



**IRIS**  
**(Imaginons un réseau Internet solidaire)**  
**294 rue de Charenton**  
**75012 Paris**  
**Tél/Fax ☐ +33(0)144749239**  
**URL ☐ <http://www.iris.sgdg.org>**  
**Email ☐ [iris-contact@iris.sgdg.org](mailto:iris-contact@iris.sgdg.org)**

**SERVICE PUBLIC D'ACCES ET**  
**PROTECTION DES DONNEES PERSONNELLES**  
*DEUX CONDITIONS POUR UN INTERNET DEMOCRATIQUE*

**CONTRIBUTION D'IRIS A LA CONSULTATION PUBLIQUE RELATIVE A**  
**L'EVOLUTION DU DROIT FRANÇAIS DES COMMUNICATIONS ELECTRONIQUES**

**RAPPORT IRIS ☐ SEPTEMBRE 2002**

## SOMMAIRE

Préambule.....	3
1 Introduction .....	4
2 Service public et service universel pour l'accès à Internet .....	5
2.1 Introduction.....	5
2.2 Service public, service universel et missions d'intérêt général .....	5
2.3 Des discours prometteurs qu'il reste à traduire en actes .....	6
2.4 Rôle de l'État et des collectivités locales pour un vrai service public de l'accès...9	
2.5 Recommandations d'IRIS pour un service public de l'accès à Internet .....	10
3 Protection de la vie privée et des données personnelles sur Internet.....	13
3.1 Introduction.....	13
3.2 État actuel de la législation française .....	13
3.2.1 Loi sur la liberté de communication.....	14
3.2.2 Loi sur la sécurité quotidienne .....	14
3.2.3 Loi de finances rectificative pour 2001 .....	15
3.2.4 Loi d'orientation et de programmation pour la sécurité intérieure .....	16
3.3 Problèmes posés par la législation actuelle .....	16
3.3.1 Inintelligibilité et absence de débat démocratique .....	16
3.3.2 Graves incohérences dans la législation .....	16
3.3.3 Difficulté de déterminer et de séparer les différentes données .....	17
3.3.4 Atteintes aux droits et libertés fondamentaux.....	18
3.4 Recommandations d'IRIS .....	19
3.4.1 Recommandations pour l'intelligibilité et l'accès au droit.....	19
3.4.2 Recommandations pour lever les incohérences .....	20
3.4.3 Recommandations pour surmonter la difficulté de déterminer les données.20	
3.4.4 Recommandations pour le respect des libertés et des droits fondamentaux.21	
Annexe□présentation d'IRIS .....	23

## Préambule

Ce document constitue la contribution de l'association IRIS (Imaginons un réseau Internet solidaire <http://www.iris.sgdg.org>) à la consultation publique relative à l'évolution du droit français des communications électroniques. Cette consultation précède l'élaboration d'un projet de loi en vue de la transposition en droit français du «paquet télécom». Il s'agit de sept textes européens, dont six Directives et une Décision.

Parmi ces sept textes, deux Directives intéressent plus particulièrement IRIS :

- La Directive 2002/22/CE du Parlement européen et du Conseil du 7 mars 2002, concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques (directive «Service universel»),
- La Directive 2002/58/CE du Parlement européen et du Conseil 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 (directive «Vie privée et communications électroniques»).

Les détails de la consultation publique sont consultables sur les sites de la Direction du développement des médias ([www.ddm.gouv.fr/consultation/com-electroniques.htm](http://www.ddm.gouv.fr/consultation/com-electroniques.htm)) et du ministère délégué à l'Industrie ([www.telecom.gouv.fr/telecom/cons\\_0702.htm](http://www.telecom.gouv.fr/telecom/cons_0702.htm)). On y trouvera une présentation de la consultation, des liens vers les textes européens, et les questions précises faisant l'objet de cette consultation.

IRIS n'entend pas répondre directement aux questions telles qu'elles ont été formulées, car celles-ci semblent particulièrement s'adresser soit à des experts techniques, soit à des groupes d'intérêts privés spécifiques. Nous regrettons cette approche qui ne laisse que peu de place à l'expression citoyenne présentant une vision politique du développement des télécommunications en France et en Europe. Toutefois, l'association entend par sa contribution rappeler sa vision des enjeux fondamentaux de l'évolution de ce secteur, et ses propositions en vue de leur traduction effective dans le droit national, conformément aux objectifs de l'association : promotion de l'accès à Internet en tant que service public, promotion des usages non marchands d'Internet, et défense des libertés individuelles et des libertés publiques sur Internet.

Certaines des analyses et recommandations d'IRIS reprennent des propositions élaborées dans d'autres circonstances, tout en les complétant. On pourra notamment se référer aux rapports que l'association a déjà publiés (cf. [www.iris.sgdg.org/documents](http://www.iris.sgdg.org/documents)) et aux dossiers mis à disposition du public par IRIS sur son site (cf. [www.iris.sgdg.org/actions](http://www.iris.sgdg.org/actions)).

Ce document a été élaboré pour IRIS par Meryem Marzouki ([Meryem.Marzouki@iris.sgdg.org](mailto:Meryem.Marzouki@iris.sgdg.org)).

## 1 Introduction

IRIS se félicite de constater que le projet de loi sur la société de l'information semble être abandonné, au profit de différentes lois sectorielles. Dans son rapport d'analyses et de recommandations sur l'avant-projet de loi sur la société de l'information, l'association contestait en effet en ces termes la pertinence d'une telle approche : « Plutôt qu'une quelconque loi portant « diverses mesures d'ordre électronique », IRIS revendique que le texte de l'avant-projet de loi donne lieu à plusieurs textes spécifiques, dont le plus important devrait être une « loi sur la liberté de communication en ligne », au même titre que la loi du 29 juillet 1881 sur la liberté de la presse et la loi du 30 septembre 1986 sur la liberté de communication audiovisuelle. Ce n'est qu'à travers une telle décision que l'article 10 de l'avant-projet, disposant que « la communication en ligne est libre », fera sens ».

La suite a donné raison à l'association, mais néanmoins pour le pire. On a vu en effet certaines mesures du projet de loi sur la société de l'information introduites en urgence et sans débat public dans d'autres textes législatifs, votés avec une belle unanimité par la gauche et par la droite. Il s'agit en particulier de mesures relatives à l'accès au réseau et à la protection des données personnelles et de la vie privée. Si l'on attend toujours un projet de « loi sur la liberté de communication en ligne », cette consultation publique en vue de la transposition du « paquet télécom » en droit français fournit déjà une excellente occasion de proposer deux autres textes, l'un relatif au service public et au service universel pour l'accès aux communications en ligne et l'autre relatif aux communications électroniques, aux droits des citoyens et aux libertés, sur le modèle de la loi « Informatique et libertés ».

Dans cette contribution à la consultation publique, IRIS fait le point sur la situation actuelle dans ces deux secteurs, et propose des recommandations simples pour mettre en œuvre à cet égard une politique volontariste et réellement soucieuse du développement démocratique d'Internet en France.

## **2 Service public et service universel pour l'accès à Internet**

### **2.1 Introduction**

Les notions de service public et de service universel sont parfois confondues, volontairement ou par ignorance, dans certains discours. On a même vu la notion de service obligatoire, au contenu législatif pourtant bien défini, présentée comme le service public dans le discours ayant accompagné le projet de loi sur la société de l'information. Or ces notions sont très différentes, d'autant qu'elles ont été élaborées dans des contextes politiques et économiques différents. La notion de service universel n'a été en effet introduite que dans le cadre de la privatisation et de la déréglementation des télécommunications, en Europe comme en France. Il apparaît donc important de rappeler en premier lieu ces notions fondamentales et les logiques qui les déterminent.

La limitation du rôle de l'État et des collectivités locales, c'est-à-dire de la puissance publique, au financement d'une infrastructure exploitée par les seuls opérateurs privés à leur entier bénéfice a longtemps pris prétexte des « Interdits européens ». Il apparaît aujourd'hui clairement que non seulement les collectivités territoriales peuvent effectivement devenir les opérateurs de leurs réseaux, mais que cette évolution est souhaitée par les collectivités elles-mêmes et par l'État, dans un but de décentralisation et d'aménagement du territoire. IRIS se félicite de cette tendance nouvelle, revendiquée par l'association depuis fort longtemps, et figurant par exemple dans son rapport d'analyses et de recommandations sur l'avant-projet de loi sur la société de l'information. Si les échecs retentissants dans le secteur des télécommunications, et plus particulièrement celui de France Télécom, peuvent avoir un effet positif, malgré le coût social et économique induit, cela doit assurément être celui de signer la fin de la régulation par le marché dans les économies de réseau, et le retour de la prise de conscience du rôle majeur de la puissance publique dans ce type d'économie, notamment à cause de ses externalités d'ordre social et économique.

Toutefois, décentralisation ne doit pas signifier désengagement — voire démission — de l'État, dont le rôle est essentiel pour pallier les disparités régionales, éviter la duplication des réseaux, favoriser les économies d'échelle et assurer une bonne péréquation sociale, géographique et tarifaire. Décentralisation ne doit pas non plus signifier opacité de gestion, ni financement abusif par l'impôt, puisque le fonds de service universel existe et peut être mobilisé à cet effet.

Après un rappel des principales notions et un approfondissement de ces points, IRIS propose dans ce document ses recommandations pour la mise en place d'un service public d'accès à Internet.

NB. Dans le cadre spécifique de cette consultation, il n'est pas pertinent de discuter des autres dimensions de l'accès à Internet, correspondant d'une part à l'acquisition d'une base culturelle informatique et électronique minimale par tous afin de maîtriser les transformations de la société dans tous ses aspects, pratiques et citoyens et d'autre part à la disponibilité de logiciels applicatifs de base ou plus spécifiques, notamment par l'encouragement de la production et de l'utilisation de logiciels libres.

### **2.2 Service public, service universel et missions d'intérêt général**

Comme le rappellent de nombreux chercheurs de ce domaine, un service public correspond à un projet politique de transformation sociale, à travers la transformation des structures économiques et sociales, sous l'impulsion d'un État porteur d'une vision politique forte. Un service public, surtout en économie de réseau, s'exerce généralement à travers un monopole, chargé de remplir des missions d'intérêt général.

La notion de service universel est consubstantielle à celle de marché dans les économies de

réseau. Elle sert à compenser le rôle prépondérant des nouveaux monopoles privés, constitués de fait par des acteurs économiques ayant acquis une position dominante (notion générale du droit de la concurrence) ou encore une position dite d'«opérateur puissant» (notion spécifique au secteur des télécommunications). Comme le souligne Philippe Bouquillon, professeur à l'université Paris8, dans une communication présentée lors d'un colloque organisé par le syndicat SUD-PTT en octobre 2001 (voir le site [www.sudptt.fr](http://www.sudptt.fr) pour les documents correspondants), le service universel a pour objectif de «réguler les [...] utilités publiques [qui] sont des actions économiques menées par des agents privés [aux] conséquences économiques ou sociales particulièrement fortes sur leur environnement. Leur régulation, à travers le service universel, doit permettre de s'assurer que le caractère privé et de gestion marchande de ces activités économiques n'entrave pas les bénéfices économiques et sociaux dont peut bénéficier l'environnement. Le service universel a donc une définition «fonctionnelle». Il est destiné à maximiser les avantages procurés à la communauté tout en respectant les intérêts légitimes des opérateurs industriels marchands».

En droit français, le service public est défini par trois composantes dont le contenu est précisément énuméré : le service universel, les services obligatoires et les missions d'intérêt général (articles L35 à L35-7 du Code des postes et télécommunications). L'opérateur chargé d'assurer le service universel et les services obligatoires est France Télécom, mais rien n'empêche d'autres opérateurs de les assurer s'ils le souhaitent et s'ils en ont la capacité. Les services contenus dans le service universel et dans les services obligatoires doivent être fournis sur l'ensemble du territoire. La différence entre service universel et services obligatoires réside dans la faculté de déterminer les tarifs de ces services : si le tarif du service universel est homologué par la puissance publique nationale, ceux des services obligatoires peuvent être librement déterminés par l'opérateur qui en a la charge, sauf dans le cas où une concurrence existe, les tarifs étant alors homologués comme pour le service universel.

Le contenu du service universel est ainsi défini : «Le service universel des télécommunications fournit à tous un service téléphonique de qualité à un prix abordable. Il assure l'acheminement des communications téléphoniques en provenance ou à destination des points d'abonnement, ainsi que l'acheminement gratuit des appels d'urgence, la fourniture d'un service de renseignements et d'un annuaire d'abonnés, sous formes imprimée et électronique, et la desserte du territoire national en cabines téléphoniques installées sur le domaine public». Il est également précisé que sa fourniture se fait «dans des conditions tarifaires et techniques prenant en compte les difficultés spécifiques rencontrées dans l'accès au service téléphonique par certaines catégories de personnes en raison notamment de leur niveau de revenu ou de leur handicap».

La loi définit ainsi le contenu des services obligatoires : «Une offre, sur l'ensemble du territoire, d'accès au réseau numérique à intégration de services, de liaisons louées, de commutation de données par paquet, de services avancés de téléphonie vocale et de service télex».

Les missions d'intérêt général sont définies en matière de défense, de sécurité, de recherche publique et d'enseignement supérieur.

La Commission supérieure du service public des postes et télécommunications est chargée de veiller au respect des principes du service public et notamment du service universel.

### **2.3 Des discours prometteurs qu'il reste à traduire en actes**

IRIS se félicite que les discours officiels au plus haut niveau reconnaissent enfin l'échec patent d'une stratégie fondée sur la seule «régulation» par le marché du déploiement de l'infrastructure et de l'accès à Internet et semblent préparer le retour à un rôle important de

l'État et des collectivités locales dans le double objectif d'une généralisation de l'accès à Internet — compris en haut débit — et d'un bon aménagement du territoire.

Le discours de la ministre chargée de la Recherche et des Nouvelles Technologies, prononcé lors de l'édition 2002 de l'Université d'été de la communication à Hourtin ([www.recherche.gouv.fr/discours/2002/dhourtin.htm](http://www.recherche.gouv.fr/discours/2002/dhourtin.htm)), est à ce titre édifiant. « Les concepts abstraits d'« Autoroutes de l'information », le gonflement puis l'éclatement de la « Bulle Internet », la réussite mitigée des « Opérateurs alternatifs », les promesses non tenues de l'Internet mobile, les tergiversations réglementaires et techniques sur le mobile de troisième génération ont, en effet, eu un impact négatif sur la perception des nouvelles technologies par les Français ».

Sur le point particulier de l'accès, la ministre poursuit ainsi : « En décembre 2001, la France comptait 7,1 millions d'abonnés actifs à l'Internet, résidentiels ou professionnels. Parmi ceux-ci, les abonnés bénéficiant du haut débit (câble, ADSL) représentaient un peu moins de 10% — soit 600 000 abonnés. L'opinion publique a clairement conscience d'une inégalité d'accès à l'Internet, aussi bien sur le mode connecté qu'en haut débit : 75% de nos concitoyens estiment que tous n'ont pas les mêmes chances d'accès à Internet, et considèrent qu'Internet devient un critère de sélection déterminant à l'embauche. Nous devons focaliser nos objectifs sur ces deux chiffres d'abonnés Internet et d'abonnés haut débit — puisque pour l'un comme pour l'autre nous sommes loin du peloton de tête en Europe — en utilisant les possibilités incitatives et régulatrices de l'État ».

Le discours du ministre de la Fonction publique et de la Réforme de l'État, prononcé à la même occasion, va dans le même sens tout en se concentrant sur la question de l'aménagement du territoire : « Certaines collectivités ont aujourd'hui dans les zones les plus dynamiques accès à de telles infrastructures. Les autres, dans les zones moins favorisées, qui sont aussi le plus souvent les zones délaissées par les opérateurs, doivent également avoir les moyens de se développer. Au-delà des aspects liés au développement de l'Internet local [...], cette problématique soulève des enjeux d'aménagement du territoire considérables » ([www.fonction-publique.gouv.fr/leministre/lesdiscours/discours-200209021647.htm](http://www.fonction-publique.gouv.fr/leministre/lesdiscours/discours-200209021647.htm)).

L'Autorité de régulation des télécommunications note quant à elle dans son rapport de juillet 2002 sur l'adaptation de la régulation : « Une telle évolution [revenir sur l'interdiction faite aux collectivités d'exercer l'activité d'opérateur] peut se justifier par les exigences d'aménagement du territoire au regard de la réalité du marché. Il apparaît aujourd'hui clairement que, même avec une aide des collectivités territoriales, certaines zones du territoire ne pourront être desservies par les opérateurs dans des conditions de rentabilité suffisante. Il pourrait donc être envisagé d'autoriser les collectivités qui le souhaitent, sous certaines conditions et dans les zones les moins desservies, à établir et à exploiter elles-mêmes un réseau de télécommunications » ([www.art-telecom.fr/publications/rarefinal.pdf](http://www.art-telecom.fr/publications/rarefinal.pdf)).

Notons par ailleurs que dans ce récent rapport, l'Autorité de régulation des télécommunications montre l'évolution de sa position depuis 1999 ([www.art-telecom.fr/dossiers/su/](http://www.art-telecom.fr/dossiers/su/)) sur l'extension du service universel aux communications mobiles et à l'Internet haut débit, qu'elle considère désormais comme justifiée, tout en soulignant les problèmes juridiques soulevés au niveau européen à cet égard, et surtout en écartant son financement par le fonds de service universel, dans une curieuse et bien soudaine invocation de la solidarité nationale à propos du service universel, lequel a justement servi à légitimer la privatisation des télécommunications et ne peut être considéré que comme un ersatz de service public dans ce secteur : « Le service universel répondant à un objectif d'intérêt général, il serait logique que son coût soit assumé en amont par le budget d'État et non par les seuls acteurs d'un même secteur, choisis arbitrairement étant donné qu'il s'agit d'un secteur en pleine croissance. La solution budgétaire semble plus conforme au principe de solidarité

nationale qui fonde la mise en oeuvre du service universel. En outre, la solution du financement par l'impôt présente l'avantage d'être neutre à l'égard du fonctionnement du marché. Cette affirmation est d'autant plus contestable que la mise en oeuvre du service universel n'est bien entendu pas fondée sur le principe de solidarité nationale — «seul le service public peut y prétendre»—, mais sur un objectif fonctionnel destiné à corriger les disparités entre opérateurs dans un contexte concurrentiel d'une part et à limiter les effets négatifs de l'abandon du service public sur la collectivité d'autre part.

Au-delà de cette prise de position favorable aux opérateurs privés de la part de l'Autorité de régulation des télécommunications à propos du fonds de service universel, on retiendra de toutes façons que le discours politique a bel et bien évolué récemment.

Ce discours politique nouveau ne saurait être expliqué de façon simpliste par un changement de majorité politique, d'autant qu'il s'expliquerait assez curieusement — «à ironiquement»— de ce fait étant donné le sens du changement. Depuis 1997, avec l'annonce et le développement du «Programme d'action gouvernementale pour la société de l'information» par la précédente majorité, on a en effet peu relevé de divergences de fond entre les principaux partis de gauche et de droite sur toutes les questions liées à Internet, comme l'a souligné IRIS à plusieurs reprises, notamment à l'occasion des débats parlementaires et des votes subséquents.

Ces directions nouvelles annoncées, dont on attend bien sûr de voir comment elles seront effectivement mises en oeuvre, doivent plutôt être mises au compte de la prise de conscience d'une réalité qui dépasse malheureusement les pires pronostics et les mises en garde les plus sévères qui ont pu être avancés par certains acteurs associatifs et syndicaux dont fait partie IRIS.

Ainsi, comme le rapporte le journal en ligne 01net dans un dossier consacré à ce sujet en date du 9 septembre 2002 «La déréglementation des télécommunications, entrée en vigueur à l'échelle européenne le 1er janvier 1998, a laissé le champ libre aux opérateurs privés pour créer des réseaux alternatifs aux monopoles publics et irriguer les territoires de technologies nouvelles. Quatre ans plus tard, le constat est sans appel : la concurrence est restée cantonnée aux grands centres économiques et, malgré les aménagements réglementaires pour éviter la création d'une trop grande fracture numérique, des zones géographiques entières restent sous-équipées. Si l'on s'en tient aux investissements des opérateurs déjà réalisés dans des infrastructures de boucle locale pour développer le haut débit, la France serait découpée en trois zones inégales. D'une part les zones blanches, c'est-à-dire les grandes agglomérations qui regroupent 65% de la population sur 10% du territoire...]. Ensuite, les zones grises, les territoires disposant d'un potentiel économique, mais isolés des grandes infrastructures qui représentent 10% de la population sur 10% du territoire...]. Enfin, les zones noires qui représentent 25% de la population sur 80% du territoire» ([www.01net.com/rdn?oid=192817&rub=3363&page=0-192817](http://www.01net.com/rdn?oid=192817&rub=3363&page=0-192817)).

Par ailleurs, il n'est plus possible de nier que la situation catastrophique du secteur des télécommunications, et l'incroyable situation dans laquelle se trouve actuellement France Télécom (plus de 70 milliards d'euros de dette, 12 milliards de pertes simplement pour le premier semestre 2002, comme le rappellent Pierre Khalfa et René Ollier dans une tribune du journal Libération du 18 septembre 2002) est non seulement le résultat de l'échec de la régulation par le marché dans les économies de réseau et de la stratégie qui visait à transformer une entreprise de service public en une firme multinationale, comme l'analysent les auteurs de cette tribune, mais aussi et surtout le produit tout à fait prévisible de la démission de l'État, voire de «la faillite de l'État régulateur porteur de l'intérêt général et d'une vision de long terme».



## 2.4 Rôle de l'État et des collectivités locales pour un vrai service public de l'accès

Il est grand temps de mettre fin à cette stratégie —~~ou~~ plutôt à cette absence de stratégie~~—~~ dont le coût social et économique est énorme. Il est grand temps de redéfinir les contours et la mise en œuvre d'une stratégie de service public pour l'accès à Internet, dans laquelle l'État comme les collectivités locales puissent jouer pleinement leur rôle dans une articulation rationnelle au service de la collectivité pour remplir leurs missions d'intérêt général, en faisant bon usage d'un service universel étendu, notamment du point de vue du financement en mobilisant le fonds de service universel dont c'est l'objet.

Toutefois, dans l'objectif d'une généralisation de l'accès à Internet à haut débit, mais aussi en vue d'améliorer plus globalement la décentralisation et l'aménagement du territoire, il n'est pas illégitime d'envisager de mobiliser, outre le fonds de service universel —~~qu'il~~ convient évidemment de maintenir, contrairement à ce que suggère l'Autorité de régulation des télécommunications, voire d'étendre~~—~~ des subventions publiques au niveau local comme au niveau national, eu égard aux externalités de réseau, dont l'impact social et économique, pour difficile à mesurer qu'il soit, s'étend très certainement au-delà du seul secteur des télécommunications.

Il convient alors de permettre aux collectivités locales d'être opérateurs de télécommunications, et non de les cantonner à un rôle d'investisseurs au service des opérateurs privés par le seul déploiement de l'infrastructure. Bien entendu, un strict contrôle de la transparence de ces procédures, de la décision démocratique de leur mise en œuvre et de la nécessité réelle des subventions publiques doit alors être mis en place, de sorte que ces subventions ne viennent pas subrepticement se substituer à la contribution des opérateurs privés.

La contribution de la puissance publique par des subventions ne peut s'envisager alors que dans le cadre de l'extension des missions d'intérêt général participant à la définition juridique du service public. Le rôle de la Commission supérieure du service public des postes et télécommunications devrait à cet égard être renforcé.

La condition la plus importante de la légitimité d'un tel schéma demeure évidemment l'extension du service universel à l'Internet haut débit, par le câble et l'ADSL lorsque c'est raisonnablement envisageable, mais sans négliger les apports des techniques nouvelles basées sur la communication sans fil, particulièrement intéressantes au niveau local.

Par ailleurs, le service public pour l'accès à Internet a une dimension plurielle. Outre le déploiement de l'infrastructure et la possibilité d'être opérateur, y compris pour la fourniture de l'accès, la question de l'attribution et de la gestion des noms de domaine doit aussi en faire partie. En effet, on ne saurait concevoir l'accès à Internet dans le seul objectif de consommation d'information. Il s'agit pour toutes les composantes de la société, et en premier lieu celles de la société civile, d'utiliser l'accès au réseau pour une meilleure participation à la collectivité et à la vie publique, locale comme nationale. Tous les acteurs économiques et sociaux ont donc vocation à déployer leurs activités visiblement sur Internet, et à utiliser ce moyen pour participer au débat public. À ce titre, le bénéfice d'un nom de domaine doit être considéré comme faisant partie du dispositif global de l'accès. Depuis 1997, l'opérateur du .fr est l'AFNIC (Association française pour le nommage Internet en coopération). L'AFNIC a le monopole de gestion d'un bien public, mais ne fonctionne pas du tout comme un opérateur de service public des noms de domaine en France, comme cela a été analysé et dénoncé à plusieurs reprises par IRIS. Il convient donc de bien définir juridiquement les conditions d'accès et de coût pour cette ressource publique qu'est l'espace du nom de domaine de premier niveau constitué par le .fr, en l'incluant dans le service public pour l'accès à Internet.

## **2.5 Recommandations d'IRIS pour un service public de l'accès à Internet**

La première nécessité est évidemment l'extension du service universel à l'Internet à haut débit, c'est-à-dire le droit à l'accès haut débit pour le même tarif en tout point du territoire, quitte à définir un calendrier pour la mise en place d'une véritable politique publique d'accès de tous à Internet, prenant en compte toutes ses dimensions □ diversité des modes de communication, (ADSL, câble, communication sans fil), diversité des acteurs publics et privés impliqués, diversité des lieux d'accès (domicile, point d'accès public, ...).

***IRIS recommande l'extension de la définition juridique du service universel à l'Internet à haut débit.***

Le second point concerne le rôle des collectivités locales. Un article de l'avant-projet de loi sur la société de l'information, relatif à la création d'infrastructure par les collectivités locales, a fait l'objet d'un amendement au projet de loi portant diverses dispositions d'ordre social éducatif et culturel. Il a été adopté comme article 19 de la loi n°2001-624 du 17 juillet 2001.

Cet article a modifié en profondeur l'article L.1511-6 du code général des collectivités territoriales, qui fixe les conditions de création, par les collectivités territoriales, d'infrastructures destinées à supporter des réseaux exploités par les opérateurs privés de télécommunications. L'ancien article était issu de la loi n°99-543 du 25 juin 1999 d'orientation pour l'aménagement et le développement durable du territoire.

L'exposé des motifs de l'avant-projet de loi justifiait de telles modifications par la volonté du gouvernement de simplifier les modalités de création d'infrastructure. Au prétexte de la simplification des procédures, cet article permet en fait une considérable régression par rapport à la situation précédente.

Régression d'abord en matière de contrôle démocratique des investissements publics □ ainsi, la décision de créer une infrastructure pour les réseaux de télécommunications n'est plus subordonnée à un constat de carence des acteurs du marché à fournir une offre de services ou de réseaux à un prix abordable et selon des exigences techniques et de qualités attendues □ ce constat de carence est remplacé par un simple recensement des besoins des opérateurs ou des utilisateurs. Mieux encore, les dépenses et recettes relatives à la construction, à l'entretien et à la location des infrastructures ne sont plus examinées de façon prévisionnelle par les organes délibérants dûment informés de la carence du marché, et il n'est plus fait mention des modalités de calcul de la location des infrastructures.

***IRIS recommande le rétablissement dans le code général des collectivités locales du contrôle démocratique des investissements publics locaux en matière de télécommunications.***

Régression ensuite en matière de service public □ l'article L.1511-6, qui figure dans le code général des collectivités territoriales au chapitre de l'aide aux entreprises, permet dans sa nouvelle version encore plus d'aide aux opérateurs privés de télécommunications, en supprimant la plupart des contraintes dont cette aide était assortie. En effet, les références aux articles L.32 et L.33-1 du code des postes et télécommunications ont disparu de la définition des opérateurs privés susceptibles d'exploiter les infrastructures. Or ces mentions permettaient respectivement la référence aux définitions précises des opérateurs de télécommunications et des exigences essentielles de garantie de l'intérêt général (L.32) et à l'exigence de respect par les opérateurs concernés d'un cahier des charges, comportant notamment l'obligation de service universel définie aux articles L.35-2 et L.35-3 du code des postes et télécommunications (L.33-1).

***IRIS recommande le rétablissement dans le code général des collectivités locales du respect de l'obligation de service universel pour les opérateurs privés utilisant les infrastructures déployées par la puissance publique.***

En outre, l'article 19 de la loi n°2001-624 du 17 juillet 2001 introduit la possibilité de subventionner la mise en place d'infrastructures dans certaines zones géographiques. IRIS soutient le principe d'une telle subvention, conforme au principe de péréquation tarifaire du service public. Toutefois, une telle subvention ne doit pas être financée abusivement par l'impôt, puisque le fonds de service universel a été créé justement dans ce but. C'est ce fonds qui doit être maintenu et prioritairement utilisé pour compenser les différences de coût des infrastructures entre les régions. Le financement par l'impôt ne doit être conçu qu'à titre complémentaire, lorsque l'effet des externalités de réseau sur le plan social et économique est démontré pour remplir des missions d'intérêt général définies dans le service public des télécommunications.

***IRIS recommande de soumettre les subventions publiques locales ou nationales pour le déploiement d'infrastructure à de réelles externalités de réseau dans l'objectif de remplir des missions d'intérêt général définies dans le service public des télécommunications.***

Pour justifier pleinement du bénéfice de subventions publiques, le déploiement d'infrastructure doit avoir pour objectif de remplir des missions nouvelles d'intérêt général. Celles-ci doivent figurer dans la définition du service public des télécommunications, et être soumises à un contrôle.

***IRIS recommande d'étendre les missions d'intérêt général du service public des télécommunications au développement social et économique et de renforcer le rôle de la Commission supérieure du service public des postes et télécommunications en la chargeant de veiller également au bon emploi des subventions publiques locales ou nationales pour remplir ces missions.***

D'autre part, tant dans son ancienne version que dans la nouvelle, l'article L.1511-6 du code général des collectivités territoriales interdit aux collectivités territoriales d'exercer elles-mêmes l'activité d'opérateur de télécommunications. Cette interdiction est extrêmement regrettable. Elle interdit l'existence d'un vrai service public de l'accès à Internet.

***IRIS recommande que les collectivités territoriales, notamment à l'échelle intercommunale, puissent exercer l'activité d'opérateur de télécommunications, au sens de l'article L.32 du code des postes et télécommunications.***

Cette possibilité ne supprimera pas le recours, le cas échéant et sur décision des organes délibérants, à d'autres opérateurs, dont l'activité devrait être soumise au respect d'un cahier des charges établi notamment en fonction d'exigences de péréquation tarifaire pour le coût du service offert aux usagers.

Le dernier aspect du service public pour l'accès à Internet concerne les noms de domaine. La première nécessité à cet égard est de reconnaître, comme le faisait d'ailleurs le projet de loi sur la société de l'information, les domaines de premier niveau dans la zone correspondant aux codes pays de la France comme une ressource publique, qui doit être gérée dans le cadre d'un service public d'enregistrement des noms de domaine, dont l'opérateur pourrait être l'organisme de gestion des ccTLD relevant de la France.

***IRIS recommande l'extension du service universel au bénéfice d'un nom de domaine dans la zone du .fr.***

Ce service public d'attribution d'un nom de domaine n'interdit pas le recours éventuel à un prestataire intermédiaire entre l'utilisateur et l'organisme de gestion, si tel est le souhait de l'utilisateur, mais ce recours ne doit aucunement être obligatoire comme c'est le cas actuellement.

Les missions de cet organisme devront lui imposer l'attribution, directe et simplifiée par des téléprocédures automatiques, de noms de domaines dans les ccTLD de sa compétence et dans les gTLD, en suivant la règle commune du « premier arrivé premier servi » dans ce

dernier cas. Le but est d'assurer des conditions d'accès objectives, transparentes et non discriminatoires, applicables tant au domaine de premier niveau (.fr par exemple) qu'aux domaines de deuxième niveau (.asso.fr ou .nom.fr par exemple).

Un coût maximal devra être fixé par domaine pour les personnes physiques et les groupements à but non lucratif, ne devant pas dépasser le double du prix unitaire le plus bas reversé à l'organisme international en charge de la gestion technique pour les noms de domaine génériques.

La péréquation tarifaire sera assurée d'une part par une surtaxe raisonnable pour l'attribution de noms de domaines aux groupements à but lucratif et d'autre part par le fonds de service universel, en tant que contrepartie logique de l'extension du service universel au bénéfice d'un nom de domaine.

### **3 Protection de la vie privée et des données personnelles sur Internet**

#### **3.1 Introduction**

La transposition en droit français de la Directive « Vie privée et communications électroniques » est une occasion unique d'une part pour la mise en cohérence de la législation actuelle française relative à la protection des données personnelles et de la vie privée dans les communications électroniques, d'autre part pour que cette législation devienne réellement protectrice des droits des citoyens, conformément aux textes fondamentaux du droit français, du droit européen et du droit international.

Deux enjeux principaux doivent être soulignés ici :

- Protection des données personnelles, de la vie privée et de la confidentialité des communications vis-à-vis de l'utilisation commerciale de leurs données personnelles,
- Protection des données personnelles, de la vie privée et de la confidentialité des communications vis-à-vis des atteintes aux droits et libertés fondamentaux.

Si le premier enjeu nous semble relativement bien couvert à la fois par le texte existant (loi « Informatique et Libertés »), par son projet de révision en cours ainsi que par les dispositions de la Directive « vie privée et communications électroniques » à transposer, il n'en va pas du tout de même pour ce qui est du second enjeu.

Durant la précédente législature, certains textes de loi ont en effet été modifiés dans des conditions très discutables : adoption d'amendements en urgence sans le nécessaire débat public digne d'un pays démocratique, amendements introduits dans des textes dont l'objet était très éloigné de la teneur de ces amendements (« cavaliers législatifs »), extension de la portée de ces amendements dans d'autres textes, menant à des incohérences dans la législation.

Cette situation a non seulement conduit à nombre de protestations de la part d'organisations citoyennes, allant jusqu'à la plainte contre la France déposée par l'association IRIS auprès de la Commission européenne pour violation de la législation communautaire, mais également à une forte insécurité ressentie par les intermédiaires techniques pour l'accès et l'hébergement à Internet, qu'il s'agisse des sociétés commerciales ou des fournisseurs du secteur associatif, coopératif et non marchand. Par ailleurs, la législation française en est devenue incohérente, ce qui explique, dans notre analyse, l'absence de publication de plusieurs décrets d'application à ce jour, pour des textes récents comme pour des textes adoptés voilà déjà deux ans. Enfin, une récente annonce, contenue dans la loi d'orientation et de programmation pour la sécurité intérieure, fait l'objet d'une forte inquiétude qu'IRIS a manifestée dès le 16 juillet dernier.

Il nous apparaît par conséquent nécessaire d'analyser finement les textes législatifs français actuels, pour en souligner à la fois les incohérences et les atteintes aux droits et libertés fondamentaux qu'ils présentent, avant de proposer nos recommandations pour leur modification, dans le cadre de la transposition du « paquet télécom » dans la législation nationale.

#### **3.2 État actuel de la législation française**

Les textes considérés comme posant problème et examinés ici sont la loi n°86-1067 du 30 septembre 1986 sur la liberté de communication (articles 43-9 et 43-10), la loi n°2001-1062 du 15 novembre 2001 sur la sécurité quotidienne (articles 29, 30 et 31), la loi n°2001-1276 du 28 décembre 2001, loi de finances rectificative pour 2001 (article 62) et la loi n°2002-1094

du 29 août 2002, loi d'orientation et de programmation pour la sécurité intérieure (article 1er approuvant l'annexeII).

### **3.2.1 Loi sur la liberté de communication**

L'article 43-9 dispose que les intermédiaires techniques, fournisseurs d'accès et d'hébergement, sont tenus de conserver toute donnée permettant l'identification des auteurs de contenus hébergés par leurs services. L'application de cette disposition reste toutefois soumise à la publication d'un décret en Conseil d'État, qui devra être pris après avis de la Commission nationale de l'informatique et des libertés (CNIL). Ce décret devra déterminer la nature des données à conserver, ainsi que la durée et les modalités de cette conservation par les fournisseurs d'accès et d'hébergement. Notons que deux ans après l'adoption de cette disposition, ce décret n'a toujours pas été adopté. Si cette loi impose aux intermédiaires techniques de détenir ces informations concernant leurs abonnés, elle fixe néanmoins des garde-fou pour l'utilisation de ces données personnelles. Ainsi, seule l'autorité judiciaire peut en requérir communication auprès des prestataires techniques concernés et ces derniers peuvent être sévèrement punis pour toute autre utilisation des données le défaut de préservation de la sécurité des données ou leur communication à des tiers est puni de cinq ans d'emprisonnement et de 300000 Euros d'amende (article 226-17 du code pénal) le fait de détourner ces données de leur finalité est puni des mêmes peines (article 226-21 du code pénal). L'application de l'article 226-22 du code pénal au traitement de ces données vient encore renforcer ces garde-fou.

L'article 43-10 fait obligation aux prestataires d'hébergement de fournir à leurs abonnés des moyens techniques d'indiquer leurs données d'identification les personnes morales doivent tenir à disposition du public leur dénomination ou raison sociale ainsi que l'adresse de leur siège social. Elles doivent aussi indiquer publiquement le nom du directeur ou du codirecteur de la publication et celui du responsable de la rédaction du service s'il y a lieu les personnes physiques doivent tenir à disposition du public leurs nom, prénom et adresse de domicile. Toutefois, si elles éditent les contenus à titre non professionnel et qu'elles ne souhaitent pas cette publicité, elles peuvent ne tenir à la disposition du public qu'un pseudonyme. C'est le fournisseur d'hébergement qui devra alors détenir les données d'identification correspondantes. Dans tous les cas, ces informations doivent être accompagnées des coordonnées du fournisseur d'hébergement (nom et dénomination ou raison sociale). On notera que cette obligation de fourniture de données d'identification est dépourvue de sanction spécifique et que les fournisseurs d'hébergement n'ont aucune obligation de vérifier l'exactitude ou la complétude des données ainsi fournies.

### **3.2.2 Loi sur la sécurité quotidienne**

L'article 29 précise, par un article L.32-3-1 à insérer dans le code des postes et télécommunications, les obligations des opérateurs de télécommunications (fournisseurs d'accès inclus) en matière d'effacement, de conservation, de traitement et/ou de transmission à des tiers des données techniques en leur possession.

Le I de l'article 32-3-1 transpose déjà l'article 6 de la Directive « vie privée et communications électroniques ». Il indique que les opérateurs « sont tenus d'effacer ou de rendre anonyme toute donnée technique relative à une communication dès que celle-ci est achevée ». Le III de l'article 32-3-1 autorise les opérateurs de télécommunications à utiliser et conserver certaines données pour des besoins de facturation et de paiement, ainsi que pour d'éventuels problèmes de contentieux, jusqu'à prescription. Les données concernées doivent être précisées par décret en Conseil d'État pris après avis de la CNIL, non encore adopté. Il dispose également que les opérateurs peuvent effectuer un traitement des données en vue de commercialiser leurs propres services de télécommunications, sous réserve du consentement exprès de leurs usagers. Le IV de l'article 32-3-1 implique que la conservation et le traitement

autorisés pour les données restent soumis à la loi Informatique et libertés, et que les données techniques concernées sont limitées, de sorte que ces données « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par l'opérateur et sur les caractéristiques techniques des communications assurées par ce dernier », et « ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications. ». Notons que ces formules excluent de la conservation et du traitement, outre bien entendu le contenu des correspondances privées, les données de navigation (consultation de sites web). Toutefois, elles n'excluent pas les données relatives à l'identité des personnes impliquées dans une communication, y compris une communication privée.

Le II de l'article 32-3-1 prévoit la possibilité, en dépit du I du même article, de conserver jusqu'à un an toute donnée technique relative à une communication, y compris les personnes impliquées, en tant qu'expéditrices ou destinataires d'une communication privée. Cette conservation de données a pour unique but éventuel leur mise à la disposition de l'autorité judiciaire. La teneur des données et leur temps de conservation sont déterminées par décret en Conseil d'État pris après avis de la CNIL. Ce décret n'a pas encore été adopté.

Le défaut d'effacement ou d'anonymisation des données, ainsi que le défaut de conservation des données, sont punis d'un an d'emprisonnement et de 75 000 Euros d'amende. Les personnes physiques encourent également l'interdiction d'exercer leur activité professionnelle pendant cinq ans, les personnes morales peuvent être déclarées responsables pénalement et encourir les sanctions prévues aux articles 131-9, 131-38 et 131-39 du Code pénal.

L'article 30 autorise le procureur de la République, la juridiction d'instruction ou la juridiction de jugement à prescrire le déchiffrement de données saisies ou obtenues dans le cadre d'une enquête ou d'une instruction. Il peut être fait appel pour le déchiffrement à toute personne ou organisme qualifié, ou, si la peine encourue est au moins égale à deux ans d'emprisonnement, aux moyens de l'État couverts par le secret de défense nationale. Dans ce dernier cas, le service de police judiciaire auquel la réquisition est adressée transmet cette dernière à un organisme technique soumis au secret de la défense nationale. Cet organisme a été créé par le décret n° 2002-1073 du 7 août 2002. Les décisions judiciaires prises en application de l'article 30 n'ont pas de caractère juridictionnel et ne sont susceptibles d'aucun recours.

L'article 31 modifie la loi n°91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications. Elle impose, à la demande d'« autorités habilitées » par le Premier ministre ou les personnes qu'il aura délégués, aux fournisseurs de prestations de cryptographie de fournir les conventions secrètes de déchiffrement, ou de les mettre en oeuvre sous peine de deux ans d'emprisonnement et de 30 000 Euros d'amende. La procédure de mise en oeuvre de cette obligation est fixée par le décret n° 2002-997 du 16 juillet 2002. Par ailleurs, cet article 31 oblige, sous peine de trois ans d'emprisonnement et de 45 000 Euros d'amende, toute personne ayant connaissance d'une convention de déchiffrement d'un moyen de cryptographie « susceptible d'avoir été utilisé pour la préparation, la facilitation ou la commission d'un crime ou d'un délit », à remettre cette convention aux autorités judiciaires.

### **3.2.3 Loi de finances rectificative pour 2001**

L'article 62 modifie l'article 65 du Code des douanes, l'article L.83 du Livre des procédures fiscales et l'article L.621-10 du Code monétaire et financier. Il implique que les données conservées et traitées par les intermédiaires techniques d'accès et d'hébergement peuvent être également exigées par les agents des douanes ayant au moins le grade d'inspecteur ou d'officier et ceux chargés des fonctions de receveur, par l'administration

fiscale, et par les enquêteurs habilités par le président de la Commission des opérations de bourse. Ces données conservées et traitées sont celles mentionnées tant dans la loi sur la liberté de communication que dans la loi sur la sécurité quotidienne.

### **3.2.4 Loi d'orientation et de programmation pour la sécurité intérieure**

Cette loi, adoptée pendant la législature actuelle, ne comporte aucune disposition normative sur la conservation et le traitement des données. Toutefois, en tant que loi d'orientation et de programmation, elle affirme, dans son annexe I approuvée par l'article 1er de la loi, la volonté du gouvernement et du Parlement de «Permettre aux officiers de police judiciaire, agissant dans le cadre d'une enquête judiciaire, sur autorisation d'un magistrat, d'accéder directement à des fichiers informatiques et de saisir à distance par la voie télématique ou informatique, les renseignements qui paraîtraient nécessaires à la manifestation de la vérité». Il s'agit donc de permettre à la fois l'interception des communications et l'accès direct aux données conservées par les intermédiaires techniques d'accès et d'hébergement, ou transitant par leurs machines.

## **3.3 Problèmes posés par la législation actuelle**

### **3.3.1 Inintelligibilité et absence de débat démocratique**

Nous ne nous étendons pas ici sur l'absence de débat démocratique qui a caractérisé l'adoption des textes évoqués ci-dessus. Cela a déjà été amplement dénoncé, par plusieurs organisations citoyennes dont IRIS (voir les dossiers et documents sur notre site). Retenons d'abord que le caractère d'urgence, invoqué notamment pour l'adoption des articles de la loi sur la sécurité quotidienne, a même permis de passer outre l'inconstitutionnalité patente, sur le plan procédural comme sur le fond, pourtant reconnue par certains parlementaires eux-mêmes. Retenons ensuite qu'il n'y avait rien d'urgent à adopter des mesures prévues de longue date dans le défunt projet de loi sur la société de l'information. Retenons surtout que l'argument de l'urgence se révèle aujourd'hui particulièrement spécieux puisque ces dispositions si urgentes attendent toujours, près d'un an, parfois deux, après leur adoption, leurs décrets d'application.

Par ailleurs, l'inintelligibilité de la législation devient de plus en plus préoccupante. Il en va de même de la dispersion des dispositions dans des textes qui ne présentent parfois aucune proximité avec la question du traitement des données personnelles et de la protection de la vie privée. Nous ne citerons à cet égard que les dispositions présentes dans la loi de finances rectificative pour 2001. Outre qu'elle contredit la jurisprudence de la Cour européenne des droits de l'homme, et plus généralement les principes les plus simples de gouvernement démocratique, cette inintelligibilité conduit à des incohérences dans la législation, sur lesquelles nous reviendrons.

### **3.3.2 Graves incohérences dans la législation**

Comme nous l'avons déjà exprimé, l'inintelligibilité des dispositions actuelles et leur dispersion dans différents textes mène à des incohérences. L'une d'elle, la plus grave, est due aux dispositions ajoutées à la loi de finances rectificative de 2001. En effet, le I de l'article 62 de cette loi se contente d'ajouter un élément à une longue énumération figurant à l'article 65 du Code des douanes

« Article 62

I. - A. - Le i de l'article 65 du code des douanes devient le j.

B. - Il est rétabli, dans le 1° du même article, un i ainsi rédigé :

« i) Chez les opérateurs de télécommunications et les prestataires mentionnés aux articles 43-7 et 43-8 de la loi no 86-1067 du 30 septembre 1986 relative à la liberté



de communication, pour les données conservées et traitées par ces derniers, dans le cadre de l'article L. 32-3-1 du code des postes et télécommunications ; »

Or le 3° de l'article 65 du Code des douanes dispose que

« Article 65

3° Les divers documents visés au 1° du présent article doivent être conservés par les intéressés pendant un délai de trois ans, à compter de la date d'envoi des colis, pour les expéditeurs, et à compter de la date de leur réception, pour les destinataires.

Il y a donc incohérence entre le délai de conservation des données de trois ans imposé par le Code des douanes et le délai maximal de un an imposé par l'article 29 de la loi sur la sécurité quotidienne. De plus, la durée maximale de conservation des données imposée par la loi sur la liberté de communication n'a pas encore été fixée puisque le décret d'application de cette disposition n'est toujours pas paru.

Il ne s'agit évidemment pas ici d'une incohérence technique bénigne, mais d'une incohérence grave dans des dispositions limitant les droits et libertés fondamentaux des citoyens, garantis par la Constitution. Si cette incohérence est probablement la cause du retard de parution de plusieurs décrets d'application de dont IRIS ne peut que se féliciter eu égard aux atteintes aux droits et libertés fondamentaux que nous avons dénoncées elle n'en témoigne pas moins d'une incurie qu'il faut impérativement réparer.

### **3.3.3 Difficulté de déterminer et de séparer les différentes données**

La loi sur la liberté de communication fait référence à des « données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elles sont prestataires ».

La loi sur la sécurité quotidienne considère des « données relatives à une communication » et des « catégories de données techniques », tout en précisant que ces données « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques techniques des communications assurées par ces derniers ».

Dans ces deux cas, la teneur de ces données doit être précisée par décret en Conseil d'État, pris après avis de la CNIL.

La loi d'orientation et de programmation sur la sécurité intérieure envisage très largement tous « fichiers informatiques » et plus généralement tous « renseignements qui paraîtraient nécessaires à la manifestation de la vérité », pour autant qu'ils soient saisissables « à distance par la voie télématique ou informatique ».

La Directive « Vie privée et communications électronique » définit en son article 2 les notions suivantes

- « données relatives au trafic » toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation
- « données de localisation » toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public
- « communication » toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un

réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit

Malgré des réflexions intenses au niveau du G8 et d'Europol, ayant mené à la publication de listes très exhaustives de données dont la conservation est jugée nécessaire par ces organismes, la détermination de la teneur des données à conserver n'est à ce jour publiquement arrêtée ni au niveau français ni au niveau européen. La distinction reste en effet très difficile à établir entre « données de localisation relatives au trafic » et « données de localisation autres que relatives au trafic ». Plus généralement, avec l'évolution de l'architecture et des protocoles du réseau Internet (notamment IPv6), le développement de nouveaux services et logiciels de communication et la convergence de ces services (par exemple les « Webmail », pour ne citer qu'un service déjà très répandu), il devient impossible de cloisonner les données en « données d'identification », « données de trafic » et même « données de contenu », toutes catégories de données qui constituent dès aujourd'hui un continuum d'informations. Par ailleurs, la quantité astronomique de données circulant sur le réseau Internet, ajoutée aux possibilités immenses de les interconnecter, y compris avec des données hors réseaux, rend les données dites simplement de trafic extrêmement significatives de la vie privée des personnes.

Il est donc nécessaire de déterminer avec précision et de manière restrictive dans la loi, et non par décret, les seules données permettant l'identification de personnes pouvant faire l'objet d'une enquête dans le cadre d'une instruction judiciaire.

### **3.3.4 Atteintes aux droits et libertés fondamentaux**

Nous nous contenterons de rappeler ici les atteintes aux droits et libertés fondamentaux déjà largement dénoncées par IRIS lors de la discussion parlementaire des quatre textes législatifs mentionnés ci-dessus. On trouvera sur le site web de l'association des analyses plus détaillées à ce sujet.

La détermination de la teneur des données à conserver et de la durée de cette conservation, par décret en Conseil d'État, même pris après avis de la CNIL, contredit l'article 34 de la Constitution : seul le législateur peut limiter les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Étant donné la difficulté de déterminer avec précision une séparation entre « données d'identification », « données de trafic » et même « données de contenu », les données mentionnées à l'article 29 de la loi sur la sécurité quotidienne induisent que les précisions qui y seront apportées par décret permettront de surveiller qui écrit à qui et qui consulte quoi sur Internet, ce qui constitue à l'évidence la limitation d'une liberté constitutionnelle.

Les dispositions relatives au déchiffrement des données ne présentent pas de garanties suffisantes pour encadrer la prescription du déchiffrement, ainsi que les conditions de sa réalisation. Cela vient d'être corroboré par la teneur des décrets parus respectivement en juillet et août 2002. Ces dispositions portent atteinte au secret garanti par certaines professions dans la législation française. L'absence de caractère juridictionnel et de possibilité de recours n'est absolument pas justifiée, et porte atteinte aux garanties qu'un citoyen est en droit d'attendre d'une justice loyale et équitable et d'un État démocratique, d'autant plus que l'application de cette disposition n'est pas limitée aux cas où la peine encourue est supérieure à un maximum donné. Ces dispositions portent en outre atteinte à la présomption d'innocence, et permettent non seulement l'auto-incrimination, mais également l'incrimination par les proches, ce qui les met encore en contradiction avec la législation française.

La conservation a priori de données, surtout pendant une durée pouvant aller jusqu'à un an, pratiquée de manière générale et systématique, à des fins exploratoires, est une pratique contraire à la Convention européenne des droits de l'homme et à la jurisprudence de la Cour européenne des droits de l'homme. Elle déroge de plus aux principes fondamentaux de l'État

de droit, comme le rappelait la CNIL dans son avis sur l'avant-projet de loi sur la société de l'information. Cette mesure ne se justifie même pas par sa nécessité, puisque les données publiées par les fournisseurs d'accès français indiquent que ceux-ci parviennent à satisfaire 500 réquisitions de données par mois, sur commission rogatoire, à l'aide de données conservées en moyenne pendant trois mois ou moins. Ces données permettent la résolution des enquêtes.

Alors que ces données n'étaient censées pouvoir être requises que par l'autorité judiciaire, on a pu voir avec la loi de finances rectificatives 2001 que les possibilités de leur utilisation avaient été très vite étendues à des organismes administratifs. Le danger de cette brèche ainsi ouverte par la disponibilité des données ne peut qu'augmenter. Il est d'ailleurs déjà prévu de l'étendre dans la loi d'orientation et de programmation sur la sécurité intérieure.

Avec les dispositions envisagées dans la loi d'orientation et de programmation sur la sécurité intérieure, on franchirait le seul garde-fou qui demeurait jusqu'ici, malgré l'adoption de la loi sur la sécurité quotidienne en France et celle de la nouvelle Directive européenne sur la protection des données dans le secteur des télécommunications : le passage obligé par une réquisition adressée à un opérateur de télécommunications. Bien que faible rempart contre les atteintes aux droits et libertés des citoyens, cette étape permet néanmoins une certaine visibilité du nombre de demandes d'accès aux données personnelles conservées, de leur teneur et de la finalité de l'enquête (renseignement ou poursuites). Elle permet également une vérification, que l'on espère scrupuleuse, de la légalité de la requête adressée à l'opérateur, tenu par le secret professionnel vis-à-vis de tout autre que l'autorité judiciaire. Par son coût financier, mais également pour des questions d'image commerciale de l'opérateur, cette étape peut constituer un certain frein à l'appétit de renseignement. Enfin, la nécessité de présenter une commission rogatoire oblige au respect de la procédure d'instruction, permet son contrôle et des recours éventuels. En supprimant cette étape, loin de constituer de simples aménagements techniques pour une meilleure efficacité, une telle nouvelle loi représenterait une atteinte gravissime aux droits, aux libertés et à la démocratie.

### **3.4 Recommandations d'IRIS**

Comme nous avons déjà pu l'évoquer, la transposition en droit français de la Directive « *Vie privée et communications électroniques*» est une occasion unique de lever les incohérences de la législation actuelle et de revenir à une législation vraiment protectrice des droits des citoyens. Ajoutons aux problèmes soulignés ci-dessus le fait que la loi sur la sécurité quotidienne, tout au moins ses dispositions qui nous intéressent ici, n'ont été adoptées que pour une durée allant jusqu'à décembre 2003, et il devient clair que cette occasion de la transposition du « *Paquet télécom*» avant fin juillet 2003 doit impérieusement être saisie. IRIS fournit ici ses recommandations à cet égard.

#### ***3.4.1 Recommandations pour l'intelligibilité et l'accès au droit***

La France a été le premier pays à se doter d'une loi protectrice des données personnelles et de la vie privée, avec la loi de 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi, bien pensée, cohérente, fondée sur des principes et définitions clairs, et regroupant en un même texte toutes les dispositions pertinentes, ne fait qu'aujourd'hui l'objet d'une révision profonde, après plus de 30 ans de « *Bons et loyaux services*». Sa première modification partielle n'est d'ailleurs intervenue qu'en 1988. Cette loi a servi de modèle à plusieurs autres pays, qui ont adopté et qui adoptent encore aujourd'hui une législation similaire, parfois au mot près (cas du Maroc par exemple). Elle a également inspiré, par bien des aspects, la rédaction de la Directive européenne 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces données.

***IRIS recommande de suivre la même approche pour redéfinir la législation française relative aux communications électroniques, aux droits des citoyens et aux libertés.***

L'effet d'une telle loi abrogerait et remplacerait notamment les dispositions examinées en section 3.2 de ce document. Une telle décision montrerait une réelle volonté gouvernementale et parlementaire pérenne d'instaurer un vrai débat démocratique dans notre pays, de mettre la loi à la portée du citoyen mais aussi, il faut bien en convenir, de faciliter le travail des juristes, des autorités de justice et de police, de l'administration dans son ensemble, de la société civile et du secteur économique. Qu'il s'agisse de l'utilisation des données dans le cadre d'enquêtes judiciaires, d'utilisations commerciales, des relations des citoyens avec l'administration ou encore dans le cadre du travail, une telle loi pourrait servir de référence à tous, sans oublier que les chantiers sont encore nombreux, ne serait-ce que dans le cadre de l'administration électronique. Enfin, une telle loi témoignerait d'un souci de démocratiser l'accès au droit.

***3.4.2 Recommandations pour lever les incohérences***

L'incohérence démontrée entre la loi sur la sécurité quotidienne et le Code des douanes ne peut subsister. En outre, le risque d'autres incohérences ne peut être pris.

***IRIS recommande de fixer une fois pour toutes, et dans un texte unique de référence, la durée maximale de conservation des données en toutes circonstances □ la teneur de ces données □ les finalités autorisées de cette conservation □ les conditions dans lesquelles ces données sont conservées □ les conditions générales dans lesquelles ces données peuvent être utilisées.***

Ces dispositions devront obéir à la définition de principes simples en ouverture du même texte. Elles pourront bien entendu faire l'objet de spécifications plus précises dans les articles pertinents. Parmi ces principes généraux, on trouvera par exemple l'affirmation de la confidentialité des communications (au sens du 1 de l'article 5 de la Directive « Vie privée et communications électroniques »).

***3.4.3 Recommandations pour surmonter la difficulté de déterminer les données***

Étant entendu que la recherche des responsables d'infractions commises est tout à fait légitime, pour autant qu'elle soit encadrée des garanties nécessaires dans un État de droit, il convient d'établir les conditions raisonnables de cette recherche.

Les données de connexion d'un utilisateur à Internet fournissent les informations sur les auteurs de contenus mis à disposition publique comme sur les auteurs de communications à destination d'un nombre fini de parties. Il s'agit d'une part des données de connexion à Internet (sans trace des services utilisés, l'adresse IP est suffisamment signifiante) détenues par les fournisseurs d'accès, et d'autre part des données de connexion au serveur sur lequel résident les contenus, ainsi que le journal des modifications des pages hébergées, ces données étant en possession du fournisseur d'hébergement. L'ensemble de ces données permet d'identifier l'auteur d'un contenu litigieux, que ce contenu soit public ou non.

Les données d'identification sont des données fournies par un abonné à un fournisseur d'accès et/ou d'hébergement, lors de la création du contrat d'abonnement. Ces données varient actuellement selon le fournisseur. Lorsque le service est payant, elles comprennent forcément des informations nécessaires à la comptabilité du fournisseur et à sa gestion des comptes, ainsi qu'à la facturation du service à l'abonné. Certains fournisseurs gratuits demandent des coordonnées postales complètes, le contrat d'abonnement prenant effet à la réception par le fournisseur d'une lettre de confirmation de l'abonné. D'autres fournisseurs gratuits proposent des abonnements immédiats par voie électronique □ il suffit alors parfois de n'indiquer qu'une adresse de courrier électronique, qui peut être ou non identifiante. Il existe toutefois peu de cas où l'anonymat est total, car on peut en général remonter jusqu'à un fournisseur d'accès détenant des informations plus complètes.

Ces données de base sont de toutes façons conservées par l'immense majorité des fournisseurs d'accès sérieux, qu'ils soient du secteur marchand ou non marchand. Elles leur permettent d'assurer la maintenance et la sécurité de leurs réseaux et machines et de répondre aux besoins de facturation et de contentieux le cas échéant. Elles constituent des données raisonnables et suffisantes pour la recherche des responsables d'infraction.

***IRIS recommande que seules les données de connexion et les données d'identification ainsi définies puissent être conservées par les intermédiaires techniques d'accès et d'hébergement, dans les conditions de secret professionnel établies dans la loi sur la liberté de communication, et pour une durée n'excédant pas la durée normale de conservation pour les besoins de maintenance et de sécurité des réseaux, ainsi que de facturation éventuelle. Pour les données autres que de facturation, la durée maximale autorisée de conservation ne doit pas excéder trois mois.***

Cette durée maximale de trois mois correspond à des besoins raisonnables de maintenance et de sécurité des systèmes, à la pratique des intermédiaires techniques, aux recommandations des autorités de protection des données, ainsi qu'aux statistiques fournies par certaines autorités de police (comme celle du National High-Tech Crime Unit du Royaume Uni), reconnaissant que 95% des infractions dites de «vie quotidienne» peuvent être résolues à l'aide de données datant de moins de trois mois (informations fournies lors d'une réunion d'experts organisée par la Commission européenne en préparation au forum sur la cybercriminalité). Toujours d'après les chiffres fournis par le Royaume Uni, les infractions dites «sérieuses et de criminalité organisée» nécessitent des données datant de 6 à 24 mois (85%) ou datant de plus de 24 mois (15%). Enfin, les crimes graves comme les meurtres ou les actes terroristes peuvent nécessiter des données datant de 5 ans. On comprend à la fois l'insuffisance d'une période de conservation de un an, voire deux ans, pour la résolution de telles affaires, et le caractère tout à fait disproportionné, dans un pays démocratique, d'une telle période de rétention systématique des données. Cela n'empêche pas que, dans le cadre d'enquêtes pour crimes graves, certaines personnes ou groupes de personnes puissent être mis sous surveillance particulière, au cas par cas et avec toutes les garanties nécessaires dans un État de droit.

#### **3.4.4 Recommandations pour le respect des libertés et des droits fondamentaux**

Outre les recommandations générales fournies ci-dessus, il nous apparaît fondamental de revenir sur certaines dispositions précises déjà adoptées afin de les abroger, ou envisagées dans la loi d'orientation et de programmation sur la sécurité intérieure afin de les abandonner.

***IRIS recommande de remplacer les articles 43-9 et 43-10 de la loi sur la liberté de communication par les dispositions générales définies ci-dessus pour la conservation des données de connexion et d'identification.***

Cette recommandation supprime en outre la nécessité de décret d'application. Il peut en aller facilement de même pour l'article 29 de la loi sur la sécurité quotidienne.

***IRIS recommande de remplacer le II de l'article L.32-3-1 du code des postes et télécommunications, introduit par l'article 29 de la loi sur la sécurité quotidienne, par les dispositions générales définies ci-dessus pour la conservation des données de connexion et d'identification.***

Les données de connexion et d'identification ne doivent servir qu'aux besoins techniques des fournisseurs d'accès et d'hébergement, ainsi qu'à la recherche des auteurs d'infractions dans le cadre d'une instruction judiciaire. Leur extension à une utilisation par l'administration, quelle qu'elle soit, n'est pas admissible dans un pays démocratique. Il se trouvera toujours de «hautes bonnes raisons», le plus souvent d'opportunité conjoncturelle, de la prescrire, mais IRIS considère que les principes de proportionnalité et de finalité de la

collecte et du traitement des données personnelles doivent demeurer, en tant que principes cardinaux, au-dessus de ces contingences.

***IRIS recommande la suppression de l'article 62 de la loi de finances rectificatives de 2001, et de ses conséquences sur le Code des douanes, le Livre des procédures fiscales et le Code monétaire et financier.***

Toujours au motif de la finalité principale de la conservation des données de connexion et d'identification (besoins techniques des intermédiaires et recherches de responsabilité) et dans le souci de garantir des garde-fou minimaux par le recours obligé à la réquisition de données sur commission rogatoire, IRIS estime nécessaire que les données soient conservées par les intermédiaires techniques eux-mêmes, et fournies à l'autorité judiciaire dans des conditions strictes établies par la loi.

***IRIS recommande que les mesures envisagées dans la loi d'orientation et de programmation sur la sécurité intérieure pour l'accès direct par les autorités de police judiciaire aux bases de données des intermédiaires techniques soient abandonnées.***

Concernant le déchiffrement des données (articles 30 et 31 de la loi sur la sécurité quotidienne), il n'est pas admissible qu'au prétexte du progrès technique, on s'autorise à bafouer les principes généraux de l'État de droit et plus spécialement les garanties relatives au respect de la présomption d'innocence, au respect du secret professionnel, à l'interdiction de l'auto-incrimination et de l'incrimination par les proches, ainsi qu'aux droits légitimes de la défense, notamment le droit à un procès équitable et au recours.

***IRIS recommande la modification des articles 30 et 31 de la loi sur la sécurité quotidienne, ainsi que de leurs décrets d'application, de sorte que toute demande de déchiffrement ne puisse émaner que de l'autorité judiciaire, sous le contrôle du juge des libertés et de la détention la procédure de déchiffrement respecte les droits de la défense, notamment l'information et le droit de recours la procédure de déchiffrement respecte le secret professionnel et les garanties accordées à certaines professions par la législation la procédure de déchiffrement n'autorise pas l'auto-incrimination ou l'incrimination par les proches.***

## **Annexe □ présentation d'IRIS**

IRIS (Imaginons un réseau Internet solidaire) est une association française à but non lucratif créée en octobre 1997.

L'objet d'IRIS est la défense des libertés individuelles et des libertés publiques sur Internet, la promotion de l'accès à Internet en tant que service public, et la promotion des usages non marchands du réseau.

En France, IRIS est membre de l'intercollectif DELIS (Droits et libertés face à l'informatisation de la société □ [www.delis.sgdg.org](http://www.delis.sgdg.org)), et du R@S (Réseau associatif et syndical □ [www.ras.eu.org](http://www.ras.eu.org)). À l'échelle européenne, IRIS est membre fondateur de la fédération EDRi (European Digital Rights □ [www.edri.org](http://www.edri.org)). Au plan international, IRIS est membre de la coalition GILC (Global Internet Liberty Campaign □ [www.gilc.org](http://www.gilc.org)).

L'association est active aux plans national (auditions et consultations institutionnelles, sensibilisation du milieu associatif et syndical aux enjeux politique et sociaux d'Internet, publication de rapports et analyses, conférences et débats, ...), européen (groupes de travail de la Commission européenne sur les contenus illégaux et offensants sur Internet et sur la cybercriminalité) et international (interventions auprès du Conseil de l'Europe et de l'Unesco, notamment dans le cadre de la coalition GILC, etc.). IRIS fait partie des ONG accréditées pour la participation au Sommet mondial sur la société de l'information.

Pour plus de renseignements, voir le site d'IRIS □ [www.iris.sgdg.org](http://www.iris.sgdg.org).