dans le droit national, y compris par des moyens électroniques appropriés.

2. Les États membres encouragent les organes de règlement extrajudiciaire, notamment en ce qui concerne les litiges en matière de consommation, à fonctionner de manière à assurer les garanties procédurales appropriées pour les parties concernées.

3. Les États membres encouragent les organes de règlement extrajudiciaire des litiges à communiquer à la Commission les décisions importantes qu'ils prennent en

matière de services de la société de l'information ainsi que toute autre information sur les pratiques, les us ou les coutumes relatifs au commerce électronique.

Article 18
Recours juridictionnels

1. Les États membres veillent à ce que les recours juridictionnels disponibles dans le droit national portant sur les activités des services de la société de l'information permettent l'adoption rapide de mesures, y compris par voie de référé, visant à mettre un terme à toute violation alléguée et à prévenir toute nouvelle atteinte aux intérêts concernés.

2. L'annexe de la directive 98/27/CE est complétée par le texte suivant:

"11. Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur ('directive sur le commerce électronique') (JO L 178 du 17.7.2000, p. 1)."

Article 19
Coopération

1. Les États membres disposent de moyens suffisants de contrôle et d'investigation nécessaires à la mise en oeuvre efficace de la présente directive et veillent à ce que les prestataires leur fournissent les informations requises.

2. Les États membres coopèrent avec les autres États membres; à cette fin, ils désignent un ou plusieurs points de contact, dont ils communiquent les coordonnées aux autres États membres et à la Commission.

3. Les États membres fournissent dans les plus brefs délais et conformément au droit national l'assistance et les informations demandées par les autres États membres ou par la Commission, y compris par les voies électroniques appropriées.

4. Les États membres établissent des points de contact accessibles au moins par voie électronique auxquels les destinataires de services et les prestataires de services peuvent s'adresser pour:

a) obtenir des informations générales sur leurs droits et obligations en matière contractuelle ainsi que sur les procédures de réclamation et de recours disponibles en cas de différends, y compris sur les aspects pratiques liés à l'utilisation de ces procédures;

b) obtenir les coordonnées des autorités, associations ou organisations auprès desquelles ils peuvent obtenir d'autres informations ou une assistance pratique.

5. Les États membres encouragent la communication à la Commission des décisions administratives et judiciaires importantes prises sur leur territoire s'agissant des litiges relatifs aux services de la société de l'information ainsi que des pratiques, des us ou des coutumes relatifs au commerce électronique. La Commission communique ces décisions aux autres États membres.

Article 20
Sanctions

Les États membres déterminent le régime des sanctions applicable aux violations des dispositions nationales adoptées en application de la présente directive et prennent toutes mesures nécessaires pour assurer leur mise en oeuvre. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives.

CHAPITRE IV
DISPOSITIONS FINALES

Article 21
Réexamen

1. Avant le 17 juillet 2003 et ensuite tous les deux ans, la Commission présente au Parlement européen, au Conseil et au Comité économique et social un rapport relatif à l'application de la présente directive accompagné, le cas échéant, de propositions visant à l'adapter à l'évolution juridique, technique et économique dans le domaine des services de la société de l'information, notamment en ce qui concerne la prévention de la criminalité, la protection des mineurs, la protection des consommateurs et le bon fonctionnement du marché intérieur.

2. Ce rapport, en examinant la nécessité d'adapter la présente directive, analyse en particulier la nécessité de présenter des propositions relatives à la responsabilité des fournisseurs de liens d'hypertexte et de services de moteur de recherche, les procédures de notification et de retrait (notice and take down) et l'imputation de la responsabilité après le retrait du contenu. Le rapport analyse également la nécessité de prévoir des conditions supplémentaires pour l'exemption de responsabilité, prévue aux articles 12 et 13, compte tenu de l'évolution des techniques, et la possibilité d'appliquer les principes du marché intérieur à l'envoi par courrier électronique de communications commerciales non sollicitées.

Article 22
Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive avant le 17 janvier 2002. Ils en informent immédiatement la Commission.

2. Lorsque les États membres adoptent les dispositions visées au paragraphe 1, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

Article 23
Entrée en vigueur

La présente directive entre en vigueur le jour de sa publication au Journal officiel des Communautés européennes.

Article 24
Destinataires

Les États membres sont destinataires de la présente directive.

ANNEXE
DÉROGATIONS À L'ARTICLE 3

Comme prévu à l'article 3, paragraphe 3, les paragraphes 1 et 2 de l'article 3 ne s'appliquent pas dans les cas suivants:

— le droit d'auteur, les droits voisins, les droits visés par la directive 87/54/CEE [1] et par la directive 96/9/CE [2] ainsi que les droits de propriété industrielle,

— l'émission de monnaie électronique par des institutions pour lesquelles les États membres ont appliqué une des dérogations prévues à l'article 8, paragraphe 1, de la directive 2000/46/CE [3],

— l'article 44, paragraphe 2, de la directive 85/611/CEE [4],

— l'article 30 et le titre IV de la directive 92/49/CEE [5], le titre IV de la directive 92/96/CEE [6], les articles 7 et 8 de la directive 88/357/CEE [7]et l'article 4 de la directive 90/619/CEE [8],

— la liberté des parties de choisir le droit applicable à leur contrat,

— les obligations contractuelles concernant les contrats conclus par les consommateurs,

— la validité formelle des contrats créant ou transférant des droits sur des biens immobiliers, lorsque ces contrats sont soumis à des exigences formelles impératives selon le droit de l'État membre dans lequel le bien immobilier est situé,

— l'autorisation des communications commerciales non sollicitées par courrier électronique.

---

(1) JO L 24 du 27.1.1987, p. 36.
(2) JO L 77 du 27.3.1996, p. 20.
(3) Non encore parue au Journal officiel.
(4) JO L 375 du 31.12.1985, p. 3. Directive modifiée en dernier lieu par la directive 95/26/CE (JO L 168 du 18.7.1995, p. 7).
(5) JO L 228 du 11.8.1992, p. 1. Directive modifiée en dernier lieu par la directive 95/26/CE.
(6) JO L 360 du 9.12.1992, p. 1. Directive modifiée en dernier lieu par la directive 95/26/CE.
(7) JO L 172 du 4.7.1988, p. 1. Directive modifiée en dernier lieu par la directive 92/49/CEE.
(8) JO L 330 du 29.11.1990, p. 50. Directive modifiée en dernier lieu par la directive 92/96/CEE.

ANNEXE 2

CHARTE DE NOMMAGE DE LA ZONE « .FR » DE L'AFNIC
(ASSOCIATION FRANÇAISE POUR LE NOMMAGE INTERNET EN COOPERATION)

I. DISPOSITIONS GÉNÉRALES

1. Préambule

1. La charte de l'Association française pour le nommage Internet en Coopération (AFNIC), ci-après dénommée « charte de nommage » est un document consensuel dont l'objectif est d'assurer une administration harmonieuse des noms de domaine de la zone de nommage en « .fr », au bénéfice de tous.

2. La charte de nommage est établie conformément aux décisions prises par les organes compétents de l'AFNIC en collaboration avec les « comités de concertation » qui composent l'association.

3. La charte de nommage est donc un document évolutif, fruit de la réflexion, des travaux et des accords de ses membres et des partenaires de l'AFNIC.

4. Au sein de la charte de nommage les termes ci-dessous auront les définitions suivantes :

- « AFNIC » : association française pour le nommage Internet en Coopération, association régie par la loi du 1er juillet 1901 et le décret du 16 août 1901 chargée par délégation d'administrer la zone de nommage Internet en « .fr ». Les statuts et la mission de l'AFNIC sont accessibles sur le site de l'AFNIC.

- « charte de nommage » : la charte est composée du présent document et du guide des procédures. Elle est complétée par un ensemble de documents et d'informations accessibles en ligne sur le site Web de l'AFNIC ou directement auprès de l'AFNIC sur simple demande.

- « prestataire Internet » : prestataire technique ayant conclu une convention d'adhésion avec l'AFNIC, en charge de traiter les demandes de ses clients (les organismes demandeurs) quant à l'administration des noms de domaine. Liste des prestataires conventionnés.

- « organisme demandeur » : toute personne physique ou morale qui demande, par l'intermédiaire d'un prestataire Internet membre de l'AFNIC, un acte d'administration sur un nom de domaine.

- « acte d'administration » : tout acte à caractère administratif ou technique relatif à un nom de domaine sur la base des demandes et documentations adressées par les prestataires Internet. Notamment, et sans que cette liste ne soit limitative, création, modification, transmission, changement de prestataire, suppression... d'un nom de domaine.

• « guide des procédures » : document qui détaille l'ensemble des éléments d'ordre technique relatif à la mise en oeuvre d'actes d'administration sur un nom de domaine.

• « nom de domaine orphelin » : nom de domaine qui n'est plus géré par un prestataire internet, soit que celui-ci ait dénoncé sa convention d'adhésion avec l'AFNIC, soit qu'il ait cessé son activité relative à la gestion de nom de domaine.

2. Conditions d'accès au « .fr »

5. La version de la charte de nommage opposable est celle disponible sur le site de l'AFNIC au jour de la réception par cette dernière d'une demande d'acte d'administration adressée par un prestataire Internet. Sauf exception, l'application des nouvelles règles n'est pas rétroactive.

6. La charte de nommage est limitée aux seuls noms de domaine de la zone de nommage en « .fr ».

7. L'attribution d'un nom de domaine au sein de la zone de nommage en « .fr » est possible pour tout organisme demandeur officiellement déclaré en France et pour les personnes physiques résidant en France ou de nationalité française dans le respect des dispositions de la présente charte.

8. Le nom de domaine attribué confère un droit d'usage à l'organisme demandeur et non au prestataire Internet.

9. Le prestataire Internet est l'interface entre l'AFNIC et l'organisme demandeur.

10. Les relations techniques établies entre l'AFNIC et le prestataire Internet dans le cadre d'un acte d'administration sur des noms de domaine sont organisées conformément à la charte de nommage et mis en œuvre en application du guide des procédures disponible sur le site de l'AFNIC.

11. Pour tout type d'acte d'administration, l'organisme demandeur est tenu de s'adresser à un prestataire Internet.

12. Le prestataire Internet a notamment pour tâche de :

• Recueillir toutes les pièces justificatives et informations relatives à une demande d'acte d'administration ;

• S'assurer de la validité des pièces justificatives et informations ;

• Suivre les prescriptions du guide des procédures ;

• Le prestataire Internet est tout particulièrement tenu d'informer les organismes demandeurs qui sont ses clients de toute modification et/ou évolution le concernant (évolution ou cessation d'activité, procédure collective...) qui pourrait avoir un impact quant à la bonne gestion du nom de domaine.

13. L'organisme demandeur doit :

- Prendre connaissance et accepter les termes de la présente charte ;

- Vérifier que sa demande, et particulièrement le choix du terme ou des termes qu'il entend utiliser pour l'attribution d'un nom de domaine :

  - Est licite au regard du droit et notamment des règles d'ordre public,

  - Ne porte pas atteinte aux droits de tiers notamment aux droits d'auteur, aux droits des marques et aux droits de la personne... sans que cette liste soit limitative,

  - Est conforme aux dispositions de la présente charte ;

- Fournir à son prestataire Internet les pièces justificatives qui lui seront demandées en application de la présente charte de nommage ;

- Vérifier l'exactitude des informations qu'il communique à son prestataire Internet et s'engager à les actualiser si nécessaire.

14. L'organisme demandeur est seul responsable des documents, informations et demandes qu'il adresse au prestataire Internet. Le prestataire Internet est responsable de la bonne transmission des documents qu'il adresse à l'AFNIC et/ou des saisies informatiques qu'il opère dans le cadre d'un acte d'administration relatif à un nom de domaine. L'organisme demandeur devra s'adresser à son prestataire Internet pour toute question ou réclamation relative à sa demande.

15. La base de données relative aux noms de domaines administrée par l'AFNIC a fait l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés.

16. L'organisme demandeur, dûment identifié, pourra avoir accès aux données personnelles le concernant et aura un droit de rectification sur l'ensemble de ces éléments en application de la loi « Informatique et libertés » du 6 janvier 1978.

17. En aucun cas l'AFNIC n'est responsable du contrôle du contenu, de la conformité ou de la légalité des éléments qui lui sont remis ou communiqués dans la mesure où ces éléments ou informations sont enregistrés ou établis par des organismes tiers (greffe du tribunal de commerce, INPI, préfecture...).

18. L'AFNIC n'effectue aucune recherche d'antériorité quant aux noms de domaine mais reste gardienne de la bonne application de la charte de nommage. En ce sens elle suspendra tout acte d'administration d'un nom de domaine dès lors que les documents et/ou informations qui lui auront été adressés ne seront pas conformes aux dispositions de la charte de nommage sans que cela constitue pour l'AFNIC une obligation de résultat.

19. L'AFNIC se réserve également le droit de suspendre un nom de domaine pendant un délai d'un mois et de procéder à sa suppression faute de régularisation dans le délai imparti et /ou toute demande d'acte d'administration dans tous les cas où les dispositions de la charte de nommage ne seraient pas respectées ou seraient détournées sans que ceci ne constitue une quelconque obligation à la charge de l'AFNIC.

20. Le droit d'usage d'un nom de domaine est conditionné par le paiement d'une redevance annuelle de maintenance.

21. Pendant toute la durée d'exploitation d'un nom de domaine, cette redevance de maintenance est due par le dernier prestataire Internet en charge dudit nom de domaine, un an après le dernier acte d'administration payant.

22. Les actes d'administration définis aux présentes (partie III) donnent lieu à une facturation due par le prestataire l'ayant demandé.

3. Dispositions pratiques

23. La charte de nommage peut être consultée à tout moment sur le site de l'AFNIC.

24. La charte de nommage est aussi disponible dans le format suivant : Adobe PDF.

25. Pour obtenir la liste des derniers noms de domaine enregistrés, l'organisme demandeur ou le prestataire Internet peut consulter le site de l'AFNIC.

26. Pour toute autre demande il convient de s'adresser aux organismes d'attribution compétents dont la liste est accessible sur le site de l'AFNIC.

II. PRINCIPES DIRECTEURS DU NOMMAGE

1. Répartition de la zone de nommage

1. La zone de nommage « .fr » est décomposée selon les catégories suivantes :

Le « domaine public »

Cette catégorie de noms de domaine est directement organisée et administrée par l'AFNIC.

Elle comporte les extensions suivantes : « .fr », « .asso.fr », « .com.fr », « .nom.fr », « .prd.fr », « .presse.fr » et « .tm.fr ».

Cette catégorie est réglementée conformément aux termes de la présente charte.

Le « domaine sectoriel »

Cette catégorie de noms de domaine permet d'identifier une branche d'activité ou un secteur professionnel et de le structurer de manière homogène.

Elle correspond à des secteurs d'activité réglementés par une autorité en particulier (exemple : ordre, conseil supérieur...).

Cette catégorie de noms de domaine est organisée à la demande de l'autorité compétente qui établit un règlement de nommage pour le secteur qui la concerne et qu'elle soumet pour accord à l'AFNIC.

Une fois le règlement de nommage validé, les noms de domaine correspondants sont administrés par l'AFNIC dans le respect de la présente charte de nommage et du règlement de nommage en cause.

L'AFNIC en accord avec les autorités compétentes des secteurs d'activités réglementés examinera, à l'occasion de chaque demande, l'opportunité de créer un ou plusieurs domaines sectoriels.

Les « conventions de nommage »

Cette catégorie de noms de domaine correspond à des noms de domaine enregistrés sous un format commun pour des entités d'un même secteur d'activité non réglementé.

Elle est organisée et administrée par l'AFNIC dans les conditions détaillées au sein de la présente charte.

Les conventions de nommage sont mises en oeuvre par l'AFNIC en tant que de besoin.

2. Attention : Toutes ces catégories sont susceptibles d'évolution et/ou de compléments.

2. Organisation générale

3. Tout acte d'administration relatif à un nom de domaine repose sur la remise de documents et/ou de justificatifs et/ou d'informations tels que précisés au sein de la présente charte de nommage, sous réserve des spécificités réglementaires régionales ou locales.

4. Tant que le nom de domaine est exploité, l'organisme demandeur qui bénéficie d'un droit d'usage doit pouvoir justifier du respect des dispositions de la présente charte de nommage. Dans l'hypothèse où, à l'occasion d'une demande d'acte d'administration, l'AFNIC devait constater qu'un des noms de domaine de l'organisme demandeur n'était plus justifié, aucune suite ne sera donnée à sa nouvelle demande tant que le sort du nom de domaine non justifié ne sera pas traité (remise des justifications ou suppression).

5. Un certain nombre de termes ne sont pas attribuables à titre de nom de domaine même si la demande répond parfaitement aux critères cités ci-dessus. Cela comprend les termes fondamentaux interdits :

- Liés à l'ordre public ou aux bonnes mœurs,
- Liés au fonctionnement de l'Internet,
- Les noms des organisations internationales et des pays signataires de la convention d'union de Paris.

6. Il en est de même pour le terme France, les noms des collectivités territoriales françaises qui leurs sont réservés, les noms des professions et titres réglementés (singulier et pluriel) sauf exception prévue dans la présente charte.

7. Compte tenu des évolutions, tout nom de domaine composé d'un terme « fondamental interdit » peut subir, un droit de préemption ou de reprise par l'AFNIC, sans dédommagement, assorti d'un délai suffisant pour assurer la migration.

8. L'application des règles relatives aux domaines sectoriels prime sur les règles propres à la catégorie du domaine public.

3. Syntaxe du nommage

9. Sont autorisés :

- les lettres de l'alphabet de « A » à « Z » (minuscule ou majuscule indifféremment), les chiffres de « 0 » à « 9 » et le symbole « - » (tiret) à l'exclusion de tout autre symbole ;
- Les noms de domaine d'une longueur maximum de 255 caractères (63 caractères entre chaque « . » ou « label »);
- Les noms de domaine composés :
  - directement sous la racine « .fr » d'au moins 3 lettres (« aaa.fr ») ou d'un chiffre et d'une lettre (« z2.fr »),
  - sous les autres domaines publics : d'au moins deux caractères « aa.tm.fr » / « m2.asso.fr »).
- le « . » (point) comme séparateur de sous-domaine dans les catégories de domaines sectoriels et de conventions de nommage.

10. Sont interdits :

- Les noms de domaine constitués uniquement de chiffres ;
- Les noms de domaine débutant ou se terminant par le caractère « - » (tiret) ;
- Les caractères accentués.

A noter, seule la lettre sera retenue dans le cas de lettre associée à des caractères accentués (ex : ñ, ë seront enregistrés respectivement n, et e).

4. Règles propres aux domaines publics

Pour l'ensemble des noms de domaine publics, le document justificatif n'est pas demandé à l'appui de l'acte d'administration à l'exception :

- des demandes sous « .fr » émanant d'organismes non identifiés auprès de l'INSEE,
- des demandes émanant d'organismes créés par loi ou décret,

• des demandes émanant d'organismes répertoriés en syndicat professionnel,

• des demandes émanant d'organismes désirant un enregistrement sous « .prd.fr ».

• L'AFNIC se réserve, en tant que de besoin, de demander communication des justificatifs dans les cas suivants :

• contrôle ponctuel réalisé à sa discrétion pour le bon suivi de la charte de nommage,

• impossibilité temporaire ou définitive d'accès aux bases de données permettant de vérifier les justifications,

• incohérence dans les informations recueillies par l'AFNIC auprès des dites bases de données.

Pour tous les contrôles réalisés après la création d'un nom de domaine, le prestataire est tenu de communiquer les documents justificatifs dans un délai maximum de 72 heures ; à défaut, le nom de domaine est suspendu pendant un délai d'un mois puis supprimé faute de régularisation dans le délai imparti.

11. Les éléments justificatifs nécessaires à la réalisation d'un acte d'administration pour un nom de domaine relevant d'une extension du domaine public de la zone de nommage « .fr » sont décrits ci-après :

Domaines	Demandeur	Justifications
.fr	Société ou personne morale dotée d'un numéro SIREN / SIRET (hors domaines sectoriels, conventions de nommage ou autres zones publiques).	- un extrait de K Bis pour les sociétés et commerçants ou, - un identifiant au répertoire INSEE pour les autres professions.
	Entité titulaire d'une marque dûment enregistrée.	- certificat définitif INPI, OHMI ou OMPI (sous réserve que la France figure parmi les pays concernés par le dépôt).
	Tout organisme non identifié auprès de l'INSEE, créé par loi ou décret, ou répertorié en syndicat professionnel.	- loi, décret ou, - copie d'immatriculation délivrée par la mairie ou la préfecture.
	Association immatriculée auprès de l'INSEE	- copie de l'identifiant au répertoire INSEE.
.asso.fr	Association	- copie de la parution au *JO* ou récépissé de déclaration à la Préfecture ou, - copie de l'identifiant au répertoire INSEE.
.nom.fr	Personne physique résidant en France	Le nom de domaine en « .nom.fr » ne peut être accordé qu'à une personne majeure et capable. - copie certifiée conforme de la carte nationale d'identité, ou du permis de conduire, ou d'une carte de séjour, et, - un justificatif de domicile de moins de 3 mois (facture EDF-GDF, téléphone).

Domaines	Demandeur	Justifications
.nom.fr	Personne physique de nationalité française résidant à l'étranger	Le nom de domaine en « .nom.fr » ne peut être accordé qu'à une personne majeure et capable. - copie certifiée conforme de la carte nationale d'identité ou du permis de conduire, - justificatif de domicile de moins de 3 mois du pays de résidence.
.prd.fr	Projet ou programme de recherche et développement	- présentation écrite du projet avec la liste des membres.
.presse.fr	Organisme de presse	- copie du document ISSN de la Bibliothèque nationale.
.tm.fr	Marque déposée	- enregistrement de la marque sur présentation du certificat définitif INPI, OHMI ou OMPI (sous réserve que la France figure parmi les pays concernés par le dépôt) ou, - copie de la demande d'enregistrement ou de la parution au BOPI et dans les six mois suivant la demande d'enregistrement, la remise du certificat INPI définitif ou du certificat d'identité avec état des inscriptions pour valider définitivement la demande.
.com.fr	Toute personne physique ou morale	- justificatif d'identité (sur la base des mêmes documents que pour les enregistrements sous les autres domaines publics).

12. Les règles suivantes régissent les conditions d'attribution des noms de domaine dans toute la zone de nommage « .fr » à l'exception de l'extension « .com.fr ».

13. Les abréviations, raccourcis ou autres adaptations de termes peuvent être envisagés de même que l'ajout d'un terme (tel que conseil, agence, société, groupe, entreprise, ...) de langue française exclusivement de nature à qualifier l'activité de l'organisme demandeur, son nom de domaine ou pallier une homonymie. Ces adaptations ne sont possibles que si elles sont justifiées au regard des documents fournis en application de la présente charte.

14. L'organisme demandeur peut obtenir l'attribution d'un nombre illimité de noms de domaine dès lors qu'ils soient justifiés au regard de la charte.

15. Pour ce qui concerne la justification par extrait K Bis ou identifiant INSEE, l'organisme demandeur choisit le ou les termes parmi les catégories suivantes : dénomination sociale, sigle, enseigne, nom commercial. Il en est de même pour les justificatifs relatifs aux autres extensions du domaine public.

16. Dans le cas où le nom de domaine figurant sur l'identifiant INSEE ou sur le K Bis serait composé de plusieurs termes, l'organisme demandeur peut choisir un seul de ces termes à l'exclusion des termes non attribuables et des termes non discriminants (ex.: article, préposition,...).

17. Une société dont la dénomination sociale est identique au nom d'une commune française peut être enregistrée directement sous « .fr » sur présentation du K Bis et du dépôt de marque antérieur à 1985.

18. Pour les noms de domaines en « .fr » créés sur la base d'un certificat définitif validé par l'INPI, il est précisé que le nom de domaine devra respecter précisément le terme tel qu'il figure sur le certificat, dans le respect des règles de syntaxe qui figurent au sein de la charte.

Attention, le certificat définitif d'enregistrement de la marque n'est délivré que dans un délai de 6 mois après la demande d'enregistrement selon les procédures INPI.

19. En cas d'homonymie, les autres marques identiques ne pourront être enregistrées que sous l'extension « .tm.fr ». Il ne sera pas possible d'ajouter un élément distinctif à ces marques de nature à obtenir une création en « .fr ».

20. Pour les noms de domaine en « .fr » créés pour les associations sur la base d'un identifiant INSEE, il est précisé que le nom de domaine doit respecter exactement les termes tels qu'ils figurent dans l'une des rubriques de l'identifiant (à savoir les nom, enseigne et sigle complets et exacts).

21. Le nom de domaine attribué engage la responsabilité de l'organisme demandeur qui ne doit enregistrer comme sous-domaine que des entités appartenant à son organisme. (À titre d'exemple l'enregistrement de « societeB.societeA.fr » est fortement déconseillé).

22. Il est par ailleurs recommandé de regrouper les entités régionales, filiales, divers services ..., d'un même organisme dans la hiérarchie de cet organisme (exemple : « branche.societe.fr », « filiale.groupe.fr »).

Spécificité de l'extension « .com.fr »

23. L'enregistrement n'est autorisé que si le terme n'est pas déjà enregistré à l'identique dans l'une des extensions du domaine public.

24. L'enregistrement sous l'extension « .com.fr » n'empêche pas un organisme demandeur d'enregistrer postérieurement le même terme dans une des autres extensions du domaine public.

Spécificité de l'extension « .nom.fr »

25. Le nom de domaine d'une personne physique obéit à la syntaxe suivante : « patronyme.nom.fr », et/ou « patronyme-champlibre.nom.fr ».

26. Le patronyme s'entend du nom de famille ou du nom de jeune fille ou du pseudonyme tel qu'il figure sur le document d'identité fourni.

27. Toute personne procédant à un enregistrement sous l'extension « .nom.fr » peut à tout moment demander à bénéficier de l'option dite « liste rouge ».

28. Lorsque l'option "liste rouge" est activée, aucune information d'ordre privé (nom, adresse, téléphone, télécopie et le cas échéant courrier électronique) n'est accessible en consultation sur la base publique Whois. Seules figurent sur cette base des informations d'ordre technique, notamment : contact technique, coordonnées du prestataire Internet et serveurs DNS.

Spécificité de l'extension « asso.fr »

29. Le nom de domaine des associations obéit par principe à l'enregistrement sous l'extension « .asso.fr ».

30. Les associations peuvent demander la création du nom de domaine correspondant au sigle sous réserve qu'il soit l'acronyme exact de leurs dénominations.

31. Les associations peuvent également demander la création du nom de domaine sur la base de leur enseigne sous réserve qu'elle figure sur les documents justificatifs.

32. Cependant, les associations qui disposent d'une identification INSEE peuvent si elles le désirent bénéficier d'un enregistrement sous l'extension « .fr ». Cette demande n'est pas exclusive d'un enregistrement sous l'extension « .asso.fr ». Les associations devront obligatoirement présenter une copie de l'identifiant au répertoire INSEE correspondant.

5. Règles propres aux domaines sectoriels

33. Les modalités propres à chaque domaine sectoriel sont définies dans le règlement de nommage correspondant, accessible auprès de chacune des autorités compétentes dont la liste est disponible ci-dessous *(la liste des contacts figurant dans la charte n'a pas été reproduite).*

Domaines sectoriels	Demandeur	Justifications et avis
.aeroport.fr	Aéroport	- un identifiant au répertoire INSEE - l'avis de l'UCCEGA.
.assedic.fr	Assedic	- un identifiant au répertoire INSEE - la validation de l'UNEDIC.
.avocat.fr *La zone « .avocat.fr » remplace définitivement « .barreau.fr »	Avocat	- un extrait Kbis ou - un identifiant au répertoire INSEE.
.avoues.fr	Avoués	- un extrait K Bis ou l'identifiant au répertoire INSEE - l'avis de la Chambre nationale des avoués.

Domaines sectoriels	Demandeur	Justifications et avis
.cci.fr	Chambre de commerce et de l'industrie. Ce domaine est sous l'autorité de l'Association des chambres françaises de commerce et d'industrie (ACFCI).	- un identifiant au répertoire INSEE, - l'avis de l'ACFCI.
.chambagri.fr	Chambre d'agriculture	-un extrait K Bis ou un identifiant au répertoire INSEE, - l'avis de l'Assemblée permanente des chambres d'agriculture.
.chirurgiens-dentistes.fr* * remplace définitivement « ch-dentiste.fr »	Chirurgien-dentiste	- l'attestation d'inscription au tableau de l'ordre délivrée par l'ordre départemental concerné ou - la photocopie recto-verso de la carte professionnelle.
.experts-comptables.fr	Expert comptable	- un extrait K Bis ou un identifiant au répertoire INSEE, - l'avis du Conseil supérieur de l'ordre des experts comptables.
.geometre-expert.fr	Géomètre expert	- un extrait K Bis ou un identifiant au répertoire INSEE, et, - la carte professionnelle et, - l'avis de l'Ordre des géomètres Experts.
.gouv.fr	Ministère	- un identifiant au répertoire INSEE et, - la validation de la Délégation interministérielle à la réforme de l'État (DIRE).
.greta.fr	Groupement d'établissement de l'éducation nationale	- un identifiant au répertoire INSEE.
.huissier-justice.fr	Huissier de justice	- un extrait K Bis ou un identifiant au répertoire INSEE, et, - l'avis de la Chambre nationale des huissiers de justice.
.medecin.fr	Médecin	- un extrait K Bis ou un identifiant au répertoire INSEE - la validation de l'Ordre national des médecins.
.notaires.fr	Notaire	- un extrait K Bis ou un identifiant au répertoire INSEE - la validation du Conseil supérieur du notariat.
.pharmacien.fr	Pharmacien	- un extrait K Bis ou un identifiant au répertoire INSEE, et, - l'avis du Conseil national de l'ordre des pharmaciens.

Domaines sectoriels	Demandeur	Justifications et avis
.port.fr	Port	- un extrait K Bis ou un identifiant au répertoire INSEE, et, - avis de l'Union des ports autonomes et des chambres de commerce et d'industrie maritimes (UPACCIM).
.veterinaire.fr	Vétérinaire	- un extrait K Bis ou un identifiant au répertoire INSEE - l'avis de l'Ordre national des vétérinaires.

6. Règles spécifiques aux conventions de nommage

34. Les conventions de nommage n'ont plus de caractère obligatoire, mais leur application relève de la seule responsabilité des autorités administratives en charge du secteur, et ceci sans contrôle de l'AFNIC.

Académies : format d'enregistrement : ac-nom.fr (« nom » étant l'Académie) Ex. : ac-lyon.fr. Un identifiant au répertoire INSEE doit être fourni. (Les lycées et collèges sont enregistrés comme sous-domaines des académies correspondantes, mais les établissements privés non pris en charge par une académie sont enregistrés directement sous .fr).

Ambassades : format d'enregistrement : amb-nom.fr (« nom » étant une ville ou un pays). Ex. : amb-wash.fr (Ambassade de France à Washington). Un identifiant au répertoire INSEE doit être fourni ou, à défaut, une lettre à en-tête de l'ambassade signée par l'ambassadeur.

Assistance publique : format d'enregistrement : ap-nom.fr (« nom » est une ville). Ex. : ap-hop-paris.fr (hôpitaux de la Ville de Paris). Un identifiant au répertoire INSEE doit être fourni.

Bibliothèques municipales : format d'enregistrement : bm-nom.fr (« nom » est un nom de ville). Ex. : bm-lyon.fr. Un identifiant au répertoire INSEE doit être fourni.

Bovin de croissance : convention de nommage mise en place par la Fédération bovins croissance. Format d'enregistrement : departement-bovins-croissance.fr (département est le nom du département). Ex. : creuse-bovins-croissance.fr (syndicat de la creuse pour les bovins de croissance). Un identifiant au répertoire INSEE ou autre justificatif doit être fourni.

Caisses d'allocations familiales : domaine sous l'autorité de la Caisse nationale d'allocations familiales (CNAF). Enregistrement sous caf.fr. Contacter le responsable administratif de la zone concernée.

Caisses régionales d'assurance maladie des artisans et commerçants : domaine sous l'autorité de la caisse nationale d'assurance maladies des professions indépendantes. Format d'enregistrement : canam.fr. Contacter le responsable administratif de la zone concernée.

Caisses d'épargne : domaine sous l'autorité du centre national des caisses d'épargne (CENCEP). Enregistrement sous caisse-epargne.fr. Contacter le responsable administratif de la zone concernée.

Centres d'économie rurale : format d'enregistrement : cerxx.asso.fr et /ou cerxx.fr (« xx » : est le n° du département). Un identifiant au répertoire INSEE, un récépissé de déclaration à la préfecture ou une copie de la parution au *JO* doit être fourni(e).

Centres hospitaliers : format d'enregistrement : chu-xx.fr ou chru-xx.fr ou ch-xx.fr ou hopital-xx.fr (« xx » est de la ville d'implantation ou le nom de l'hôpital). Ex. : chu-rouen.fr (centre hospitalier universitaire de Rouen). Un identifiant au répertoire INSEE doit être fourni.

Centres régionaux de la propriété forestière : domaine sous l'autorité du centre régional de la propriété forestière d'Alsace Lorraine. Enregistrement sous le domaine crpf.fr. Contacter le responsable administratif de la zone concernée.

Chambres des métiers : format d'enregistrement : cm-nom.fr et/ou cm-numérodedépartement.fr (« nom » est une ville, d'un département ou d'une région). Ex. : cm-annecy.fr (Chambre des métiers de Haute Savoie). Un identifiant au répertoire INSEE doit être fourni.

Comités départementaux du tourisme : format d'enregistrement : cdt-nom.fr et/ou cdt-tourisme-nom.fr (« nom » est un département). Ex. : cdt-vaucluse.fr (comité départemental du tourisme du Vaucluse). Un identifiant au répertoire INSEE doit être fourni.

Comités régionaux du tourisme : format d'enregistrement : crt-nom.fr (« nom » est un nom de région). Ex. : crt-aquitaine.fr (comité régional du tourisme d'Aquitaine). Un identifiant au répertoire INSEE doit être fourni.

Communautés d'agglomérations (nouvelle appellation des districts) : format d'enregistrement : agglo-nom.fr (« nom » est la communauté d'agglomérations). Ex. : agglo-montbeliard.fr (communauté d'agglomérations du pays de Montbeliard). Un identifiant au répertoire INSEE doit être fourni.

Communautés de communes : format d'enregistrement : cc-nom.fr (« nom » officiellement déclaré). Ex. : cc-confolentais.fr (communauté de communes du Confolentais). Un extrait K Bis ou un identifiant au répertoire INSEE doit être fourni.

Confédération de l'artisanat et des petites entreprises du bâtiment : convention de nommage mise en place par la confédération de l'artisanat et des petites entreprises du bâtiment. Format d'enregistrement : 3 noms de domaine dont l'un doit être capeb-xx.fr (xx correspond au nom du département ou de la région). En cas d'existence de plusieurs entités dans un même département, xx est le nom de la ville d'implantation de la structure et non le numéro du département. Les autres noms de domaine doivent conserver la racine capeb. Ex. : capeb-ain.fr / capeb01.fr (Confédération de l'Ain). Un identifiant au répertoire INSEE doit être fourni.

Conseils généraux : format d'enregistrement : cgxx.fr et/ou cg-xx.fr et /ou xx.fr (xx est le numéro ou le nom du département). Ex. : cg23.fr /creuse.fr/cg-creuse.fr (Conseil Général de la Creuse). Un identifiant au répertoire INSEE doit être fourni. Attention « numerodedepartement.fr » n'est pas enregistrable.

Conseils régionaux : format d'enregistrement :crxx.fr et/ou cr-xx.fr et /ou xx.fr (xx est le « nom » de la région). Ex. : cr-aquitaine.fr, aquitaine.fr, craquitaine.fr (Conseil régional d'Aquitaine). Un identifiant au répertoire INSEE doit être fourni.

Consulats : format d'enregistrement : consulfrance-nomdelaville.fr (pour les consulats français à l'étranger) et consulnomdupays-nomdelaville.fr (pour les consulats étrangers en France). Un identifiant au répertoire INSEE doit être fourni ou à défaut, une lettre à en-tête du consulat signée par le consul.

Contrôle laitier : convention de nommage mise en place par la fédération de Contrôle Laitier. Format d'enregistrement : departement-controle-laitier.fr (« departement » est le nom du département). Ex. : calvados-controle-laitier.fr (Syndicat d'Élevage du contrôle laitier du Calvados). Un identifiant au répertoire INSEE ou autre justificatif doit être fourni.

Crédit agricole : convention de nommage mise en place par la Caisse nationale du crédit agricole. 3 noms de domaine ; format d'enregistrement des agences et des filiales du Crédit Agricole : ca-nom.fr, + 2 autres domaines selon justificatif (« nom » est celui de l'agence). Ex. : ca-alsace.fr. Un extrait K Bis ou un identifiant au répertoire INSEE doit être fourni.

Districts (ancienne appellation des communautés d'agglomérations) : format d'enregistrement : district-xxx.fr (« xxx » est le nom du district ou à défaut le nom de la ville d'implantation). Ex. : district-parthenay.fr ou district-vernon.fr Un identifiant au répertoire INSEE doit être fourni.

Ecoles d'agriculture : enregistrement des lycées publics en sous domaines de : educagri.fr Ex. : esa-angers.educagri.fr Les demandes sont à déposer directement auprès du responsable administratif du domaine educagri.fr.

Ecoles régionales des beaux-arts : format d'enregistrement : erba-nom.fr : erba-nom.fr (« nom » est une ville). Ex. : erba-rennes.fr (écoles régionales des Beaux-Arts de Rennes). Un identifiant au répertoire INSEE doit être fourni.

Fédération nationale des centres de lutte contre le cancer : domaine sous l'autorité de la Fédération nationale des centres de lutte contre le cancer. Enregistrement sous fnclcc.fr. Contacter le responsable administratif de la zone concernée.

Fédération départementale des syndicats d'exploitants agricoles : convention de nommage mise en place par la Fédération nationale des syndicats d'exploitants agricoles. Format d'enregistrement : fdseaXX.fr (xx est le numéro de département). Ex. : fdsea51.fr (fédération départementale de la Marne).

Fédération départementale et régionale du bâtiment, unions et syndicats nationaux : convention de nommage mise en place par la Fédération française du Bâtiment. Format d'enregistrement : ffbatiment-XX.fr (xx est le

numéro de département), ffbatiment-nomreg.fr (nomreg est le nom de la région en lettres ou abrégé), ffbatiment-nomunion.fr (nomunion est le nom ou sigle de l'union ou du syndicat).

Groupama et Crama : format d'enregistrement : groupama-nom.fr (« nom » est une entité en toutes lettres, sigle ou abrégé). Ex. : groupama-ca.fr ou groupama-centre-atlantique.fr pour le Groupama Centre Atlantique ; groupama-normandie.fr pour la crama de Normandie. Un extrait K Bis ou un identifiant au répertoire INSEE doit être fourni.

Instituts universitaires de formation des maîtres : domaine sous l'autorité de l'Institut universitaire des maîtres de Paris. Enregistrement sous iufm.fr. Contacter le responsable administratif de la zone concernée.

Instituts Universitaires de Technologie : format d'enregistrement : iut-nom.fr (« nom » est une ville). Ex. : iut-lannion.fr - Il est recommandé d'inclure un IUT dans la hiérarchie de l'université dont il dépend. Ex. : iut.univ-aix.fr plutôt qu'iut-aix.fr. Un identifiant au répertoire INSEE doit être fourni.

Mairies et villes : format d'enregistrement : mairie-xx.fr et/ou ville-xx.fr et/ou xx.fr (« xx » est le nom d'une ville). Ex. : mairie-metz.fr, ville-metz.fr, metz.fr. Un identifiant au répertoire INSEE doit être fourni. Attention : - pour les communes homonymes, le numéro de département sera systématiquement ajouté.

– l'ajout du numéro de département à tout ou partie du nom de la commune est possible sur demande à condition qu'il n'existe pas de communes homonymes dans le même département ;

– une entreprise détentrice d'un dépôt de marque antérieur à 1985, peut obtenir le nom de domaine correspondant au nom d'une ville. Ex : evian.fr pour la société Evian.

Offices de tourisme : format d'enregistrement : ot-nom.fr (« nom » est une ville). Ex. : ot-avignon.fr. Un identifiant au répertoire INSEE doit être fourni.

Offices de tourisme étrangers : format d'enregistrement : nom-tourisme.fr (nom du pays en français). Ex. : italie-tourisme.fr. Un identifiant au répertoire INSEE doit être fourni.

Technopoles : format d'enregistrement : tech-nom.fr (« nom » est une ville). Ex. : tech-quimper.fr. Un identifiant au répertoire INSEE doit être fourni.

Unions des associations des familles : domaine sous l'autorité de la fédération des unions des associations des familles. Enregistrement sous : unaf.fr. Contacter le responsable administratif de la zone concernée.

Universités : format d'enregistrement : univ-nom.fr ou u-nom.fr (« nom » est le nom d'université, souvent lié à une ville). Ex. : univ-rennes1.fr (université de Rennes1), u-grenoble3.fr (université de Grenoble3). Un identifiant au répertoire INSEE doit être fourni.

III. ACTES D'ADMINISTRATION SUR LES NOMS DE DOMAINE

1. Création du nom de domaine

1. La phase de création du nom de domaine, c'est-à-dire la phase qui vise à permettre l'enregistrement et l'attribution d'un nom de domaine, est réalisée pour le compte de l'organisme demandeur auprès de l'AFNIC par l'intermédiaire du prestataire Internet qu'il aura choisi parmi la liste des prestataires Internet disponible sur le site de l'AFNIC.

2. Toute demande de création de nom de domaine est réalisée selon la règle du « premier arrivé, premier servi », dans le strict respect de la présente Charte de nommage.

3. Les demandes de création de noms de domaine ne doivent en aucun cas porter atteinte aux droits des tiers ni à l'ordre public.

4. A ce titre, l'AFNIC se réserve le droit d'exercer toutes mesures afin de faire cesser l'atteinte aux droits des tiers et la possibilité d'engager toutes procédures adaptées, à l'encontre de tout contrevenant, sans que cela constitue pour elle une obligation quelconque.

5. Dans le cas où le nom de domaine serait créé sur la base de pièces justificatives provisoires, (K Bis provisoire ou en cours de modification...), et à défaut pour l'AFNIC de pouvoir vérifier sur les bases de données l'existence de la justification définitive dans les délais impartis, l'AFNIC procède à la suspension du nom de domaine.

6. Le nom de domaine reste enregistré au nom de l'organisme demandeur dans les bases de données mais ne peut plus être utilisé pour accéder aux services correspondants (Site web, courrier électronique...). Le nom de domaine est suspendu pour une période maximum d'un mois.

7. Il appartient à l'organisme demandeur de régulariser la situation en fournissant à l'AFNIC via son prestataire Internet les justifications. Pendant cette période l'AFNIC fait ses meilleurs efforts pour procéder à la remise en service du nom de domaine dans les 72 heures ouvrées à compter de la réception des justificatifs définitifs.

8. Faute de régularisation dans les délais impartis, le nom de domaine est supprimé sans préavis ni indemnité. Une fois le nom de domaine supprimé celui-ci peut être ré-attribué à un tiers qui en ferait la demande dans le respect des termes de la présente Charte.

9. Dans le cas où le nom de domaine créé sur la base d'une demande d'enregistrement de marque sous l'extension « .tm.fr » n'aboutit à aucune parution au BOPI dans les délais prévus par les procédures de l'INPI, l'AFNIC procède à la suppression du nom de domaine.

10. Pour la bonne gestion de la zone de nommage, l'AFNIC s'interdit de donner suite à toute démarche préalable à une demande de création de nom de domaine. Elle s'interdit ainsi de donner suite à des demandes de préenregistrement ou de réservation de noms de domaine. Une procédure de préenregistrement est toutefois possible auprès d'organismes habilités à cet effet et dont la liste est accessible ici, dans les conditions qui y sont précisées.

2. Modifications relatives au nom de domaine ou aux éléments techniques et administratifs

11. L'organisme demandeur peut, via son prestataire, solliciter la modification du nom de domaine créé pour tenir compte d'une modification intervenue dans le ou les éléments de justification (modification de la raison sociale, de la dénomination commerciale, de l'enseigne, changement du nom de l'association, modification d'une marque...).

12. La demande de modification ne peut être prise en compte par l'AFNIC qu'à la condition que l'organisme demandeur fournisse les éléments de justification correspondants.

13. La modification d'un nom de domaine s'accompagne, au choix de l'organisme demandeur, d'une période initiale de 1 (un) ou 2 (deux) mois dite « période de migration » au cours de laquelle le nom de domaine initial et le nouveau nom de domaine coexistent.

14. L'organisme demandeur peut solliciter un délai supplémentaire qui ne saurait excéder 1 (un) an à compter de la demande de modification adressée par le prestataire Internet à l'AFNIC et sous réserve de fournir les éléments de justification correspondants. Le délai supplémentaire accordé par l'AFNIC varie en fonction de l'ancienneté du nom de domaine initialement enregistré.

15. L'organisme demandeur peut, via son prestataire Internet, demander des modifications d'éléments administratifs le concernant (Changement du contact technique ou administratif, changement d'adresse).

16. Dans le cadre d'une « transformation de société » c'est-à-dire du changement de forme juridique d'une société au cours de son existence (à titre d'exemple, lorsqu'une société à responsabilité limitée change de forme sociale pour devenir une société anonyme), l'organisme demandeur est tenu de communiquer à l'AFNIC, via son prestataire Internet les éléments justificatifs faisant état de cette transformation.

3. Transmission du nom de domaine

17. La « transmission » du nom de domaine peut intervenir dans les cas détaillés ci-après.

18. Pour des raisons administratives et techniques, la transmission du nom de domaine dans les cas susvisés impose une procédure de suppression/re-création du nom de domaine en cause. La procédure de suppression/re-création du nom de

domaine est réalisée le même jour. La procédure de transmission est destinée à éviter qu'une fois supprimé le nom de domaine puisse être re-attribué à un tiers non autorisé.

19. Comme tout acte d'administration, la demande de transmission d'un nom de domaine est adressée par un prestataire Internet pour le compte de l'organisme demandeur.

20. L'organisme demandeur bénéficiaire de la transmission doit satisfaire aux exigences de la Charte notamment pour ce qui concerne la fourniture des pièces justificatives.

21. La transmission de nom de domaine ne saurait avoir des effets contraires à la charte de nommage.

22. Le prestataire Internet est tenu d'intervenir dans le strict respect du guide des procédures.

23. Dans tous les cas, l'AFNIC se réserve la faculté de demander tout justificatif complémentaire à ceux d'ores et déjà identifiés au sein de la présente Charte de nommage pour procéder à toute vérification nécessaire.

3.1. Fusion

24. Le terme de « fusion » s'entend de l'opération décrite aux articles L. 236-1 et L. 236-3 du Code de commerce, par laquelle deux sociétés au moins se réunissent pour n'en former qu'une seule. Cette opération peut résulter de la transmission du patrimoine d'une ou plusieurs sociétés soit à une société existante, soit à une société nouvelle qu'elles constituent.

25. Lorsqu'une demande de transmission de nom de domaine est effectuée suite à une opération de fusion, l'organe dirigeant de la société nouvellement créée ou de la société absorbante, doit joindre à sa demande, pour chacune des sociétés concernées :

- Une copie de l'extrait K Bis des sociétés concernées faisant état de la fusion ;

- Une copie certifiée conforme des publications effectuées dans le ou les journaux d'annonces légales ;

- La lettre d'acceptation selon le modèle type de l'AFNIC accessible ici signée par l'organisme demandeur initial confirmant son acceptation ou tout autre document attestant de l'acceptation de l'ancien organisme demandeur (ex : PV) sous réserve de la transmission et la réalisation de toutes les démarches préalables à l'égard des tiers (notamment à l'égard du prestataire Internet d'origine).

3.2. Scission

26. Le terme « scission » s'entend de l'opération décrite aux articles L 236-1 et L 236-3 du Code de commerce, par laquelle une société (la société « scindée ») transmet son patrimoine à deux ou plusieurs sociétés existantes ou nouvelles.

27. Lorsqu'une demande de transmission de nom de domaine est effectuée suite à une opération de scission, l'organe dirigeant de la société bénéficiaire de celle-ci, doit joindre à sa demande :

- Une copie de l'extrait K Bis des sociétés concernées faisant état de la scission ;

- Une copie certifiée conforme des publications effectuées dans le ou les journaux d'annonces légales ;

- La lettre d'acceptation selon le modèle type de l'AFNIC accessible ici signée par l'organisme demandeur initial confirmant son acceptation ou tout autre document attestant de l'acceptation de l'ancien organisme demandeur (ex : PV) sous réserve de la transmission et la réalisation de toutes les démarches préalables à l'égard des tiers (notamment à l'égard du prestataire Internet d'origine).

3.3. Apport partiel d'actif

28. Le terme « apport partiel d'actif » s'entend de l'opération décrite à l'article L 236-22 du code de commerce par laquelle une société fait l'apport à une autre société (existante ou nouvelle) d'une partie de ses éléments d'actif et reçoit, en échange, des parts ou actions émises par la société bénéficiaire des apports à la condition expresse que l'apport partiel d'actifs en cause ait pour objet les éléments actifs et passifs d'une branche complète d'activité.

29. Lorsqu'une demande de transmission de nom de domaine est effectuée suite à un apport partiel d'actif placé sous le régime des scissions, l'organe dirigeant de la société bénéficiaire doit joindre à sa demande une attestation du commissaire aux comptes si elle en a un, ou le cas échéant, d'un expert comptable certifiant que :

- Le traité d'apport partiel d'actif mentionne l'option pour le régime des scissions ;

- Le nom de domaine de la société apporteuse a effectivement été compris dans cet apport.

30. L'organisme demandeur doit également joindre à sa demande :

- Une copie du K Bis des sociétés concernées faisant état de l'apport partiel d'actif ;

- Une copie certifiée conforme des publications effectuées dans le ou les journaux d'annonces légales ;

- La lettre d'acceptation selon le modèle type de l'AFNIC accessible ici signée par l'organisme demandeur initial confirmant son acceptation ou tout autre document attestant de l'acceptation de l'ancien organisme demandeur (ex : PV) sous

réserve de la transmission et la réalisation de toutes les démarches préalables à l'égard des tiers (notamment à l'égard du prestataire Internet d'origine).

3.4. Cession de fonds de commerce

31. La cession de fonds de commerce s'entend des articles L 141-1 et suivants du Code de commerce. Cette cession, qui peut être totale ou partielle, peut intégrer un ou plusieurs noms de domaine.

32. Dans l'hypothèse où la cession totale ou partielle d'un fonds de commerce porte, entre autres éléments sur un ou plusieurs noms de domaine, l'AFNIC procède à la transmission du nom de domaine au bénéfice du cessionnaire à la condition de recevoir de sa part :

- La copie certifiée conforme du contrat de cession de fonds de commerce portant justificatif de l'enregistrement du centre des impôts faisant mention exacte du ou des noms de domaines en cause,

- La copie de la publication au journal d'annonces légales et de l'avis au bulletin officiel des annonces civiles et commerciales,

- La lettre d'acceptation selon le modèle type de l'AFNIC accessible ici signée par l'organisme demandeur initial confirmant son acceptation ou tout autre document attestant de l'acceptation de l'ancien organisme demandeur (ex : PV) sous réserve de la transmission et la réalisation de toutes les démarches préalables à l'égard des tiers (notamment à l'égard du prestataire Internet d'origine).

3.5. Apports en société

33. Sont ici visés les apports en société portant sur un ou plusieurs noms de domaine tels que visés par les articles 1832 et 1843-1 du code civil et des articles appropriés du Code de commerce.

34. Dans l'hypothèse d'un apport en société portant sur un ou plusieurs noms de domaine, l'AFNIC procède à la transmission du nom de domaine à la société bénéficiaire de cet apport à la condition de recevoir de sa part :

- Pour le cas où l'apport a lieu au moment de la constitution de la société : statut de la société constituée justifiant des apport et le cas échéant rapport du commissaire aux apports ;

- Pour le cas où l'apport a lieu en cours d'existence de la société : procès verbal de l'assemblée générale extraordinaire de la société bénéficiaire de l'apport et le cas échéant rapport du commissaire aux apports.

3.6. Dissolution amiable

35. La dissolution amiable s'entend de la volonté commune de mettre un terme à l'existence d'une société induisant le transfert au bénéfice d'une des parties, d'un ou de plusieurs noms de domaine.

36. Dans l'hypothèse d'une dissolution amiable portant sur un ou plusieurs noms de domaine, l'AFNIC procède à la transmission du nom de domaine à la société bénéficiaire du transfert à la condition de recevoir de sa part :

- Le procès verbal de l'assemblée générale extraordinaire décidant de la liquidation ;

- Le rapport du liquidateur portant transfert du ou des noms domaine, s'il existe un.

3.7. Relations entre société mère et filiale

37. Le terme « société mère » s'entend d'une société possédant plus de la moitié du capital d'une autre société ; celui de « filiale » s'entend d'une société dont plus de la moitié du capital est possédée par une autre société conformément à l'article L 233-1 du Code de commerce.

38. Lorsqu'une demande de transmission de nom de domaine est effectuée dans le cadre des relations entre une société mère et sa filiale, l'organe dirigeant de la société mère ou de la filiale doit joindre à sa demande :

- Tout document justifiant cette transmission,

- Une attestation du commissaire aux comptes ou, le cas échéant, l'attestation d'un expert comptable certifiant l'existence d'un lien entre « société mère » - « société filiale »,

- La lettre d'acceptation selon le modèle type de l'AFNIC accessible ici signée par l'organisme demandeur initial confirmant son acceptation ou tout autre document attestant de l'acceptation de l'ancien organisme demandeur (ex : PV) sous réserve de la transmission et la réalisation de toutes les démarches préalables à l'égard des tiers (notamment à l'égard du prestataire Internet d'origine).

3.8. Cession de marque

39. En cas de cession d'une marque régulièrement déposée, le nom de domaine est supprimé sauf demande expresse du cédant et du concessionnaire visant à bénéficier d'une procédure de transmission.

40. Dans cette hypothèse, il revient à la partie la plus diligente de communiquer à l'AFNIC via son prestataire Internet :

- L'État des inscriptions au Registre national des marques mentionnant la cession de la marque ;

- La lettre d'acceptation selon le modèle type de l'AFNIC accessible ici signée par l'organisme demandeur initial confirmant son acceptation ou tout autre document attestant de l'acceptation de l'ancien organisme demandeur (ex : PV) sous réserve de la transmission et la réalisation de toutes les démarches préalables à l'égard des tiers (notamment à l'égard du prestataire Internet d'origine).

3.9. Procédures collectives

41. Dans l'hypothèse ou l'organisme demandeur serait affecté d'une procédure collective, l'AFNIC procède à la transmission du nom de domaine telle qu'ordonnée par les autorités judiciaires compétentes.

3.10. Décisions judiciaires

42. L'AFNIC procèdera à tout acte d'administration ordonné par une décision judiciaire, dans les termes de ladite décision, et ce dans les conditions suivantes :

- lorsque l'ensemble des parties à l'instance convient d'exécuter la décision de justice et en informe l'AFNIC par lettre recommandée avec avis de réception, ou
- après signification à l'AFNIC par huissier de justice, par la partie la plus diligente, d'une décision de justice bénéficiant de l'exécution provisoire de plein droit en application de l'article 514 du nouveau Code de procédure civile et justification de la notification à partie de cette décision, ou
- après signification à l'AFNIC par huissier de justice, par la partie la plus diligente, d'une décision de justice assortie de l'exécution provisoire au sens de l'article 515 du nouveau Code de procédure civile et justification de la notification à partie de cette décision et sur présentation de la justification de l'éventuelle constitution de garantie ordonnée par le Juge en application de l'article 517 du nouveau Code de procédure civile, ou
- après signification à l'AFNIC par huissier de justice, par la partie la plus diligente, d'une décision de justice investie de la force de la chose jugée au sens de l'article 500 du nouveau Code de procédure civile dont il sera justifié. Cette justification pourra par exemple être constituée, selon les cas, soit par la communication d'un certificat de non-recours, soit par la communication de l'arrêt d'appel.

43. Dans l'hypothèse où une décision de justice serait réformée, l'AFNIC procèdera dans les mêmes conditions à la mise en œuvre des nouveaux actes administratifs ordonnés.

44. L'AFNIC ne pourra donner suite à des demandes qui ne respecteraient pas ces conditions et ne saurait être tenue, par exemple, par l'envoi de lettre ou d'assignation.

45. Les actes d'administration pris par l'AFNIC en application d'une décision de justice ne sauraient engager l'AFNIC pour quelque motif que ce soit, l'organisme demandeur garantissant l'AFNIC contre tout recours.

46. L'organisme demandeur doit, dans un délai maximum d'un mois, fournir à l'AFNIC par l'intermédiaire du prestataire Internet, les justificatifs exigés par la Charte de nommage. A défaut, l'usage du nom de domaine par l'organisme demandeur peut être suspendu jusqu'à régularisation. Si la régularisation n'intervient pas au maximum dans un délai de 6 mois passé la date de suspension du nom de domaine, celui-ci retombe dans le domaine public. Dans l'hypothèse où une personne condamnée à transférer un nom de domaine souhaite réaliser ce transfert

en urgence, et sans attendre que le bénéficiaire puisse remettre à l'AFNIC via son prestataire sa demande de création (notamment dans le cadre d'une obligation conditionnée par une astreinte), l'AFNIC procède à un blocage du nom de domaine c'est à dire que le nom de domaine ne peut plus subir de modification. Il appartient à l'organisme demandeur bénéficiaire de la décision de fournir à l'AFNIC, dans le délai sus-visé de régulariser son dossier faute de quoi le nom de domaine retombe dans le domaine public passé un délai de 6 mois.

47. Les frais techniques et administratifs liés à la transmission incombent à l'organisme demandeur, à charge pour lui, en tant que de besoin, d'en obtenir le remboursement par l'une ou l'autre des parties à l'instance.

4. Cession d'un nom de domaine

48. L'exploitation d'un nom de domaine de la zone « .fr » repose sur un droit d'usage. En conséquence, la cession d'un nom de domaine sous quelque forme que ce soit, à titre gratuit ou onéreux, n'est pas opposable à l'AFNIC.

49. En conséquence, toute opération de suppression/re-création d'un nom de domaine, est réalisée aux risques et périls des organismes demandeurs. Il est rappelé, en effet, que dès lors qu'un nom de domaine est supprimé celui-ci retombe dans le domaine public et peut donc à tout moment être ré-attribué à n'importe quel autre organisme demandeur justifiant du respect de la présente Charte de nommage.

5. Changement de prestataire

50. L'organisme demandeur peut, sous réserve des accords conclus avec son prestataire Internet, demander un changement de prestataire qui consiste en un transfert technique du nom de domaine d'un prestataire Internet vers un autre prestataire Internet.

51. Pour ce faire, il appartient :

- A l'organisme demandeur de prendre toutes mesures à l'égard de ses prestataires Internet pour qu'ils procèdent au changement de prestataires ;

- Aux prestataires Internet intéressés par le changement de prestataire de procéder au mieux des intérêts de l'organisme demandeur.

52. Le prestataire bénéficiant du changement de prestataire doit veiller à ce que cette modification d'ordre technique n'affecte en rien la titularité administrative du nom de domaine.

53. La procédure et les délais relatifs au changement de prestataire sont détaillés dans l'annexe « Guide des procédures ».

6. Suppression du nom de domaine

54. A tout moment, l'organisme demandeur, par l'intermédiaire du prestataire Internet peut demander la suppression du nom de domaine. Cette demande est irréversible et ne nécessite aucun justificatif.

55. Dans l'intérêt des organismes demandeurs et afin d'éviter tout dysfonctionnement et tout litige, la demande de suppression d'un nom de domaine par un tiers, n'est pas acceptée. En revanche dans le cas où le nom de domaine aurait déjà fait l'objet d'une transmission, le nouveau titulaire peut demander la suppression de ce nom de domaine.

56. Tout nom de domaine supprimé peut être recréé au bénéfice d'un organisme demandeur dans respect de la présente Charte.

7. Noms de domaine orphelins

57. En cas de cessation d'activité du prestataire Internet pour quelque cause que ce soit (procédure collective, arrêt de l'activité, résiliation de la convention d'adhésion...), il appartient à ce dernier d'aviser ses clients de la nécessité de faire appel à un nouveau prestataire pour la gestion de leur nom de domaine.

58. A défaut pour le prestataire de s'être exécuté, l'AFNIC adresse directement aux organismes demandeurs un courrier RAR pour les informer qu'ils doivent choisir un nouveau prestataire dans un délai maximum d'un mois [(1)] à compter de la réception de ladite lettre.

59. A défaut de changement de prestataire dans le délai imparti, l'AFNIC procède à la suppression du nom de domaine orphelin correspondant qui peut alors être réattribué à un nouvel Organisme demandeur.

60. Il appartient en tout état de cause aux prestataires Internet de gérer les risques liés aux noms de domaine orphelins.

61. Les prestataires Internet s'engagent à communiquer à l'AFNIC tout changement de coordonnées des organismes demandeurs.

62. En application de cet article, les organismes demandeurs sont invités à vérifier que l'AFNIC dispose en permanence d'informations exactes permettant de les contacter directement.

---

(1) La remise ou non de la lettre d'engagement est fonction de l'option retenue par le prestataire dans le cadre de la convention signée avec l'AFNIC.

LISTE DES PERSONNES AUDITIONNÉES PAR LE RAPPORTEUR POUR AVIS

— Mme Aline PEYRONNET, sous-directrice à la sous-direction C, en charge de la protection du consommateur à la direction générale de la concurrence, de la consommation et de la répression des fraudes, ministère de l'Économie et des finances, accompagnée de M. Jean-Luc DANIEL, administrateur civil.

— Mme Catherine CHAMBON, commissaire principale, directeur de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), ministère de l'Intérieur.

— Mmes Nadine BELLUROT et Catherine CHADELAT, conseillers techniques au cabinet de M. Dominique Perben, garde des Sceaux, ministre de la Justice, accompagnées de Mme Isabelle VENDRYES et de M. Gilles SORBA, des services de la Chancellerie.

— M. Jean-Christophe LETOQUIN, délégué permanent de l'Association des fournisseurs d'accès (AFA), accompagné de Mmes Véronique ETIENNE-MARTIN, conseiller auprès de la direction général de Microsoft France, et Sandrine MOLGATINI, chargée des relations extérieures de Worldcom, de MM. Stéphane MARCOVITCH, responsable juridique des portails de Wanadoo et Olivier de BAILLEUX, directeur délégué aux affaires extérieures de Noos, membres de l'AFA.

— M. Éric CAPRIOLI, avocat au barreau de Nice.

— M. Marc GUEZ, directeur général de la société civile des producteurs de phonogrammes, accompagné de M. Philippe JOGUET, consultant.

— M. Gilles BRÉGANT, secrétaire général de la mission pour l'économie numérique et M. Didier ÉTIENNE, chargé de mission sur les questions commerciales électroniques, ministère de l'Économie et des finances.

— M. Jérôme HUET, professeur de droit, directeur du centre d'études juridiques et économiques du multimédia, université de Paris II.

N°608 – Rapport de Mme Michèle Tabarot sur le projet de loi pour la confiance en l'économie numérique