



LE DROIT DE L'INFORMATIQUE, DES  
RESEAUX ET DES TECHNOLOGIES DE  
L'INFORMATION ET DE LA  
COMMUNICATION

---

AVRIL 2004

---

## Sommaire

La Loi sur l'Economie Numérique - 29/04/2004.....	2
Point de vue: Projet de loi sur la confiance dans l'économie numérique : le Sénat rectifie le tir. - 29/04/2004 .....	8
Comment prouver l'antériorité d'un droit d'auteur ? - 24/04/2004.....	12
L'Internet et la déontologie de l'avocat : quelles conciliations possibles ? (Seconde partie) - 19/04/2004 .....	16
L'Internet et la déontologie de l'avocat : quelles conciliations possibles ? (1ère partie) - 13/04/2004.....	21
Courriels et secret des correspondances privées. - 08/04/2004 .....	25
Données personnelles des passagers aériens : Le Parlement européen et la Commission en profond désaccord - 04/04/2004 .....	30
Données personnelles dans le secteur des communications électroniques : La Commission rappelle leurs obligations à huit Etats. - 02/04/2004 .....	37

---

## Commerce électronique, Thème transversal

---

### La Loi sur l'Economie Numérique -29/04/2004

*Par Me. Murielle-Isabelle Cahen, Avocate .*



Après l'Assemblée nationale, c'est au tour du Sénat d'avoir adopté, en 2ème lecture, le 8 avril dernier, le projet de loi sur l'économie numérique. Il ne manque plus que l'aval de la commission mixte paritaire (composée de députés et sénateurs) pour qu'il soit définitivement adopté.

▸ Avec ce projet de loi et conformément aux objectifs fixés par la Commission européenne, notamment la directive du 8 juin 2000 sur le commerce électronique (Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur) le gouvernement "souhaite tirer les enseignements des premières années d'ouverture à la concurrence du secteur des télécommunications et prendre en compte les importantes mutations intervenues ces dernières années dans les secteurs des télécommunications et de l'audiovisuel, afin de faciliter le développement de ces industries, de renforcer leur compétitivité, de consolider le service public, et d'offrir à nos concitoyens et à nos entreprises une gamme élargie de services".

Le projet de loi précisera la position technique des hébergeurs, en disposant dans la règle suivie pour tous les autres opérateurs de télécommunication, les cas précis où leur responsabilité pourra être engagée en cas de litige. Ces précisions marquent la volonté du Gouvernement de limiter la mise en cause abusive de ces professionnels, et d'identifier les auteurs réels des contenus illégaux et autres responsables éditoriaux susceptibles de poursuite.

La question de la responsabilité des intermédiaires techniques sur Internet est enfin traitée, dans une rédaction proche de la directive commerce électronique. Cette dernière pose deux principes essentiels :

- l'absence d'obligation générale de surveillance des contenus et de recherche active des activités illicites, et
- l'absence de responsabilité en cas de neutralité vis-à-vis du contenu et, le cas échéant, d'intervention prompte dès que l'intermédiaire a connaissance du caractère illicite ou préjudiciable d'un contenu.

Le projet de loi reprend l'idée de neutralité en prévoyant que « Les prestataires techniques [...] 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. »

Ces principes sont ensuite déclinés en fonction des spécificités des prestataires concernés: fournisseurs d'hébergement, opérateurs télécoms et fournisseurs d'accès à Internet.

La LEN ne contient aucune disposition traitant spécifiquement de la responsabilité des fournisseurs d'accès. Ceux-ci sont englobés avec les opérateurs de télécommunications dans le nouvel article L. 32-3-3 du Code des Postes et Télécommunications introduit par la LEN qui dispose que : "Toute personne assurant une activité de transmission de contenus sur un réseau de télécommunications ou de fourniture d'accès à un réseau de télécommunications ne peut voir sa responsabilité civile ou pénale engagée à raison de ces contenus que dans les cas où soit elle est à l'origine de la demande de transmission litigieuse, soit elle sélectionne le destinataire de la transmission, soit elle sélectionne ou modifie les contenus faisant l'objet de la transmission."

En ce qui concerne le régime des hébergeurs, la loi reprend assez strictement les dispositions de la directive commerce électronique. Il n'en est pas moins critiqué, car susceptible de mettre à la charge des prestataires d'hébergement une obligation de qualification des contenus, c'est à dire des informations qu'ils hébergent. En effet, techniquement, quand un tiers prétend subir un préjudice du fait d'un tel contenu, il peut s'adresser soit aux juridictions, soit directement au prestataire d'hébergement. Si la juridiction constate le caractère illicite ou préjudiciable d'un contenu déterminé, elle informe le prestataire et lui ordonne de procéder au retrait ou à la suppression du contenu.

Le prestataire est amené à analyser le contenu afin de pouvoir, s'il estime la demande du tiers fondée, retirer ou supprimer le contenu. Il est alors susceptible d'engager sa responsabilité s'il procède indûment au retrait (manquement contractuel) et/ou s'il ne procède pas au retrait alors que le contenu porte effectivement atteinte au tiers concerné. Par conséquent dans cette hypothèse, en cas de demande émanant d'un tiers qui estime subir un préjudice du fait de l'existence et de la disponibilité du contenu, la détermination de la nature illicite ou préjudiciable du contenu appartient en premier ressort à l'intermédiaire. Le risque de voir sa responsabilité engagée (notamment sur le plan pénal) s'il ne se conforme pas aux demandes du tiers pourrait inciter le prestataire à systématiquement retirer ou supprimer tout contenu visé. En matière de connaissance des faits litigieux, le prestataire technique est présumé avoir eu connaissance de ces faits dès lors un certain nombre d'information lui auront été communiquées (date, identité du notifiant, identité du destinataire, description des faits litigieux et leur localisation, motifs du retrait, mention des dispositions légales et copie de la correspondance adressée à l'auteur ou l'éditeur des informations litigieuses).

Les Articles 43-8 et 43-9, modifiés par le Sénat, prévoient l'engagement de la

responsabilité civile ou pénale des hébergeurs si ces derniers avaient « effectivement connaissance du caractère illicite des activités ou informations stockées à la demande du destinataire du service » ou si ils en avaient connaissance mais n'ont pas « agi promptement pour retirer ces données ou en rendre l'accès impossible ». Un nouvel alinéa prévoit que la disposition précédente ne s'applique pas lorsque les contenus ont été créés par une personne agissant sous l'autorité et le contrôle du prestataire technique.

Par ailleurs, soucieux peut-être de préserver les fournisseurs d'hébergement d'un flot incontrôlable de réclamations, les Sénateurs ont eu l'idée d'introduire un nouvel article 43-9-1 A au projet de loi créant une nouvelle infraction pénale rédigée en ces termes : "Le fait, pour toute personne, de présenter aux personnes mentionnées à l'article 43-8, un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est punie d'une peine d'un an d'emprisonnement et de 15 000 € d'amende". Cet article a été maintenu lors du vote des sénateurs en deuxième lecture.

L'article 43-12 quant à lui, prévoit que l'autorité judiciaire peut demander aux fournisseurs d'accès et aux "hébergeurs" de supprimer un contenu s'il est hébergé en France, et de le filtrer s'il est situé à l'étranger. Si la suppression d'un contenu hébergé en France ne pose aucun problème particulier, il n'en va pas de même pour le filtrage des contenus hébergés à l'étranger. Cette disposition a pourtant été entérinée par les Sénateurs en deuxième lecture.

Le futur article 43-11 de la loi de 1986, introduit par les Députés, et non modifié par les Sénateurs dispose que les fournisseurs d'hébergement "ne sont pas soumis à une obligation générale de surveiller les informations qu'ils stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites". Ce texte reprend l'article 15 de la directive sur le commerce électronique du 8 juin 2000 qui fait obligation aux Etats membres de ne pas imposer aux fournisseurs d'hébergement une telle obligation "générale" de surveillance.

Le texte de loi prévoyait l'obligation pour les hébergeurs d'empêcher l'accès aux sites Internet pédophiles, négationnistes et racistes, sans attendre une décision de justice. Un exercice qui aurait imposé aux exploitants de services communautaires sur Internet d'effectuer un contrôle au préalable des contenus - licites ou illicites - avant diffusion en ligne. Un dispositif de filtrage qui allait à l'encontre de la liberté d'expression et qui se révèle délicat d'un point de vue technique, avait estimé l'Association des fournisseurs d'accès et de services Internet (AFA).

En deuxième lecture, le Sénat est venu limiter ce point. En effet, un amendement a été adopté, avec l'appui du gouvernement, limitant l'obligation de filtrage des hébergeurs. L'obligation de surveillance a priori des hébergeurs est donc abandonnée. En revanche, sur saisine de l'autorité judiciaire, les hébergeurs seront obligés d'accepter un contrôle des sites Internet a posteriori. Le Sénat a précisé, par ailleurs, que l'absence d'obligation générale de surveillance est « sans préjudice de toute activité de surveillance ciblée et temporaire demandée par l'autorité judiciaire ». Le juge conserve donc la possibilité

d'imposer à l'hébergeur une mesure de surveillance généralisée.

Les Sénateurs entérinent, de plus, la disposition selon laquelle les fournisseurs d'hébergement sont responsables en cas d'hébergement de contenus illicites s'ils n'agissent pas avec "promptitude" pour interdire l'accès à ces informations "dès le moment où [ils] ont eu la connaissance effective de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère illicite". La conséquence importante de ce texte est qu'il ne sera pas possible pour un fournisseur d'hébergement de se voir reprocher la seule mise en ligne d'un contenu illicite. En effet, puisque l'hébergeur n'a pas une obligation générale de surveillance des contenus illicites (ce qui serait contraire à la Directive européenne relative au commerce électronique), il sera nécessaire que l'existence d'un tel contenu soit portée à son attention.

L'obligation du fournisseur d'hébergement n'est donc pas une obligation de surveillance mais une obligation de célérité. Ce n'est que le défaut de promptitude du fournisseur d'hébergement alerté qui pourra être sanctionné. Mais c'est sur le point de départ du délai "d'inaction" du fournisseur d'hébergement que se cristallisent les difficultés. Les reproches ne deviennent possibles à l'encontre de l'hébergeur qu'à partir du moment où celui-ci acquiert une "connaissance effective" du caractère illicite du site ou à connaissance de "faits et circonstances faisant apparaître ce caractère illicite". Les circonvolutions dans la formulation adoptée par les Députés, et à leur suite les Sénateurs, dissimulent mal l'embarras du législateur.

Le projet de loi modifié en deuxième lecture par les Sénateurs apporte, enfin, deux nouvelles dispositions :

- une charte de bonne conduite élaborée par les prestataires techniques est préconisée pour identifier au mieux les contenus illicites (transposition de la Directive européenne),
- le juge des référés ne peut désormais plus imposer aux intermédiaires des mesures allant jusqu'à la suppression du contenu manifestement illicite. Elle peut toutefois prescrire « toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne ».

En ce qui concerne le e-mail non confidentiel, le projet de loi transpose les dispositions de la directive européenne et prévoit :

- l'interdiction de la prospection directe (« au moyen d'un automate d'appel, d'un télécopieur et d'un courrier électronique, de toute personne physique qui n'a pas exprimé son consentement préalable à recevoir des prospections directes par ce moyen » (article 12 I. du projet LEN, modifiant les articles L. 33-4-1 du code des Postes et Télécommunications et L. 120-20-5 du code de la consommation), et
- par dérogation, la prospection directe par courrier électronique est autorisée si les coordonnées électroniques du destinataire ont été recueillies directement auprès de lui, dans le respect des dispositions de la loi de 78 (Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), à l'occasion d'une vente ou d'une prestation de service, si elle concerne des produits ou services analogues à ceux antérieurement fournis par la même personne, et si le destinataire se voit offrir, de manière expresse et dénuée d'ambiguïté, la possibilité de s'opposer, sans frais et de manière simple, à

L'utilisation de ses coordonnées électroniques lorsque celles-ci sont recueillies et chaque fois qu'un courrier électronique de prospection lui est adressé.

- dans tous les cas, « il est interdit d'émettre, à des fins de prospection directe, des messages au moyen d'automates d'appel, télécopieurs et courriers électroniques, sans indiquer des coordonnées valables auxquelles le destinataire puisse utilement transmettre une demande » afin d'obtenir la cessation, sans frais, de ces communications.

Concernant la prospection directe ou spam, un amendement du rapporteur a été adopté pour distinguer les courriers non sollicités provenant de personnes physiques et morales non inscrites au registre du commerce et des sociétés. Ceux-ci ne seraient plus soumis à l'opt-in, recueil du consentement préalable de l'internaute à recevoir des messages publicitaires. S'il est toujours bon d'établir une distinction entre sociétés commerciales et acteurs non commerciaux, on peut légitimement se demander s'il n'était pas plus pertinent d'opérer une distinction sur le type de courrier non sollicité (par exemple : commercial par opposition à non commercial ou publicitaire par opposition à informatif) plutôt que sur le statut de l'expéditeur. En effet, le fait que l'expéditeur ne soit pas inscrit au registre du commerce n'implique pas forcément que les spams envoyés ne seront pas, eux, d'ordre commercial.

Le dernier groupe d'amendements adoptés renforce en revanche la lutte contre le spam, puisqu'il restreint le recours à l'opt-out prévu à titre dérogatoire par l'article 12 du projet de LEN. Il s'agit des cas de prospection directe de destinataires dont les coordonnées électroniques ont été recueillies préalablement dans le cadre d'une vente de « produits et services analogues ».

En son article 12, le texte propose, sur la question du spamming, un compromis relativement équilibré mais probablement difficile à mettre en oeuvre. Il a en tous cas le mérite de poser frontalement une question aux ramifications multiples.

L'enjeu est de taille, puisque le Code pénal prévoit, notamment : article 226-16 « Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de trois ans d'emprisonnement et de 45 000 euros d'amende. »

L'article 226-18 : "Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique malgré l'opposition de cette personne, lorsque cette opposition est fondée sur des raisons légitimes, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

De manière apparemment délibérée, aucune référence n'est faite à une définition du spamming ou de la notion de nuisance :

- ni quant aux modalités d'envoi de l'e-mail : Le texte ne différencie pas emails "manuels" et recours à un automate, (le terme d'"automate" n'est employé que

concernant les appels téléphoniques) et ne fait pas référence à la quantité d'emails envoyés. On ne voit pas l'intérêt de telles distinctions sauf à pouvoir invoquer l'article 226-16 du Code pénal, déjà mentionné, qui vise les "traitements automatisés".

- ni quant à la teneur du mail lui-même : Le projet élude totalement la question, mettant à la même enseigne les emails à caractère pornographique ou agressif, ceux induisant une escroquerie ou un virus, et les publicités honnêtes, alors que cette dernière catégorie peut être considérée au nombre des victimes des précédentes.

La question essentielle est pourtant bien de placer la frontière entre e-mailing et spamming, sauf à vouloir s'attaquer à la notion d'"email" en tant que tel, ce qui, d'évidence, n'est pas l'intention des auteurs du texte de la loi.

En conclusion on peut noter que l'une des difficultés de ce début de siècle sera d'élaborer des systèmes juridiques adaptés au contexte de disciplines au potentiel mal cerné mais influant profondément, et très rapidement, sur la mouvance sociale.

**Par Me. Murielle-Isabelle Cahen, Avocate .**

---

## Commerce électronique, Thème transversal

---

### **Point de vue: Projet de loi sur la confiance dans l'économie numérique : le Sénat rectifie le tir. -29/04/2004**

*Par M. Guillaume Bigot, Juriste LAMY .*



C'est dans la nuit du 8 au 9 avril que les sénateurs ont adopté, en seconde lecture, le projet de loi LEN. La controversée obligation de surveillance a priori des contenus par les hébergeurs, décidée par l'assemblée nationale, a été supprimée.

#### La responsabilité des hébergeurs

Ainsi, c'est sans surprise que le Sénat a enterré la mesure d'obligation de surveillance générale du Web. Sous couvert de lutte contre la pédophilie et les messages à caractère haineux, il était en effet demandé aux hébergeurs de surveiller tout ce qui devait être publié, sous peine d'engager leur responsabilité civile et pénale. On se souvient que cet article avait fait bondir ces derniers, qui avaient alors menacé de fermer tous les sites d'hébergement de pages personnelles. L'Ancienne ministre déléguée de l'Industrie, Nicole Fontaine, avait donc fait machine arrière. En outre, plus récemment, la Commission des affaires économiques du Sénat a jugé cette disposition disproportionnée et contraire à la Directive européenne sur le commerce électronique. De fait, l'Association des Fournisseurs d'Accès (AFA) se félicite de cette nouvelle version du texte.

Néanmoins, les amendements déposés en vue de reconnaître au seul juge le droit de juger du caractère illicite d'un site ont été rejetés. Pour Patrick Devedjian, nouveau ministre délégué à l'Industrie et rapporteur du texte, *« il n'est pas dans l'esprit de la directive de soumettre tous les cas litigieux à la justice. Avant qu'elle se prononce, les délais seraient considérables et il est hors de question de laisser consulter pendant des mois ou des années des sites litigieux. »*. De fait, la procédure de *notification*, élaborée par les députés, reste d'actualité. Un amendement la rend même obligatoire. Concrètement, les fournisseurs d'accès Internet et hébergeurs seront présumés avoir eu connaissance de faits litigieux sur simple notification par un internaute et dans des conditions détaillées par la LEN. Ceux-ci auront alors le choix de supprimer ou non le site, sans passer par la case Tribunal. On comprend, dès lors, la menace que pourrait constituer un tel système sur la liberté d'expression et certaines voix dénoncent d'ores et déjà une justice privée. Pour M. Devedjian, au contraire, *« le système retenu ne transforme nullement l'hébergeur en juge, au contraire. Il oblige à notifier avant de saisir le juge »*.

Pourtant, il n'est pas interdit de penser que les hébergeurs pourraient être tentés de

censurer l'ensemble des sites ainsi dénoncés. Or, certains faits « litigieux », au sens figuré du terme, ne sauraient être jugés que par... des juges. Nous pensons notamment aux affaires de diffamation ou de contrefaçon de logos pour des causes consuméristes ou écologistes. Là où les tribunaux peuvent se montrer cléments, les hébergeurs prendront-ils le risque de voir leur responsabilité engagée ? Rien n'est moins sûr.

Le système judiciaire n'est toutefois, fort heureusement, pas absent du projet de loi. Le juge des référés est ainsi invité à faire prévenir ou faire cesser un dommage en demandant l'interdiction d'accès, pour les internautes français, à un site illicite. Mais les sénateurs ont supprimé la référence aux mesures propres à faire cesser un dommage. Les députés avaient en effet admis que le juge des référés pouvait ordonner aux intermédiaires de prendre toutes mesures « *visant à cesser de stocker ce contenu d'un service de communication publique en ligne* ». Cette suppression inquiète particulièrement l'industrie du disque. Rien ne semble pourtant indiquer une remise en question des pouvoirs de droit commun du juge en la matière.

## **Le régime juridique du courrier électronique.**

Durant les débats devant l'Assemblée nationale, une polémique était née quant au caractère de correspondance privée du courriel. La Commission des affaires économique de l'Assemblée avait, dans un premier temps, reconnu la notion avant de la supprimer. Aux yeux de la Commission, créer un régime spécifique au courrier électronique aurait rendu plus difficile la lutte contre les courriers indésirables et aurait été contraire à la lettre de la Directive qui exigeait expressément de ne pas étendre la notion de correspondance privée. Certaines associations avaient alors dénoncé le risque d'atteinte à la vie privée. On comptait donc sur les sénateurs pour clarifier la situation. Raté ! Ces derniers n'ont pas touché au texte.

On remarquera cependant que le courrier électronique est régi par la loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, qui en garantit le secret. De même l'article 226-15 al 2 du code pénal punit d'un an d'emprisonnement et de 45 000 euros d'amende la violation de correspondances émises ou reçues par la voie des télécommunications. Une telle précision dans la future loi sur la confiance dans l'économie numérique ne s'imposait donc effectivement pas. (Pour approfondir voir : J.Le Clainche, « Courriels et secret des correspondances privées », 8 avril 2004, [DROIT-TIC.com](http://DROIT-TIC.com), consulté le 22 avril 2004).

## **Le nouveau régime de la diffamation**

La prescription de la diffamation sur Internet pose problème depuis déjà quelque temps. A plusieurs reprises, la cour de cassation avait considéré qu'à l'instar de la presse traditionnelle, le délit de diffamation sur le web devait être prescrit trois mois après sa première mise en ligne. Certains s'étaient alors inquiétés du fait qu'une personne pouvait parfaitement publier un texte sur Internet et ne le rendre véritablement accessible au

public que passé ce délai de prescription. Le sénateur René Trégoüet pensait certainement mettre tout le monde d'accord en déposant un amendement par lequel le délit de diffamation sur Internet devait être prescrit trois mois après avoir retiré l'article ou le message incriminé.

Erreur ! Cette fois, c'est Reporter Sans Frontière qui monte au créneau, dénonçant une responsabilité « *à vie des contenus publiés en ligne* ». Citant Lionel Thoumyre, juriste au Forum des droits sur l'Internet, l'organisation observe que « *le problème de la résurgence de certains contenus aurait tout aussi bien pu être traité par la jurisprudence* ». Le juge pourrait parfaitement considérer que la date de publication d'un écrit, au sens de la loi, est celle de sa mise à disposition du public et non celle de sa mise en ligne.

Il est toutefois malaisé de dissocier date de publication et mise à disposition d'un message, notamment sur Internet. Que penser, par exemple, d'un site accessible mais difficile à trouver par l'intermédiaire d'un moteur de recherche ? Le meilleur point de départ serait très certainement la date effective de la connaissance de l'écrit par la victime. Mais aussi sûrement serait-il difficile d'en apporter la preuve. De fait, la jurisprudence se montre souvent très sourcilleuse quand il s'agit de juger un écrit diffamant. Le meilleur moyen pour éviter une condamnation restant encore de ne pas l'écrire.

## **Le commerce électronique.**

Dans un souci de protection du consommateur, les députés avaient fait peser l'entière responsabilité de la bonne exécution du contrat en ligne sur les seules épaules du vendeur, que « *ces obligations soient à effectuer par lui-même ou par d'autres prestataires de services* ». L'intention est louable et doit bien évidemment être saluée. Il s'agissait de rompre avec les situations où vendeur, fournisseur et société de livraison se renvoyaient la balle suite à la non-exécution du contrat. Les sénateurs sont toutefois revenus sur ce point, avec une version plus indulgente puisque le vendeur peut désormais « *s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable soit à l'acheteur* », soit à la force majeure.

Toujours en la matière, les sénateurs ont validé le principe du « double-clic » pour la conclusion du contrat électronique. Par dérogation au principe du consensualisme, et pour protéger le consommateur, le nouvel article 1369-2 du code civil stipule que ce dernier « *doit avoir eu la possibilité de vérifier le détail de sa commande et son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation* ».

## **La lutte contre le piratage**

Afin de protéger les droits de propriété intellectuelle, les services Internet proposant le

téléchargement d'œuvres protégées devront désormais afficher « *une mention facilement identifiable et lisible rappelant que le piratage nuit à la création artistique* ». Tremblez Pirates !

A moins d'un inattendu retournement de situation, le texte voté par le Sénat devrait être très proche de la future loi pour la confiance dans l'économie numérique. Il appartient désormais à la commission mixte paritaire, composée de 14 députés et sénateurs, d'établir la version définitive du texte.

**Par M. Guillaume Bigot, Juriste LAMY .**

---

## Propriétés intellectuelles, Droit d'auteur

---

### Comment prouver l'antériorité d'un droit d'auteur ? - 24/04/2004

*Par Me. Murielle-Isabelle Cahen, Avocate .*



**Lorsqu'il y a conflit sur l'existence d'un droit, la question principale qui se pose est de savoir qui a la charge de la preuve.**

► Lorsqu'il y a conflit sur l'existence d'un droit, la question principale qui se pose est de savoir qui a la charge de la preuve. Il existe un principe fondamental du droit selon lequel c'est à celui qui invoque l'existence ou l'absence d'un droit de le prouver : "actori incombis probatio". Dans certaines hypothèses, la loi a admis l'existence de présomptions légales (l'admission d'un fait par la loi à partir d'un autre fait qui fait présumer l'existence du premier). Il y a alors renversement de la charge de la preuve. Il appartiendra au défendeur de prouver le contraire de ce qui est admis par la présomption.

Le droit français fait une très large place à la prévention, en matière civile. La loi a prévu une présomption de la qualité d'auteur (art. L 113-1). La qualité d'auteur appartient sauf preuves contraires à celui ou ceux sous le nom de qui l'œuvre est divulguée. Cette présomption peut être invoquée par tous les autres auteurs dont le nom a été porté à la connaissance du public d'une manière quelconque. Elle peut être combattue par tout moyens. La preuve de la qualité d'auteur est libre, les juges peuvent tenir compte de toutes présomptions. En jurisprudence, la qualité d'auteur est caractérisée par un apport spécifique de création intellectuelle qui ne se conçoit pas sans une forme matérialisée.

Le droit d'auteur désigne l'ensemble des droits dont jouissent les créateurs sur leurs oeuvres littéraires et artistiques. En droit français, l'œuvre est protégée du seul fait de sa création. L'article L.111-1 du CPI dispose "l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous".

Le mot "œuvre" étant un terme juridiquement assez faible, il y a très peu de cas où cette qualité a été refusée en jurisprudence. Les oeuvres protégées par le droit d'auteur comprennent notamment les oeuvres littéraires (romans, poèmes, pièces de théâtre,

ouvrages de référence, journaux et logiciels), les bases de données, les films, les compositions musicales et chorégraphiques, les oeuvres artistiques telles que les peintures, dessins, photographies et sculptures, architecture, et les créations publicitaires, cartes géographiques et dessins techniques. Dès lors que l'oeuvre est mise en forme, son originalité est présumée. Le problème va se poser en terme de preuve : qui a l'antériorité de la création de l'oeuvre ?

En théorie, il n'y a donc aucune formalité à remplir pour faire valoir ses droits. En pratique, il est essentiel de déposer l'oeuvre pour pouvoir, en cas de litige, faire la preuve de son antériorité. Le dépôt offre l'avantage d'apporter une date certaine. En effet, le dépôt donne la preuve qu'à la date où il a été effectué, le déposant était en possession de l'oeuvre, objet du dépôt. Il permet en cas de conflit de faire jouer une antériorité de création devant un juge et aide à démontrer qu'un tiers a divulgué l'oeuvre sans autorisation.

Toutefois, certaines oeuvres sont soumises au dépôt légal, tant pour constituer et enrichir un patrimoine culturel, pour assurer l'information de certaines autorités administratives que pour offrir à l'auteur lui-même un moyen de preuve d'antériorité. Le régime du dépôt légal est organisé par la loi 92-546 du 20.6.92 et le décret 93-1429 du 31.12.93. Il est applicable aux documents imprimés, graphiques, photographiques, sonores, audiovisuels, multimédia, quel que soit leur procédé technique de production, d'édition et de diffusion, dès lors qu'ils sont mis à la disposition du public. L'obligation du dépôt légal incombe aux personnes physiques et morales qui éditent, produisent ou importent les documents visés. On est en présence d'un dépôt administratif, obligatoire, à la bibliothèque nationale, au centre national de la cinématographie ou à l'institut national de l'audiovisuel et concerne " tous documents " « dès lors qu'ils sont mis à la disposition d'un public ». Pour les oeuvres cinématographiques et audiovisuelles, il existe un registre spécial, le registre public de la cinématographie et de l'audiovisuel qui avait été initialement créé par une loi du 22 février 1944.

Pour protéger son droit il est indispensable de mettre en place une procédure visant à conserver des preuves matérielles de l'antériorité de la marque, de la création ou des modèles : enregistrement des dates de création par voie d'huissier, conservation des documents datés liés à l'objet à protéger (factures, extraits de presse, correspondance commerciale, etc.).

Ce dépôt permet d'avoir la date précise de la création de l'oeuvre. Les dépôts les plus utilisés sont.:

1. Le dépôt auprès d'une société d'auteur (Société des Compositeurs et des Auteurs Multimédias, Société des Auteurs Compositeurs Dramatiques, Société Nationale des Auteurs Compositeurs). Aucune société d'auteurs n'est pas investie d'un pouvoir d'apporter "preuve certaine" au même titre qu'un officier ministériel (huissier ou notaire). C'est en fait un service que rendent les sociétés d'auteurs à leurs membres (ou non membres). Mais sur un plan juridique il s'agit d'une preuve simple, tout aussi contestable en cas de litige devant un juge que toute autre. Elle n'a aucune force supérieure.

L'intérêt de ces dépôts, réside en ce que l'on peut déposer des documents parfois volumineux. En cas de dépôt d'œuvres de collaboration, il convient de bien mentionner tous les auteurs, et de préciser que le manuscrit ne pourra être retiré que par une démarche conjointe des coauteurs, ceci afin d'éviter que l'un des coauteurs ne retire seul le dépôt et supprime ainsi la preuve de la collaboration.

2. Dépôt auprès d'un notaire ou huissier. Ce mode de dépôt est possible, mais il a l'inconvénient d'être onéreux.

3. L'envoi à soi même d'un courrier recommandé cacheté. Il s'agit d'envoyer à des personnes de confiance et/ou à soi-même par la poste et en objet recommandé un exemplaire de l'œuvre créée. Il convient à sa réception de ne pas ouvrir l'enveloppe. En cas de contestation de paternité (c'est-à-dire dans la plupart des cas, d'antériorité de preuve) on fera ouvrir l'enveloppe restée inviolée devant huissier. La date de la poste faisant foi, sauf à prouver une complicité avec un agent des postes, cette preuve acquiert date quasi-certaine.

4. Le système de l'enveloppe Soleau. Il est fondé sur le décret du 10 mars 1914 et avait pour but à l'origine, d'établir la date de création de dessins et modèles, selon la loi du 14 juillet 1909 et l'arrêté du 9 mai 1986. Mais, rapidement, les inventeurs l'ont utilisée pour établir la date certaine de conception de leur invention en attendant qu'elle soit suffisamment au point pour permettre le dépôt d'un brevet. L'enveloppe Soleau est envoyée par poste à l'Institut National de la Propriété Industrielle (INPI). Il s'agit d'un mécanisme pratique, peu onéreux et qui a l'avantage d'offrir une garantie étatique au dépôt, dans la mesure où il consiste en un dépôt géré par l'INPI.

Il est effectué au moyen d'une enveloppe double que l'on achète à l'INPI, ou auprès des greffes des tribunaux de commerce. On insère dans chacun des volets de l'enveloppe le document que l'on entend protéger (maximum de 7 pages) et on l'envoie à l'INPI par la poste en recommandé avec accusé de réception. L'enveloppe est perforée à son arrivée à l'INPI, et se voit octroyer un numéro d'ordre. L'un des volets est renvoyé au déposant, l'autre est conservé par l'INPI pendant une période de cinq années, qui peut être prorogée.

En cas de problème, le volet conservé à l'INPI est transmis au juge chargé de statuer sur le conflit. L'INPI renvoie un des volets au demandeur et conserve l'autre pendant 5 ans, renouvelables une fois par paiement d'une nouvelle taxe de 10 €. Après 10 ans, le premier volet est restitué au demandeur qui doit le conserver intact (de même que le second volet), car sa valeur de preuve serait encore acceptable par un Tribunal en cas de litige.

L'ensemble de ces droits est codifié en France dans le Code de la Propriété Intellectuelle (partie législative: loi 92-597 du 1.7.92, partie réglementaire: décret 95-385 du 10.4.95) qui abroge et remplace les lois du 11.3.57 et du 3.7.85.

Les autres méthodes utilisées par des auteurs pour prouver l'antériorité de leur œuvre sont :

- le visa des documents par la Gendarmerie ou le Commissariat de Police ;
- la gravure sur CD-ROM ou DVD-ROM non-réenregistrable ;
- l'enregistrement à date certaine de microfilms ou microfiches par les services de l'Enregistrement de la D.G.I. (Direction Gén. des Impôts) et
- une demande de brevet déposée puis retirée avant publication, conservée en archives à l'I.N.P.I., (normalement pendant 25 ans).

**Par Me. Murielle-Isabelle Cahen, Avocate .**

---

## Commerce électronique, Informatique juridique

---

### L'Internet et la déontologie de l'avocat : quelles conciliations possibles ? (Seconde partie) -19/04/2004

*Par Me. Héloïse Comte, Avocate stagiaire .*



L'avocat du 21<sup>e</sup> siècle, connecté, est confronté à une problématique spécifique de sécurisation de ses échanges par Internet.

#### ► Partie II : la sécurisation des échanges par Internet

L'avocat du 21<sup>e</sup> siècle, connecté, est confronté à une problématique spécifique de sécurisation de ses échanges par Internet.

L'avocat est en effet soumis aux règles déontologiques de son Ordre qui font sa spécificité et qui constituent autant de garanties pour ses clients.

Tout d'abord, il doit respecter rigoureusement le secret professionnel, principe général et absolu d'ordre public. Cela signifie qu'il doit être à même de garantir la destination des documents qu'il envoie par Internet.

Ensuite, il doit impérativement garantir l'intégrité des correspondances et documents de preuve qu'il communique par Internet.

En dehors des problèmes généraux de sécurité qui se posent à tout émetteur et récepteur de message via Internet, l'avocat, garant de la confidentialité et de la sécurité des messages qu'il expédie via Internet, est donc soumis aux exigences d'une sécurité renforcée.

Le Règlement Intérieur Harmonisé (RIH) des Barreaux, élaboré par le Conseil National des Barreaux (CNB), tente de répondre à cette problématique en précisant l'étendue des règles déontologiques pesant sur l'avocat qui souhaite utiliser Internet et le système de messagerie électronique au service de sa profession.

Notamment, par deux délibérations d'Assemblée Générale en date des 5 avril et 28 juin 2003, le CNB pose sans équivoque les règles s'imposant à l'avocat connecté.

Nous verrons dans un premier temps quelles sont les règles déontologiques pesant sur l'avocat qui souhaite se servir d'Internet comme d'un outil de communication.

Nous verrons ensuite quels sont les moyens technologiques offerts pour garantir la sécurité générale des messages sur Internet.

## I - Sur l'étendue des exigences d'ordre déontologique pesant sur l'avocat connecté

Les préoccupations de l'avocat connecté sont essentiellement de deux ordres : garantir le secret professionnel d'une part, garantir l'intégrité des documents qu'il communique par Internet d'autre part.

### Le secret professionnel

L'article 2.2 du RIH, qui précise la portée du principe, dispose que « *le secret professionnel couvre toutes matières, que ce soit dans le domaine du conseil comme dans celui de la défense, et quels qu'en soient les supports matériels ou immatériels (papier, télécopie, voie électronique...)* ».

De même, selon l'article 3.1 du RIH, « *tous échanges entre avocats, verbaux ou écrits quel qu'en soit le support (papier, télécopie, voie électronique...) sont par nature confidentiels* ».

Les messages et documents produits par l'avocat (correspondances, consultations...) sont ainsi indifféremment soumis au secret professionnel.

Par ailleurs, les articles 6.6 et suivants du RIH organisent la manière dont l'avocat peut donner des consultations en ligne et s'en faire rémunérer.

L'article 6.6.2 du RIH dispose que « *lorsqu'un avocat est interrogé ou sollicité en ligne par une personne demandant des prestations juridiques, il lui appartient de s'assurer de l'identité et des caractéristiques de la personne à laquelle il répond, afin de respecter le secret professionnel, d'éviter le conflit d'intérêts et de fournir des informations adaptées à la situation de l'interrogateur. L'avocat qui répond doit toujours être identifiable.* »

Il en résulte que l'avocat peut parfaitement travailler en ligne, recevoir des demandes de consultation et en donner. Cependant, il doit au préalable identifier son correspondant par le procédé de son choix (courrier, téléphone, rendez-vous...). Le texte impose également à l'avocat de s'identifier, ce qui revient à l'obligation de se doter d'un procédé de signature électronique.

L'article 6.6.3 du RIH ajoute quelques précisions, en ce que « *l'avocat qui fournit des prestations juridiques en ligne doit toujours être en mesure d'entrer personnellement et directement en relation avec l'internaute, notamment si la demande qui lui est transmise lui paraît mal formulée (...)* ».

Enfin, l'article 6.6.4 du RIH permet à l'avocat créateur d'un site Internet de prestations juridiques de percevoir librement "*toute rémunération des clients de ce site*". Toujours selon cet article, "*il peut le cas échéant percevoir celle-ci par l'intermédiaire de l'un des établissements financiers assurant la sécurité des paiements en ligne, pour autant que l'identification du client reste aussi possible à cette occasion*".

Dans un autre domaine, l'article 8.2 du RIH, dont le but est d'organiser les modalités de prise de contact entre l'avocat et l'adversaire en vue d'une solution amiable d'un différend, prévoit que « *la prise de contact ne peut avoir lieu qu'en adressant à cette partie par une lettre, qui peut être transmise par voie électronique, en s'assurant préalablement de l'adresse électronique de son destinataire.* »

L'obligation est ici moins forte que celle évoquée à l'article 6.6.2 du RIH, mais elle traduit ce souci permanent au plan déontologique d'obliger l'avocat à faire preuve de prudence et de circonspection lorsqu'il correspond avec un interlocuteur en ligne. Il doit être à tout moment en mesure de garantir la destination des messages échangés sur Internet.

Ainsi, afin de répondre aux exigences d'une sécurité renforcée liée au principe du secret professionnel, l'avocat connecté est soumis à l'obligation d'identification certaine de son correspondant en ligne.

### **La garantie de l'intégrité des correspondances et documents de preuve communiqués par Internet**

L'article 5.5 du RIH prévoit que « *la communication de pièces [par un avocat à l'adresse figurant sur les documents professionnels de son adversaire] peut être faite par voie électronique, par la remise de tout support de stockage de données numériques, ou l'envoi d'un courrier électronique, s'il est justifié de sa réception effective par le destinataire.* »

Ainsi, l'avocat connecté peut correspondre et communiquer valablement des pièces à ses confrères en utilisant la voie électronique, pourvu qu'il ait gardé preuve de la réception, qu'il se soit doté d'un outil d'horodatage, et bien sûr qu'il puisse garantir l'intégrité des pièces transmises.

De même, l'avocat doit garantir l'intégrité des consultations juridiques qu'il envoie en ligne.

## **II – Sur les moyens technologiques à son service pour garantir la sécurité générale**

Pour sécuriser ses échanges sur Internet, l'avocat est d'abord confronté au problème

général de sécurité qui est celui de tout utilisateur d'un système d'information communiquant, mais renforcé par les exigences de son ordre.

Si l'on raisonne par analogie avec le monde du papier, on remarque que tout message, quel que soit son support, est exposé à cinq risques majeurs :

- . altération de son contenu : c'est la problématique de l'intégrité,
- . doute sur son auteur : c'est la problématique de l'identité,
- . preuve de son émission et/ou de sa réception : c'est la problématique de la « non répudiation »,
- . étendue de sa diffusion : c'est la problématique de la confidentialité,
- . durée de sa conservation : c'est la problématique de l'archivage.

La culture du papier étant encore très fortement ancrée chez les avocats, le tournant vers un support numérique ne peut aller de pair qu'avec une importante sécurisation des échanges numériques et un développement des outils permettant de l'obtenir.

Or, les outils de sécurisation du monde numérique sont à utiliser avec prudence et circonspection, même si leur degré d'efficacité apparaît en définitive identique aux méthodes utilisées dans le monde du papier, et même s'ils sont exposés aux mêmes risques.

De première part, la longévité du message électronique est assurée par les techniques d'archivage numérique. Comme dans le monde du papier, on peut décider d'assumer soi-même cette tâche ou de s'en remettre à un tiers spécialisé, dit « tiers archiveur ».

De seconde part, la confidentialité des supports numériques est assurée par les techniques de chiffrement, prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens conçus à cet effet. La confidentialité dans le monde du papier est de son côté garantie par l'enveloppe et par les mentions « personnel et confidentiel » interdisant l'ouverture du message par une autre personne que son destinataire.

Les techniques de chiffrement peuvent être mises en œuvre soit directement par l'utilisateur, à l'aide d'un certificat de signature qu'il détient, soit en passant par un tiers de confiance dont le site, dit sécurisé, assure le chiffrement des messages aussi bien lorsqu'ils circulent que lorsqu'ils sont stockés, étant souligné naturellement que c'est l'auteur du message qui détient la clé de décryptage.

Dans le monde du papier, la garantie de non répudiation résulte du recours à un tiers de confiance, la poste, à qui l'on confie l'acheminement du message et qui délivre un

récépissé de dépôt et de remise (LRAR). Dans le monde numérique, la non répudiation oblige à recourir aux services d'un tiers de confiance, par lequel transitent les messages, et qui à ce titre peut émettre des attestations d'émission et de réception.

Enfin, l'identité et l'intégrité des messageries sont assurées par les procédés de signature électronique, qui prennent la forme de certificats de signature. Par papier, l'identité est sensée être garantie par la simple association entre un nom et une signature manuscrite de l'auteur de l'acte.

Ainsi, le RIH consacre de manière large le recours à Internet comme d'un outil de communication. Il précise que, pour ce faire, l'avocat connecté est soumis non seulement aux préoccupations de sécurité générales (intégrité, identité, confidentialité, ...), mais également aux obligations de sécurité liées aux règles déontologiques (identification).

En pratique, afin d'être en conformité avec les exigences déontologiques qui pèsent sur lui, il doit recourir à des fournisseurs spécialisés.

Toutefois, même si les outils et les services technologiques qui lui sont proposés ne sont pas moins fiables que les procédés du monde du papier, il n'en demeure pas moins qu'ils doivent être utilisés avec prudence.

**Par Me. Héloïse Comte, Avocate stagiaire .**

---

## Commerce électronique, Informatique juridique

---

### L'Internet et la déontologie de l'avocat : quelles conciliations possibles ? (1ère partie) -13/04/2004

*Par Me. Héloïse Comte, Avocate stagiaire .*



L'avocat est confronté à une réglementation spécifique en matière de publicité personnelle. Il en résulte que les moyens auxquels l'avocat peut recourir pour sa propre publicité doivent être mis en œuvre avec discrétion et sont étroitement encadrés par les règles déontologiques.

#### ► Partie I : la création par l'avocat de son site Internet

L'avocat est confronté à une réglementation spécifique en matière de publicité personnelle.

En effet, la concurrence entre avocats doit s'accommoder d'une certaine modération obligée par la confraternité. Le confrère ne convoite pas les clients de ses pairs, un peu comme il est défendu de convoiter la femme du voisin !

Il en résulte que les moyens auxquels l'avocat peut recourir pour sa propre publicité doivent être mis en œuvre avec discrétion et sont étroitement encadrés par les règles déontologiques.

Dans un tel contexte, il convient de s'interroger sur l'application de ces règles à la création par l'avocat du 21<sup>e</sup> siècle de son site Internet.

#### 1. La publicité personnelle de l'avocat, un domaine très encadré

En vertu de l'article 131 du décret n° 91-1197 du 27 novembre 1991 sur la déontologie de l'avocat, "*la publicité est permise à l'avocat dans la mesure où elle procure au public une nécessaire information. Les moyens auxquels il est recouru à cet égard sont mis en œuvre avec discrétion, de façon à ne pas porter atteinte à la dignité de la profession, et communiqués au conseil de l'Ordre*".

En d'autres termes, la publicité est permise, c'est le modernisme qui le veut, mais les moyens de publicité personnelle ne doivent pas porter atteinte à la dignité de la profession, tradition oblige !

Ainsi, il en résulte que l'avocat ne peut faire paraître des placards publicitaires dans les journaux ou diffuser des spots à la radio, à la télévision, au cinéma, exhiber sa photographie sur les murs, ou encore distribuer des prospectus.

Il en résulte également une réglementation étroite concernant la plaquette - document de présentation du Cabinet apparaissant matériellement comme une sorte de dépliant -, le papier à lettres, ou encore la plaque apposée à l'entrée de l'immeuble de l'avocat.

Ainsi, la liste des mentions que la plaquette peut contenir est soigneusement encadrée. Il s'agit en particulier de l'ancienneté dans la profession de chacun des avocats membres du cabinet, la structure du Cabinet et son organisation interne, les domaines d'activité, les langues étrangères pratiquées, les correspondants à l'étranger. Le texte figurant sur la plaquette doit être préalablement soumis au Conseil de l'Ordre.

De même, la liste des mentions pouvant figurer sur les papiers à lettres des avocats est limitée pour éviter que ce dernier tourne au placard publicitaire. Les sigles et logos doivent également être déposés au Conseil de l'Ordre.

A Paris, les plaques ont pendant bien longtemps été interdites à l'extérieur des immeubles. Bien heureusement, cette discrétion n'est plus de mise depuis 1994. Toutefois, les plaques doivent encore avoir des dimensions raisonnables, et les mentions y figurant sont elles aussi limitées.

En application de ces règles relatives à la publicité, l'avocat a été pendant bien longtemps soumis à une réglementation plus que restrictive quant aux possibilités pour lui de diffuser des informations par Internet.

Mais, depuis peu, les règles déontologiques ont considérablement évolué sur ce point, dans l'optique plus large d'une adaptation aux moyens technologiques mis à la disposition de l'avocat.

## **2. L'évolution des règles relatives à la création de site**

Le Règlement Intérieur Harmonisé (RIH) des Barreaux, élaboré par le Conseil National des Barreaux (CNB), a pendant longtemps considéré le site Internet de l'avocat comme un mode de publicité. Il renvoyait, quant aux mentions autorisées, aux dispositions retenues pour les plaquettes.

Ainsi, le site de l'avocat mentionnait notamment l'ancienneté dans la profession de chacun des avocats membres du cabinet, la structure du Cabinet et son organisation interne, les domaines d'activité, les langues étrangères pratiquées, les correspondants à

l'étranger.

Par deux délibérations d'Assemblée Générale en date des 5 avril et 28 juin 2003, le CNB a révisé le RIH et consacré une évolution essentielle dans la manière dont les instances ordinales considèrent désormais le site Internet.

Il s'agit ici d'une petite révolution. En effet, « *le site Internet est aujourd'hui considéré comme le prolongement du cabinet et non comme un mode de sollicitation et de démarchage de clientèle.* » (Utilisation des messageries électroniques – Règles de prudence » M. Le Bâtonnier Georges TONNET, Revue Maître n° 143).

Internet étant par principe un espace de liberté, conséquence de la circulation de l'information et du renouvellement des technologies, l'avocat peut parfaitement recevoir des demandes de consultation en ligne et en donner (à ce titre, les articles 6.6 et suivants du RIH organisent la manière dont l'avocat peut donner des consultations en ligne et s'en faire rémunérer), ou encore proposer des commentaires de décisions, des informations sur des évolutions législatives et jurisprudentielles.

Plutôt que d'instaurer une réglementation à caractère général, le RIH a préféré organiser un système de contrôle a priori par les Ordres sur le contenu et les modalités d'accès aux sites (référencement, liens hypertextes permettant à partir d'une page web d'atteindre directement une autre page web, etc...).

A cette fin, l'avocat qui se propose d'ouvrir un site Internet doit en informer l'Ordre et lui communiquer des informations complètes sur le contenu et les modalités d'accès, ainsi que les références du centre d'hébergement. Cette obligation de déclaration existe également en cas de modification ou d'évolution du site.

La conformité du site aux principes de la profession est ainsi passée en revue. Par exemple, sa dénomination doit être conforme au principe de dignité régissant la dénomination des cabinets d'avocats.

Le site de l'avocat peut comporter des liens hypertextes permettant d'accéder directement ou indirectement à des sites de documentation juridique ou d'enseignement (Journal Officiel, Ministère de la Justice, INSEE...), mais également à des sites ou messageries électroniques à caractère commercial ou du secteur marchand (sites d'éditeurs juridiques, d'annuaires en ligne, de portails généralistes...).

Sur ce point encore, l'article 10.11 du RIH a préféré s'en remettre à l'appréciation au cas par cas et au contrôle des Ordres sur le respect des valeurs essentielles de la profession plutôt que d'interdire tout lien vers un site marchand ou commercial.

Ainsi, la profession d'avocat est depuis longtemps "écartelée" entre ses traditions et principes déontologiques de confraternité, délicatesse, modération et désintéressement qui en font une profession à part, et la mouvance vers une soumission aux lois du marché et à la concurrence.

Les règles déontologiques consacrées par le RIH permettent de nos jours une adaptation croissante de l'avocat au "monde des affaires". Les règles encadrant la création par l'avocat de son site Internet en sont un exemple.

**Par Me. Héloïse Comte, Avocate stagiaire .**

Pas de notes de bas de page

---

## Informatique et libertés, Droit de la communication et des télécommunications

---

### Courriels et secret des correspondances privées. - 08/04/2004

*Par Julien Le Clainche, Allocataire de recherche .*



Par le biais de son nouveau service de messagerie électronique «Gmail» la société « Google » se propose d'analyser le contenu des courriels afin d'y insérer des publicités ciblées, et ce faisant violer le secret garanti aux correspondances privées. En effet, le courriel peut accéder à la qualification de correspondance à caractère privé (I) et à ce titre jouir de la protection, assurée par la loi 91-646 du 10 juillet 1990[1] en l'absence d'atteinte à la vie privée.(II)

Par le biais de son nouveau service de messagerie électronique «Gmail» la société « Google » se propose d'analyser le contenu des courriels afin d'y insérer des publicités ciblées, et ce faisant violer le secret garanti aux correspondances privées. En effet, le courriel peut accéder à la qualification de correspondance à caractère privé (I) et à ce titre jouir de la protection, assurée par la loi 91-646 du 10 juillet 1990[1] en l'absence d'atteinte à la vie privée.(II)

#### I. Certains courriels peuvent accéder à la qualification de correspondance à caractère privé

La loi 91-646[2] a vocation à garantir le secret des correspondances privées émises par voie de télécommunication. Il convient donc de déterminer si un courriel est une correspondance (A) privée (B).

#### A. Le courriel est une correspondance.

L'accession du courriel au statut de correspondance n'est pas aussi évidente qu'elle peut le paraître. En effet, le « Vocabulaire juridique » de l'association Henry Capitant[3] définit la correspondance comme un « échange de lettres ou d'autres messages assimilés (telex, télégrammes) » et le secret s'y rapportant comme « la protection des objets confiés à la poste... ». Le courriel n'est alors peut être pas totalement exclu de la catégorie des correspondances puisqu'il peut être considéré comme un « message assimilé », mais ne semble pas pouvoir bénéficier du secret dans la mesure où il n'est pas un « objet confié à la poste ». Ces définitions ne semblent guère adaptées à l'usage

social du courrier électronique.

Fort heureusement, la décision du tribunal correctionnel du 2 novembre 2000[4] est venue éclaircir le statut du courrier électronique en confirmant l'assimilation du courriel à l'échange épistolaire.

Dans cette affaire, un étudiant se plaignait d'une atteinte au secret des correspondances privées à la suite de l'altération et de la disparition de ses courriers électroniques. Pour le tribunal, il ne fait pas de doute que les courriels sont des correspondances : **«le terme "correspondance" désigne toute relation par écrit existant entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts.»** et **« (...) ont manifesté sans équivoque leur volonté (...) de prendre connaissance par surprise des correspondances contenues dans la messagerie électronique de(...) ».**

Si cette décision émane d'une juridiction de première instance, elle n'en reflète pas moins l'usage social de cet outil.

Les courriels étant des correspondances, celles-ci ont-elles un caractère privé ?

## B. Dans quelle mesure les courriels sont-ils des correspondances privées ?

Les correspondances sont traditionnellement appréhendées par le biais d'une distinction entre les messages émis par voie de télécommunication ayant un caractère privé et ceux émis par voie de communication audiovisuelle constituant des communications au public.

La loi 86-1067 du 30 septembre 1986[5] définit successivement les deux notions :

*«On entend par **télécommunication** toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature, par fil, optique, radio-électricité ou autres systèmes électromagnétiques.*

*On entend par **communication audiovisuelle** toute mise à disposition du public ou de catégories de public, par un procédé de télécommunication, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ».*

Le cas des courriels peut donc s'analyser comme une utilisation du réseau Internet à des fins de télécommunication, alors même que celui-ci est susceptible de constituer un moyen de communication audiovisuelle. Rien ne s'oppose alors techniquement à ce que le courriel puisse être considéré juridiquement comme étant susceptible de constituer une correspondance à caractère privé dès lors qu'il satisfait aux autres conditions du caractère privé.

Le tribunal d'instance de Puteaux du 28 septembre 1999[6] précise ces conditions : « *Il y a correspondance privée lorsque le message est exclusivement destiné à une ou plusieurs personnes, physiques ou morales, déterminées et individualisées.* ».

Dans le même sens et appliqué aux courriels, le jugement du 2 novembre 2000[7] affirme que la correspondance « *est protégée par la loi, dès lors que le contenu qu'elle véhicule est **exclusivement destiné par une personne dénommée à une autre personne également individualisée**, à la différence des messages mis à disposition du public* ».

**Cette définition rend éligible à la protection par le secret des correspondances privées les courriers électroniques dont l'émetteur et le récepteur sont identifiés ou individualisés.** Le tribunal correctionnel de Paris s'empresse alors de préciser la distinction.

Le message : « *...s'adresse à une **personne individualisée**, si son adresse est nominative, ou déterminée, si son adresse est fonctionnelle, le destinataire final du message n'étant pas précisé en ce cas, mais son récepteur ayant qualité pour recevoir ledit message, ... est **personnalisé** en ce qu'il établit une relation entre l'expéditeur et le récepteur, laquelle fait référence à l'existence d'un lien les unissant qui peut être familial, amical, professionnel, associatif, etc.* »[8]

**Si tous les courriels ne sont pas des correspondances à caractère privé, il n'en reste pas moins au terme de cette analyse, que bon nombre d'entre eux le sont et bénéficient à ce titre de la protection par le secret au titre de la loi 91-646[9].**

## **II. La protection des courriels au titre du secret des correspondances privées a un fondement autonome de la vie privée .**

### **A. La protection des courriels au titre du secret des correspondances privées.**

L'article 1<sup>er</sup> de la loi relative à la liberté de communication consacre le secret des correspondances privées : « *Le secret des correspondances émises par la voie des télécommunications est garanti par la loi. Il ne peut être porté atteinte à ce secret que par l'autorité publique, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci* ».

Il ne peut dès lors y être porté atteinte que si l'interception est ordonnée par l'autorité judiciaire sur le fondement de l'article 100 du code de procédure pénale, ou si elle a fait l'objet d'une autorisation écrite du premier ministre dans les conditions des articles 3 et suivants de la loi[10].

C'est dans ce contexte normatif que la société « Google » se propose d'analyser le

contenu des courriels afin d'y insérer des publicités ciblées.

Il ne s'agit pas seulement d'analyser le contenu de courriels susceptibles d'être protégés par le secret des correspondances privées, mais éventuellement de les reproduire et de les stocker comme l'indique clairement sa charte de « protection » de la vie privée :

« *Residual copies of email may remain on our systems, even after you have deleted them from your mailbox or after the termination of your account*»<sup>[11]</sup> (des copies résiduelles des courriels peuvent demeurer sur nos systèmes, même après les avoir effacés de votre messagerie électronique ou après la clôture de votre compte).

Dès lors, cette analyse des courriels se heurte de plein fouet au secret des correspondances privées.

## **B. Ne pas confondre protection de la vie privée et secret des correspondances.**

La « Foire aux questions » du service «Gmail» met en avant le fait que les courriels ne sont ni accédés par un être humain, ni communiqués aux annonceurs<sup>[12]</sup> :

« *No humans read your email to target the ads, and no email content or other personally identifiable information is ever provided to advertisers*». (Aucun humain ne lit vos courriels afin de cibler les publicités, ni le contenu des messages, ni d'autres informations à caractère personnel permettant l'identification ne sont transmis aux annonceurs).

Par cet argumentaire « Gmail » semble essayer de se justifier au regard de la protection de la vie privée, et plus précisément de la protection des données personnelles.

**Or, la confidentialité des courriels est assurée par le secret des correspondances privées issu de la loi 91-646 du 10 juillet 1991<sup>[13]</sup> et non sur le fondement de la protection de la vie privée consacrée par l'article 9 du code civil.**

Par conséquent, le plaignant n'aura pas à rapporter la preuve d'une atteinte à sa vie privée ou aux droits garantis par la loi de 1978<sup>[14]</sup> mais celle d'une violation de la confidentialité de sa correspondance privée. **Le fait que l'interception soit réalisée par des robots permet d'atténuer le risque d'atteinte à la vie privée, mais suffit néanmoins à caractériser une interception de correspondance privée** sanctionnée par les articles 226-15 et 432-9 du code pénal.

L'état de l'art ne permettant pas de distinguer un courriel constitutif d'une correspondance privée d'un autre et les stipulations contractuelles étant encore insuffisamment claires et précises, il semble que pour le moment, le service « Gmail » soit promis à bel avenir judiciaire. Il illustre également, la tendance actuelle qui tend à faire fief des lois territoriales au détriment des droits des personnes. Si la libre circulation de l'information est aujourd'hui une réalité, les systèmes juridiques peinent encore à

s'entendre à l'échelle mondiale sur des questions jusqu'alors pétries de valeurs sociales mais présentant aujourd'hui un intérêt économique de plus en plus important.

Par Julien Le Clainche, Allocataire de recherche .

[1] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, JORF 13 juillet 1991.

Adresse : <http://www.legifrance.gouv.fr/texteconsolide/PCEAR.htm> - Consulté le 07/04/2004.

[2] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, précitée note 1.

[3] G.CORNU, « Vocabulaire juridique », Association Henry Capitant, PUF, p.236 et p.810.

[4] Trib.corr Paris, 17<sup>ème</sup> ch, 2 novembre 2000, note X.FURST in Expertise, mai 2001, p.191.

Adresse :

[http://www.legalis.net/jnet/decisions/illicite\\_divers/jug\\_tgi\\_paris\\_021100.htm](http://www.legalis.net/jnet/decisions/illicite_divers/jug_tgi_paris_021100.htm) - Consulté le 07/04/2004.

[5] Loi 86-1067 du 30 septembre 1986 relative à la liberté de communication, JORF 2 octobre 1986.

[6] Trib.corr Puteaux, 28 septembre 1999, Legalis.net

Adresse : [http://www.legalis.net/jnet/decisions/diffamation/jug\\_ti-puteaux\\_280999.htm](http://www.legalis.net/jnet/decisions/diffamation/jug_ti-puteaux_280999.htm) - Consulté le 07/04/2004.

[7] Trib.corr Paris, 17<sup>ème</sup> ch, 2 novembre 2000, précité note 3.

[8] Trib.corr Paris, 17<sup>ème</sup> ch, 2 novembre 2000, précité note 3.

[9] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, précitée note 1.

[10] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, précitée note 1.

[11] Gmail privacy policy, « What type of information do we collect and how do we use it » §2.

Adresse : <http://gmail.google.com/gmail/help/privacy.html> - Consulté le 07/04/2004.

[12] Gmail FAQ, 8. « Are there ads in Gmail ? » .

Adresse: <http://gmail.google.com/gmail/help/about.html#faq> - Consulté le 07/04/2004.

[13] Loi 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, précitée note 1.

[14] Loi 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux Libertés, JORF 7 janvier 1978.

Adresse : <http://www.droit-ntic.com/index2.php?page=l78complete.inc> - Consulté le 07/04/2004.

---

## Informatique et libertés, Loi applicable et juridiction compétente

---

### Données personnelles des passagers aériens : Le Parlement européen et la Commission en profond désaccord -04/04/2004

*Par Julien Le Clainche, Allocataire de recherche .*



Depuis plusieurs mois le Parlement européen et la Commission s'affrontent sur la question de savoir si le transfert de données personnelles des passagers aériens exigé par les services de sécuri...

Depuis plusieurs mois le Parlement européen et la Commission s'affrontent sur la question de savoir si le transfert de données personnelles des passagers aériens exigé par les services de sécurité américains est compatible avec le droit communautaire. Le 16 décembre 2003, la Commission avait négocié un projet d'accord avec les autorités américaines qui doit être adopté en commission cette semaine et en plénière au cours de la session d'avril. Dans ce contexte, le Parlement a adopté mercredi 31 mars 2004 une résolution<sup>1</sup> soulignant l'absence de bases légales du projet d'accord et le caractère inadéquat de la protection des données personnelles dans le domaine des transports aux Etats-Unis au regard du droit communautaire.

A la suite des attentats du 11 septembre 2001, les Etats-Unis ont souhaité mieux maîtriser le flux des personnes naviguant au dessus de leur territoire, ils ont dès lors exigé des compagnies aériennes la possibilité de consulter le « Passenger Name Record » (PNR). Ce fichier, propre à chaque compagnie, rassemble diverses informations relatives

au passager, telle que : son nom, ses coordonnées, son numéro de téléphone, son numéro de carte de crédit, son état de santé ou encore ses préférences alimentaires. Les compagnies aériennes doivent donc laisser les autorités américaines accéder à leur fichier nominatif, le refus étant sanctionné d'une amende dont le montant peut atteindre six mille dollars par demande, et pouvant aboutir à une interdiction d'atterrissage.

Les données personnelles des passagers européens à destination ou transitant par les Etats-Unis sont donc déjà quotidiennement accédées et traitées par les services de sécurité américains.

Le droit communautaire des flux transfrontières de données personnelles : le caractère adéquat de la protection.

Le transfert des données personnelles des individus résidant sur le territoire de la Communauté européenne relève du champ d'application de l'article 25 de la directive 95/46<sup>2</sup>. Cet article dispose : « *le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si (...) le pays tiers en question assure un niveau de protection adéquat* ». Le transfert de données personnelles est donc en principe interdit, sauf à démontrer le caractère adéquat de la protection garantie par le pays tiers.

L'appréciation du caractère adéquat de la protection doit prendre en considération : « *toutes les circonstances relatives à un transfert ou à une catégorie de transfert* »<sup>3</sup>. La directive dresse également une liste exemplative des facteurs à prendre en compte : « *(...) en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées* ». De la sorte, un pays peut par exemple présenter une protection adéquate quant aux traitements de données personnelles réalisés dans le cadre de la recherche dans le domaine de la santé et une protection inadéquate en ce qui concerne les traitements réalisés à des fins commerciales.

Si le pays ne présente pas un *niveau de protection adéquat* le transfert peut néanmoins être possible pour certaines catégories de traitement<sup>4</sup> ou si la protection des données est aménagée par voie contractuelle<sup>5</sup>.

Le Parlement et la Commission s'opposent sur le caractère adéquat ou non de la protection des données personnelles offerte par les Etats-Unis aux personnes à destination ou transitant par les Etats-Unis.

Aux Etats-Unis, si la notion de « *Privacy* » prend appui sur le quatrième amendement de la constitution, elle n'accède pas au rang de droit fondamental. Dès lors, le respect de la *Privacy* n'est pas assuré par un corpus juridique uniforme mais par le droit commun

(torts, diffamation, libel, trepass...) et des normes sectorielles, inexistantes dans le domaine des transports. En outre, seuls les ressortissant des Etats-Unis peuvent prétendre à la protection fondés sur le « *Privacy Act* » de 1974 contre les traitements de l'administration.

En outre, les transferts effectués à partir du « PNR » se font à destination d'autorités publiques et servent à alimenter d'autres programmes de surveillance librement accessibles par « *de nombreuses administrations américaines, y compris tous les services secrets* »<sup>6</sup>.

Le traitement des informations du « PNR » par les autorités américaines ne peut donc être considéré comme garantissant un niveau de *protection adéquat*. En effet, les informations sont susceptibles de circuler d'une administration à l'autre sans que le passager puisse en être informé, ni exercer ses droits, notamment celui d'accéder aux informations qui le concernent. Enfin, le traitement semble disproportionné quant à la finalité à atteindre. L'illégalité du traitement au regard du droit communautaire n'a cependant pas empêché les Etats-Unis d'y procéder en pratique. C'est pourquoi, la Commission a entrepris de négocier un accord au terme duquel les autorités américaines devraient pouvoir accéder à un nombre plus limité d'informations : le nom du passager, sa date de naissance, son numéro de passeport et ses informations de vol.

Le projet d'accord de la Commission est illicite

La Commission n'est pas compétente pour réduire les droits issus de la directive 95/46

La résolution B5 0156/2004 du Parlement conteste la légalité même de ce projet d'accord, la Commission n'étant pas compétente pour aménager les ingérences des Etats dans la vie privée des personnes. En Europe, le droit de la protection des données personnelles est une des composantes de la notion de vie privée. La Convention Européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales (CEDH) consacre en son article 8 le « droit au respect de la vie privée et familiale » en tant que droit fondamental. Dès lors, selon l'interprétation de la Cour européenne des droits de l'Homme<sup>7</sup>, une ingérence dans la vie privée des personnes n'est possible seulement lorsqu'elle est, « (...) *prévue par la loi, qu'elle est nécessaire dans une société démocratique à la poursuite de buts légitimes et qu'elle n'est pas disproportionnée eut égard à l'objectif poursuivi* »<sup>8</sup>. Le projet d'accord de la Commission ne saurait donc abaisser le niveau de protection garanti par la directive 95/46<sup>9</sup>.

A cet égard la résolution du Parlement dispose<sup>10</sup> :

Le projet de la Commission « *est une mesure de simple exécution de la directive 95/46/CE qui ne peut avoir comme effet de réduire les normes de protection des données au sein de l'Union européenne telles qu'elles ont été établies par la voie de la directive*

*95/46/CE (...) dans la pratique, [il] enlèvera, dès son adoption, aux États membres, actuellement responsables d'assurer la protection des personnes à l'égard des données du PNR, toute possibilité de bloquer les transferts pour garantir les droits de leurs citoyens ».*

Le Parlement s'élève donc contre cet empiètement de la Commission sur ses propres prérogatives, mais aussi sur celles des États membres.

Les garanties du projet d'accord ne sont pas satisfaisantes

Le Parlement regrette : « *que la Commission, tout au long de l'année 2003, n'ait pas tenu compte des requêtes réitérées du Parlement européen et des autorités de contrôle des données l'invitant :*

*a) à définir quelles données pourraient être transférées légitimement sans risques (voir la liste des 19 données suggérées le 13 juin 2003 par le Groupe visé à l'article 29,*

*b) à remplacer immédiatement le système «PULL», utilisé sans base légale par l'administration américaine, et sans filtres pour les données sensibles ou pour les vols non transatlantiques, par le système «PUSH», qui permet à chaque compagnie aérienne de ne transférer que les données légitimes et pour les seuls vols à destination des États-Unis,*

*c) à négocier un accord international avec ce pays prévoyant de réelles garanties pour les passagers ou, tout au moins, la même protection que celle assurée aux citoyens américains »<sup>11</sup>*

Le Parlement conteste également le caractère contraignant des « undertakings » sur lesquels s'appuie le projet d'accord de la Commission.

En effet, leur source purement administrative ne saurait les préserver des « réorganisations internes au Department of Home Security, qui rendraient obsolètes les séparations entre structures internes »<sup>12</sup>. En outre, les garanties évoquées n'ont pas encore de bases juridiques aux États-Unis et restent susceptibles d'être modifiées à tout moment, notamment en ce qui concerne les modalités d'utilisation et de réutilisation des données.

Une crise de l'universalité des droits fondamentaux ?

L'opposition du Parlement et de la Commission peut s'analyser comme étant

symptomatique d'une crise de l'universalité des droits fondamentaux. Les Etats-Unis et les Etats membres ont souscrit à la Déclaration Universelle des Droits de l'Homme<sup>13</sup> qui consacre en son article douze, la protection des personnes contre les immixtions dans leur vie privée. Cette déclaration n'a cependant qu'une faible portée juridique et ne peut être invoquée devant un juge.

La conception européenne de la vie privée l'érige en droit fondamental devant être reconnu à tout individu<sup>14</sup>. Il s'agit donc d'un droit universel qui justifie l'application des dispositions communautaires à des européens voyageant ou transitant par les Etats-Unis. Réciproquement, c'est toujours sur le fondement de l'universalité du droit au respect de la vie privée que les Etats membres garantissent la même protection à toutes les personnes présentes sur leur territoire, citoyen ou non. Vue des Etats-Unis, cette conception de la vie privée est souvent perçue comme un impérialisme normatif et par conséquent, difficilement acceptée.

La conception américaine de la « *Privacy* » se démarque de cette analyse notamment dans la mesure où, comme le souligne le Parlement européen, elle ne s'applique qu'aux citoyens américains.

Dés lors, se pose avec acuité la question de l'effectivité du droit au respect de la vie privée et plus largement de l'ensemble des droits fondamentaux, dans un monde qui ne reconnaît pas uniformément leur caractère universel. Néanmoins, les Etats-Unis et les pays européens se retrouvent dans une communauté de valeurs, dont notamment la liberté de circulation des personnes, des biens et des informations. L'expérience américaine d'extraction des informations du « PNR » illustre assez opportunément la réalité pratique de la libre circulation des informations. Il n'en reste pas moins qu'elle est susceptible de constituer une entrave aux déplacements des personnes en plus d'être contraire aux principes européens de protection des données personnelles.<sup>15</sup>

A une époque où les échanges internationaux de données sont une réalité quotidienne, il est étonnant de dresser le constat que le régime juridique entourant ces opérations est flou, contradictoire et par conséquent incertain. Les Etats-Unis s'opposent farouchement depuis toujours à la création d'une autorité indépendante susceptible de rendre des décisions contraignantes. Il s'agit donc d'un formidable défi pour le droit international public, mais aussi privé, que de parvenir à définir un cadre juridique effectif pour les flux internationaux de données personnelles.

Le parlement européen propose la négociation d'un accord international

Dans cet esprit, le Parlement propose une issue par le biais d'un « *véritable accord international* »<sup>16</sup>. Il dresse la liste de ses points incontournables pour parvenir à une entente sur la question du transfert des données du « PNR » dans le cadre des traitements de sécurité américains.

Il devrait être distingué entre les données personnelles donnant lieu à un transfert automatisé et celles qui ne seraient transférées qu'au cas par cas. Toujours dans cet esprit de proportionnalité, le Parlement suggère que soit dressée la liste des crimes graves pour lesquels une demande supplémentaire pourrait être faite et celle des agences susceptibles de partager ces données ainsi que les conditions de protection à respecter.

La période de conservation devra également figurer dans l'accord. Les représentants de la France souhaitent que les informations relatives aux passagers soient effacées vingt quatre heures après qu'ils aient quitté le territoire américain. Finalement, le projet de la Commission laisse la durée de conservation des données à la discrétion des Etats-Unis.

Un « véritable accord international » devra également préciser les modalités d'exercice des droits des personnes et le régime de responsabilité en cas d'inexactitude des informations ayant entraîné la survenance d'un dommage. Enfin, une autorité indépendante devrait être créée et des mécanismes de recours être élaborés en cas de violation des droits des passagers.

Pour l'heure, le Parlement s'indigne de l'absence de volonté d'assurer l'effectivité de la norme tant au niveau communautaire qu'étatique : « constatant que cet accès est illégal aux termes du droit national et du droit européen sur la vie privée et que, malgré cela, ni la Commission, ni les États membres, ni les autorités garantes de la vie privée dotées de pouvoirs contraignants n'ont agi pour assurer l'application de la loi »<sup>17</sup>. Il est à noter que la Commission Nationale de l'Informatique et des Libertés (CNIL)<sup>18</sup> et d'autres autorités indépendantes ayant en charge la protection des données personnelles<sup>19</sup> ainsi que le groupe de l'article 29 ont néanmoins formulé des observations quant à ce projet d'accord.

Il n'en reste pas moins que les données personnelles des passagers européens sont traitées quotidiennement en violation du droit communautaire, que la proposition d'accord de la Commission est loin d'être satisfaisante et que la négociation d'un « véritable accord international » n'est pas encore à l'étude.

Par Julien Le Clainche, Allocataire de recherche .

1 B5 0156/2004, Résolution du Parlement européen sur le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (2004/2011(INI)) (C5 0124/2004) -

<http://www2.europarl.eu.int/omk/sipade2?L=FR&OBJID=72288&LEVEL=3&MODE=SIP&NAV=X&LSTDOC=N> - Consulté le 1<sup>er</sup> avril 2004.

2 Directive 95/46 CE du Parlement et du Conseil, 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, JOCE L 281 du 23.11.1995, p. 31.

3 Article 25-2 de la directive 95/46 précitée note 2.

4 Article 26.1.a de la directive 95/46 précitée note 2, le transfert vers un pays n'offrant pas un niveau adéquat de protection est possible si la personne concernée a donné son consentement indubitable.

Directive 95/46 précitée note 2, section II « Principes relatifs à la légitimation des traitements de données », article 7 et section IX article 26 : Le transfert vers un pays n'offrant pas un niveau adéquat de protection est possible s'il est nécessaire à l'exécution du contrat ou de mesures précontractuelles, au respect d'une obligation légale, ou encore si le transfert sert à la sauvegarde d'un intérêt vital ou d'un intérêt public important ou s'opère dans le cadre d'une action en justice.

5 Article 26.2 de la directive 95/46 précitée note 2 : « *Sans préjudice du paragraphe 1, un Etat membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.* »

6 Bases de données du programme US-VISIT, sur ce point voir Andreas Dietl, directeur de European Digital Rights (EDRI), cité par Imaginons un Réseau Internet Solidaire (IRIS) : <http://www.iris.sgdg.org/actions/pnr/comm-edri0104.html> (consulté le 2 avril 2004).

7 Voir : Cour eur.D.H, Amann c. Suisse, 16 février 2000, recueil des arrêts et des décisions 2000-II, §65.

8 Voir la résolution B5 0156/2004 notes 6,7 et 8 : Résolution du Parlement européen sur le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (2004/2011(INI)) (C5 0124/2004) - <http://www2.europarl.eu.int/omk/sipade2?L=FR&OBJID=72288&LEVEL=3&MODE=SIP&NAV=X&LSTDOC=N> - Consulté le 1<sup>er</sup> avril 2004.

9 Directive 95/46 précitée note 2.

10 Résolution B5 0156/2004 K. a) et c) , précitée note 1.

11 Résolution B5 0156/2004 L. précitée note 1.

12 Résolution B5 0156/2004 L.1.2.(a précitée note 1.

13 ONU, résolution 217 a (III) du 10 décembre 1948, Déclaration Universelle des Droits de l'Homme.

<http://www.justice.gouv.fr/textfond/dudh1948.htm> (consulté le 2 avril 2004).

14 Voir l'article 8 de la Convention Européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales, précitée.

15 L'atteinte à la liberté d'aller et venir est caractérisée dès lors que la seule solution pour un passager européen de ne pas voir ses libertés individuelles bafouées est de ne pas transiter ou ne pas voyager vers les États-Unis.

16 Terminologie utilisée par le Parlement européen, Résolution B5 0156/2004 L.2. précitée note 1.

17 Résolution B5 0156/2004 B. précitée note 1.

18 CNIL, "*Transfert des données passagers : les dernières évolutions*", 20 février 2004, Commission Nationale de l'Informatique et des Libertés.

[http://www.cnil.fr/frame.htm?/thematic/PNR/PNR\\_donnees\\_passagers.htm](http://www.cnil.fr/frame.htm?/thematic/PNR/PNR_donnees_passagers.htm) - (html), Consulté le 21/01/2004.

19 Notamment la Commission pour la protection de la vie privée, autorité de protection des données en Belgique.

---

## Informatique et libertés, Loi applicable et juridiction compétente

---

### Données personnelles dans le secteur des communications électroniques : La Commission rappelle leurs obligations à huit Etats. -02/04/2004

*Par Julien Le Clainche, Allocataire de recherche .*



La directive 2002/58 CE relative à la protection de la vie privée dans le secteur des communications électroniques aurait dû être transposée dans l'ensemble des pays membres depuis le 31 octobre 2003. La Belgique, l'Allemagne, la Grèce, la France, le Luxembourg, les Pays-Bas, la Finlande et le Portugal n'ont pas encore suffisamment modifié leur cadre normatif et sont donc menacés par la Commission d'être poursuivis devant la Cour de justice européenne.

► La directive 2002/58 CE[1] relative à la protection de la vie privée dans le secteur des communications électroniques aurait dû être transposée dans l'ensemble des pays membres depuis le 31 octobre 2003. La Belgique, l'Allemagne, la Grèce, la France, le Luxembourg, les Pays-Bas, la Finlande et le Portugal n'ont pas encore suffisamment modifié leur cadre normatif et sont donc menacés par la Commission d'être poursuivis devant la Cour de justice européenne.

La Commission ouvre la deuxième phase de la procédure d'infraction contre huit États membres pour défaut d'adoption des nouvelles règles sur la protection de la vie privée

applicables aux réseaux et services numériques. Les Etats en cause se sont vus adresser un « avis motivé »[2] par la Commission au terme duquel ils ont deux mois pour réagir, justifier leur retard dans la transposition ou l'absence d'effectivité des dispositions qu'ils ont adopté.

La procédure avait débuté en novembre 2003 par le biais d'un premier avertissement contre neuf pays. Depuis, seule la Suède a adopté une législation spécifique pour endiguer le phénomène des pourriels et encadrer l'utilisation des « témoins de connexion » (« cookies »).

Le commissaire Erkki Liikanen affirme sa volonté d'assurer une mise en œuvre effective de la directive dans l'ensemble des Etats membres :

*« Nous avons la ferme intention de maintenir la pression sur les États membres qui n'ont pas encore mis en œuvre la législation à laquelle ils ont adhéré en 2002. Cette directive est essentielle pour garantir que la vie privée et les données soient protégées dans un monde en ligne. Elle montre que des mesures efficaces peuvent être prises et mises en œuvre au niveau national pour lutter contre les « spams ». Ces règles fixant des conditions communes dans toute l'Union, les utilisateurs sauront à quoi s'attendre, et les entreprises et les États membres sauront ce qu'ils doivent faire. »*

La France, déjà en retard depuis près de cinq dans la transposition de la directive 95/46 du 24 octobre 1995[3], devra donc réagir promptement si elle ne souhaite pas se voir condamnée.

Par Julien Le Clainche, Allocataire de recherche .

[1] Directive 2002/58 CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, JOCE n° L 221 du 04/09/2003 p. 0013 - 0016.

[2] DN: IP/04/435

[http://europa.eu.int/rapid/start/cgi/guesten.ksh?p\\_action.gettxt=gt&doc=IP/04/435|0|R APID&lg=fr&display=](http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/04/435|0|R APID&lg=fr&display=)

[3] Directive 95/46 CE du Parlement et du Conseil, 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, JO L 281 du 23.11.1995, p. 31.